,

מדינת ישראל - רשות שוק ההון, ביטוח וחיסכון

חטיבת חיסכון פנסיוני

מכרז 5/2025

למערכת סליקה פנסיונית מרכזית - הפעלה, תחזוקה ופיתוח

את מסמכי המכרז ניתן למצוא באתר האינטרנט של מינהל הרכש הממשלתי בכתובת: www.mr.gov.il תחת הכותרת – מכרז 5/2025 – למערכת סליקה פנסיונית מרכזית - הפעלה, תחזוקה ופיתוח

הקדמה

רשות שוק ההון, ביטוח וחיסכון (להלן – **הרשות** או **המזמין**) מזמינה בזאת מציעים להציע הצעות להפעלה, תחזוקה ותמיכה של מערכת סליקה פנסיונית מרכזית (להלן – **מערכת הסליקה**) המשמשת להעברה של מידע אודות לקוחות או כספים בין גופים מוסדיים, בעלי רישיון, מעסיקים ולקוחות, והכל בהתאם להוראות חוק הפיקוח על שירותים פיננסיים (ייעוץ שיווק ומערכת סליקה פנסיוניים), התשס"ה-2005 (להלן – **חוק הייעוץ הפנסיוני**), ולהוראות הממונה על שוק ההון, ביטוח וחיסכון (להלן – **הממונה**) ועל פי תנאי מכרז זה.

החיסכון הפנסיוני מהווה מקור הכנסה מרכזי של הציבור לגיל הפרישה ונדבך מרכזי ברשת ההגנה הסוציאלית שמעניקה המדינה לפרט או לתא המשפחתי שלו כאשר הפרט מאבד את יכולתו לעבוד בעת פרישה לפנסיה, אבדן היכולת להשתכר מעבודה או פטירה. בשני העשורים האחרונים הרשות קידמה מגוון רחב של צעדים במטרה להבטיח את היכולת של הפרט להשיג פנסיה הולמת בגיל פרישה ולהבטיח הליך שיווק וייעוץ מיטבי ללקוח. לאור הקושי באיסוף המידע לצורך קבלת החלטות מושכלת ומתן שירות שיווק וייעוץ פנסיוני מיטבי וכן לאור חוסר היעילות בתהליכי העבודה בין השחקנים השונים בשוק החיסכון הפנסיוני, קידמה הרשות צעדים שתכליתם הגברת התחרות בשוק החיסכון הפנסיוני, הבטחת הזכות של הפרט לבחור במוצר הפנסיוני המתאים למאפייניו, צמצום ניגודי העניינים בין השחקנים השונים הפועלים בשוק ומתן כלים ללקוח ולבעל הרישיון לשם קבלת החלטות מושכלת.

בשנת 2012 הוקמה מערכת הסליקה על מנת להנגיש מידע פנסיוני באופן מרוכז ומלא לציבור החוסכים על ידי יצירת תשתית מיכונית אחידה לקבלת מידע לצורך מתן ייעוץ ושיווק פנסיוני וקבלת החלטות מושכלת של ציבור החוסכים. כמו כן, מערכת הסליקה נועדה לייעל את תהליכי העבודה המורכבים המאפיינים את שוק החיסכון הפנסיוני ולסנכרן בין הגורמים השונים. כמו כן, נקבע כי במסגרת פעילות מערכת הסליקה הפנסיונית לצד העברת מידע, המערכת תוכל לסלוק כספים פנסיוניים, הן לצורך העברת כספים בין גופים מוסדיים לשם ניוד לקוחות והן לצורך הפקדת כספים פנסיוניים בעד לקוח אצל הגוף המוסדי.

מערכת הסליקה כיום משמשת כפלטפורמה מרכזית להעברה של מידע על חוסכים באופן ממוכן, מכלל הגופים המוסדיים וביניהם, לכלל בעלי הרישיון או מהם או להעברת מידע מכלל הגופים המוסדיים לחוסכים, והכל לגבי מוצרים פנסיוניים או תכנית ביטוח. כמו כן, הגופים המוסדיים מחויבים להתחבר למערכת הסליקה לצורך הנגשת מידע וביצוע פעולות במוצרים הפנסיוניים ואילו מערכת הסליקה מחויבת לספק שירותים לכלל השחקנים בשוק החיסכון הפנסיוני, המחויבים או המעוניינים לפעול באמצעותה, ובהתאם להוראות הדין בעניין זה.

פעילותה של מערכת סליקה תרמה לפיתוח תחום החיסכון הפנסיוני והגברת התחרות בו, לצד שמירת יציבותה של מערכת הפנסיות ופעילותה הסדירה. תרומה זו באה לידי ביטוי, בין השאר, בהעברה יעילה של מידע וכספים במוצרים פנסיוניים והפחתת הפוטנציאל לטעויות בתהליך ההעברה; בתמיכה בתהליכי עבודה מבוקרים ושקופים על ידי גורם מרכזי מפוקח; בסיוע במיצוי זכויות של חוסכים ועוד. כך למשל, פעולת מערכת הסליקה מסייעת להעמיד בפני הלקוח תמונה מלאה לגבי כלל מוצריו הפנסיוניים כבסיס לקבלת החלטות מושכלות לגבי החיסכון הפנסיוני שלו, ומספקת לבעלי הרישיון מידע לקיום הליך ייעוץ ושיווק פנסיוני אפקטיבי ונאות לחוסכים.

סעיף 31ב לחוק הייעוץ הפנסיוני קובע את התנאים לתת רישיון להפעלת מערכת סליקה והנושאים שעל הממונה לשקול בבואו לשקול בקשה למתן רישיון. סעיף 31ב(ד) לחוק קובע כי הממונה רשאי לקבוע כי הענקת רישיון להפעלת מערכת סליקה פנסיונית תיעשה בדרך של מכרז, אם שוכנע כי זוהי הדרך המיטבית להענקתו. בהמשך לכך, קבע הממונה כי הענקת רישיון להפעלת מערכת סליקה תיעשה בדרך של מכרז. המכרז כאמור, יכלול את התנאים הקבועים בחוק הייעוץ הפנסיוני, ויכול הוא לכלול אף תנאים נוספים.

עוד קבע הממונה כי במכרז ייבחר זוכה יחיד מבין המציעים אשר עמו ייחתם הסכם התקשרות, למשך 8 שנים, עם 4 תקופות אופציה להארכת הסכם ההתקשרות למשך שנתיים כל אחת (התקופה המקסימלית להתקשרות היא 16 שנים). במכרז ייבחר זוכה שני למקרה שהזוכה הראשון לא יוכל לספק את השירותים, וזוכה שלישי למקרה שבו הזוכים הראשון והשני לא יוכלו לספק את השירותים והכל לפי שיקול דעת של המזמין.

יודגש, זכייה במכרז אין משמעה קבלת רישיון להפעלת מערכת סליקה. רישיון להפעלת מערכת סליקה יינתן על ידי הממונה רק ככל שהזוכה יעמוד בכל הדרישות המפורטות בהתאם לחוק הייעוץ הפנסיוני, ההוראות השונות המפורטות במכרז זה, וקבלת האישורים המתאימים.

לשלמות התמונה, מכרז זה נכתב בהתאם למדיניות המפורטת במסמך האסטרטגיה של הרשות המפורסם במקביל למכרז זה, בו נקבע, בין השאר, כי יבוצע מעבר הדרגתי ומלא של הטכנולוגיה המשמשת לצורך העברת הנתונים בתחום החיסכון הפנסיוני לטכנולוגיה סינכרונית (API- Application Programming Interface) מ"טכנולוגיית כספות" בתקשורת א-סינכרונית הקיימת היום, בהתאם להוראות ולוחות הזמנים אשר יפורסמו במסגרת אסדרה על ידי הממונה. עוד נקבע במסמך האסטרטגיה כי המערכת תפעל כגורם מרכזי המנהל ומנפיק תעודות אבטחה חתומות דיגיטלית (סרטיפיקט) לשחקנים השונים בשוק, המבקשים לקבל מידע ולבצע פעולות בטכנולוגיית API. זאת על מנת לייצר סטנדרטיזציה בשוק ובמטרה להקל על פיתוח ותחזוקה של מערכות המשתמשות בתעודות אלו. בנוסף, מסמך האסטרטגיה מפרט את השירותים אשר לגביהם תחול חובת שימוש במערכת הסליקה.

הזוכה שיוכרז במכרז יחתום על הסכם התקשרות (חלק ד' למכרז) עם המזמין לתקופה של 96 חודשים ("תקופת ההתקשרות"), כאשר למזמין הזכות להאריך את תקופת ההתקשרות בתקופות נוספות, ועד ל-96 חודשים נוספים.

מסמכי המכרז מחולקים לפרקים, כמפורט להלן:

- חלק א' – הליך המכרז.
- חלק ב' – תוכן השירותים ופירוט ההתקשרות עם הספק הזוכה.
- חלק ג' – חוברת ההצעה, אשר תוגש על ידי מציע המתמודד במכרז.
- חלק ד' – הסכם ההתקשרות עם הזוכה במכרז.

<u>המועד האחרון להגשת הצעות במכרז הוא בתאריך 30/04/2026 בשעה 14:00</u>

הגדרות[1]

בעל רישיון	כהגדרתו בחוק הייעוץ הפנסיוני;
גוף מוסדי	כהגדרתו בחוק הפיקוח על שירותים פיננסיים (ביטוח), תשמ"א-1981;
גורם מתפעל	כהגדרתו בחוזר גופים מוסדיים 9-3-2015 "ביצוע פעולות על ידי גוף מוסדי עבור מעסיק";
הוראות הממונה	כל הוראה שתינתן על ידי הממונה בין אם באמצעות חוזרי הממונה ובין אם באמצעות הוראה פרטנית של נציגיו;
החברה	חברה להפעלת מערכת סליקה פנסיונית מרכזית אשר המציע מחויב להקים לפי מכרז זה, ככל שיוגדר כזוכה;
המזמין או **הרשות**	רשות שוק ההון, ביטוח וחיסכון או ועדת המכרזים של רשות שוק ההון, ביטוח וחיסכון (בהתאמה);
הממונה	הממונה על רשות שוק ההון, ביטוח וחיסכון;
המכרז	כלל מסמכי מכרז זה, לרבות נספחיו;
הסכם ההתקשרות או **ההסכם**	הסכם שיחתם בין הזוכה במכרז לבין המזמין ואשר מצורף כחלק ממסמכי המכרז בחלק ד';
הספק או **הספק הזוכה**	המציע שהצעתו תוכרז כזוכה במכרז, כפי שייקבע על ידי ועדת המכרזים, ו/או החברה אשר תוקם על ידי המציע שיוכרז כזוכה במכרז.
הפרויקט	מכלול השירותים על פי מכרז זה שעל הספק הזוכה לספק, לרבות הפעלתה באופן שוטף במהלך תקופת ההתקשרות;
חוזר מבנה אחיד	חוזר גופים מוסדיים 3-9-2024 "מבנה אחיד להעברת מידע ונתונים בשוק החיסכון הפנסיוני", כפי שישתנה מעת לעת;
חוזר חובת שימוש	חוזר גופים מוסדיים 12-9-2019 שעניינו "חוזר חובת שימוש במערכת סליקה פנסיונית מרכזית – עדכון", כפי שישתנה מעת לעת;
חוזר ייפוי כוח	חוזר סוכנים ויועצים 8-10-2018 שעניינו ייפוי כוח לבעל רישיון;

[1] יש להתייחס לגרסה העדכנית ביותר (לרבות חוזר המחליף חוזר שבוטל) שפורסמה על ידי הרשות בהתייחס לכל חוזר הממונה אשר מוזכר בסעיף הגדרות.

חוזר ניהול סיכוני סייבר	חוזר גופים מוסדיים 2016-9-14 שעניינו "ניהול סיכוני סייבר בגופים מוסדיים", כפי שישתנה מעת לעת;
חוזר פניות איכות המידע	חוזר גופים מוסדיים 2018-9-22 שעניינו "טיפול בפניות איכות מידע – עדכון", כפי שישתנה מעת לעת;
חוזר תשלומים	חוזר סוכנים ויועצים 2022-10-5 שעניינו "תשלום עבור שימוש במערכת סליקה פנסיונית מרכזית – עדכון", כפי שישתנה מעת לעת;
חוזרי הממונה	הוראות אשר מפורסמות מטעמו של הממונה, לרבות העדכונים של הוראות אלה והוראות נוספות שיפורסמו מעת לעת על ידי הממונה;
חוק הגנת הפרטיות	חוק הגנת הפרטיות, התשמ"א-1981;
חוק הייעוץ הפנסיוני או **החוק**	חוק הפיקוח על שירותים פיננסיים (ייעוץ, שיווק ומערכת סליקה פנסיוניים), התשס"ה-2005;
חוק המחשבים	חוק המחשבים, התשנ"ה-1995;
חוק הפיקוח על הביטוח	חוק הפיקוח על שירותים פיננסיים (ביטוח), התשמ"א-1981;
חוק התקנים	חוק התקנים, תשי"ג-1953;
חוק חובת מכרזים	חוק חובת המכרזים, תשנ"ב-1992;
חוק חתימה אלקטרונית	חוק חתימה אלקטרונית, התשס"א- 2001;
חשבון תשלום ואמצעי תשלום	כהגדרתם בחוק שירותי תשלום, התשע"ט-2019;
ייזום תשלומים	שירות יזום בסיסי ושירות יזום מתקדם, כהגדרתם בחוק הסדרת העיסוק בשירותי תשלום וייזום תשלום, תשפ"ג-2023;
כללי המערכת	כהגדרתם בחוק הייעוץ הפנסיוני, סעיף 31י(1); בקישור שלהלן כללי המערכת הקיימים כיום: https://www.swiftness.co.il/%d7%9b%d7%9c%d7%9c%d7%99-%d7%9e%d7%a2%d7%a8%d7%9b%d7%aa/;

לקוח	כהגדרת המונח בחוק הייעוץ הפנסיוני;
מועד ההתקשרות	המועד שבו נחתם הסכם ההתקשרות בין הספק הזוכה לבין הרשות;
מערכת סליקה או **המערכת**	כהגדרת המונח בחוק הייעוץ הפנסיוני. מערכת הסליקה, לרבות קוד המקור, ההתאמות, ממשקים וכל רכיב אחר הנחוץ לשם הפעלתה, לרבות פורטל האינטרנט באמצעותו ניתנת גישה לשירותי המערכת;
מערכת תשלומים	מערכת המבצעת תשלומים והינה מבוקרת כהגדרתה בחוק מערכות תשלומים, תשס"ח – 2008, כגון מערכת "**זה"ב**" (מערכת זיכויים והעברות בזמן אמת) ומערכת "**מס"ב**" (מערכת סליקה בנקאית);
משתמש	גוף מוסדי, בעל רישיון או מעסיק העושים שימוש במערכת הסליקה;
סטנדרט טכנולוגי	תקן לפעילות בשוק הפנסיוני שייקבע בהוראות הממונה ויכלול בין היתר: ארכיטקטורה, אבטחת מידע והגנת הסייבר, הגדרת תהליכים עסקיים, תהליכי הזדהות של משתמשים לקוחות וגורמים אחרים, תהליכי מתן הרשאת גישה וביטול הרשאת גישה, כללים לרמת שירות, הגדרת השירותים ומבנה הפניה והתשובה לכל שירות, אופן ניהול הגרסאות והשירותים שיינתנו על ידי הגופים המוסדיים;
ספק משנה	ספק אשר מספק לספק הזוכה שירותים או מוצרים אשר יותאמו באופן ייחודי לצורך מימוש הפרויקט;
עסקה	כהגדרתה בחוק הייעוץ הפנסיוני;
פורטל האינטרנט	אתר האינטרנט של המערכת באמצעותו, בין השאר, הלקוחות והמשתמשים עושים שימוש במערכת, הפעיל כיום בכתובת https://www.swiftness.co.il;
פנייה איכות מידע	פנייה בנושא עדכניות, מהימנות או שלימות המידע שהועבר מגוף מוסדי באמצעות הסליקה הפנסיונית או בנוגע לאי השלמת ביצוע פעולה במסגרת הסליקה הפנסיונית;
פקודת הראיות	פקודת הראיות [נוסח חדש], התשל"א-1971;
שעות עבודה מקובלות	בימים א'-ה' בין השעות 8:30-17:00;
תכנית העבודה	כפי שמפורטת בפרק המימוש סעיף 5.8.3;

תעודה חתומה דיגיטלית או **סרטיפיקט**	תעודה אשר הונפקה באמצעות מערכת סליקה פנסיונית מרכזית, לשם קבלת גישה לתעבורת מידע באמצעות מערכת ;
תקופת ההתקשרות	פרק הזמן כמפורט בסעיף 2 להסכם ההתקשרות (חלק ד');
תקנות אבטחת מידע	תקנות הפיקוח על שירותים פיננסיים (ייעוץ, שיווק ומערכת סליקה פנסיוניים) (אבטחת מידע במערכת סליקה פנסיונית מרכזית), התשע"ב-2012 ;
תקנות הגנת הפרטיות	תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 ;
תקנות חובת המכרזים	תקנות חובת המכרזים, התשנ"ג-1993 ;
טכנולוגית API	טכנולוגיה סנכרונית (Application Programming Interface) ;
IVR	מענה קולי אינטראקטיבי (Interactive voice response) ;
FCR	אחוז פניות השירות למוקד המקבלות מענה ראוי ומקצועי ומסיימות את כלל מעגל הטיפול כבר בשיחה הראשונה (First Call / Contact Resolution).

תוכן עניינים

חלק א' – הליך המכרז

פרק 1 - מנהלה

1.1. עקרונות המכרז

1.1.1. מכרז זה הוא מכרז פומבי הנערך בהתאם להוראות חוק חובת המכרזים, התשנ"ב-1992 (להלן – **חוק חובת המכרזים**) ותקנותיו, ובכלל זה תקנות חובת המכרזים, התשנ"ג-1993 (להלן – **תקנות חובת המכרזים**).

1.1.2. במסגרת הליך המכרז, הצעות אשר יוגשו במכרז יידרשו לעמוד בתנאי הסף להשתתפות במכרז המפורטים להלן. רק הצעות אשר עמדו בתנאי הסף של המכרז, ידורגו בהתאם לאמות המידה המפורטות במכרז.

1.1.3. בתום הליך המכרז, המזמין יכריז על המציע המדורג ראשון כזוכה במכרז ויחתום עימו על הסכם התקשרות, הכל כמפורט להלן.

1.1.4. המכרז יתנהל בהתאם לדין, ולפי כללי המכרז המפורטים במסמכי המכרז.

1.2. תנאי סף להשתתפות במכרז

1.2.1. **תנאי סף להשתתפות במכרז**

1.2.1.1. רשאי להשתתף במכרז מציע אשר עומד, במועד האחרון להגשת ההצעות, בדרישות המפורטות להלן.

1.2.1.2. הוכחת העמידה בתנאי הסף תתבצע בהתאם להוראות חוברת ההצעה (חלק ג').

1.2.2. **תנאי סף מנהליים**

1.2.2.1. ככל שחלה על המציע חובת רישום בישראל, עליו להיות רשום כדין (להמחשה: על מציע שהוא חברה ישראלית להיות רשום במרשם שמנהל רשם החברות).

1.2.2.2. המציע עומד בדרישות חוק עסקאות גופים ציבוריים, התשל"ו- 1976 (להלן – **חוק עסקאות גופים ציבוריים**).

1.2.2.3. כלל המוצרים והשירותים המוצעים על ידי המציע עומדים בדרישות הרישוי והתקנים הנדרשים על פי דין לצורך אספקתם.

1.2.3. **תנאי סף מקצועיים**

1.2.3.1. <u>ניסיון המציע</u>

למציע ניסיון מוכח של 3 שנים לפחות, בין השנים 2018-2024, בהקמה או בהפעלה של מערכות מידע מורכבות בתחומי הפיננסים או שוק ההון או החיסכון הפנסיוני.

1.2.3.2. המציע העסיק בכל אחת מ-3 השנים אחרונות (2022-2024) לפחות 30 עובדים בתחומי טכנולוגיות המידע.

1.2.3.3. לצורך הוכחת עמידה בתנאי סף זה ניתן לבקש להכיר בניסיונו של בעל השליטה במציע.

לעניין סעיף זה "**שליטה**" – כהגדרתה בחוק ניירות ערך, התשכ"ח-1968.

1.2.3.4. <u>צוות ניהול הפרויקט:</u>

המציע נדרש לצרף להצעתו את פרטי צוות ניהול הפרוייקט המוצע על ידו, על פי הפירוט שלהלן:

1.2.3.4.1. **מנכ"ל** – הכישורים והידע הנדרשים יהיו לפחות:

1.2.3.4.1.1. ניסיון ניהולי של 5 שנים בניהול חברה או גוף ממשלתי עם צוות של 20 עובדים לפחות;

1.2.3.4.2. **מנהל פרויקט** – הכישורים והידע הנדרשים יהיו לפחות:

1.2.3.4.2.1. ניסיון ניהולי של 5 שנים בניהול פרויקט פיתוח והפעלת מערכות מידע מורכבות, עם צוות של 20 אנשי פיתוח טכנולוגי לפחות;

1.2.3.4.2.2. ידע, היכרות מעמיקה וניסיון של 5 שנים בפרויקטים טכנולוגיים בתחומי הפיננסיים.

1.2.3.4.3. **ממונה אבטחת מידע** – הכישורים והידע הנדרשים יהיו לפחות:

1.2.3.4.3.1. בעל הסמכה רשמית ממוסד לימודים מוכר בתחום אבטחת מידע כדוגמת – CISO, CISSP או CISM;

1.2.3.4.3.2. בעל ניסיון של 5 שנים בניהול בתחום אבטחת המידע בפעילות בעלת מורכבות והיקפים דומים לאלו הנדרשים במכרז זה.

1.2.3.4.4. **מנהל פיתוח טכנולוגי** – הכישורים והידע הנדרשים יהיו לפחות:

1.2.3.4.4.1. תואר ראשון במדעי המחשב, הנדסת תעשייה וניהול או מדעים מדויקים ממוסד לימודים מוכר;

1.2.3.4.4.2. בעל ניסיון של 5 שנים בניהול פרויקטים של פיתוח מערכות עם צוות של 10 אנשי פיתוח טכנולוגי לפחות.

לעניין סעיף זה "מערכת מידע מורכבת" – מערכת מרובת תהליכים אשר נותנת שירות למעל ל-500 משתמשים.

1.2.4. **יציבות פיננסית**

1.2.4.1. <u>מחזור כספי</u>

למציע מחזור כספי שנתי בהיקף שלא יפחת מ-25,000,000 ₪ (עשרים וחמישה מיליון שקלים חדשים), בכל אחת מהשנים 2022-2024.

1.2.4.2. <u>הון עצמי</u>

המציע יצרף התחייבות להעמיד הון עצמי עבור החברה שתוקם במידה שיוכרז כזוכה במכרז (כאמור בסעיף 1.3 להלן), על פי הפירוט שלהלן וכל עוד לא נקבעו תקנות לענין זה לפי סעיף 31ב(א)(3) לחוק:

1.2.4.2.1. הון עצמי שלא יפחת מסך של 15,000,000 ₪ (חמישה עשר מיליון שקלים חדשים) אשר יעמוד לאורך כל תקופת החפיפה ועד להשלמתה;

1.2.4.2.2. הון עצמי שלא יפחת מסך של 10,000,000 ₪ (עשרה מיליון שקלים חדשים) אשר יעמוד החל מהשלמת שלב החפיפה ועד סוף תקופת ההתקשרות.

1.2.4.2.3. סכומי ההון עצמי האמורים לעיל, יהיו נקיים מכל שיעבוד, עיקול וזכות צד ג' כלשהי.

1.2.4.2.4. המציע יפרט בתצהיר ההתחייבות להעמדת ההון העצמי את האמצעים ההוניים העומדים לרשותו, לרבות סעיף עודפים בהון העצמי.

1.3. התחייבויות ומסמכים נוספים שעל המציע להגיש במסגרת ההצעה

להלן פירוט ההתחייבויות, המסמכים והאישורים הנוספים שעל המציע להמציא במסגרת הצעתו למכרז זה:

1.3.1. **התחייבות להקמת חברה להפעלת מערכת סליקה פנסיונית מרכזית**

1.3.1.1. בהתאם להוראות סעיף 31ב חוק הייעוץ הפנסיוני, הממונה רשאי לתת רישיון להפעלת מערכת סליקה פנסיונית מרכזית לחברה שעיסוקה הבלעדי הוא הפעלת מערכת סליקה פנסיונית מרכזית.

1.3.1.2. המציע יצרף להצעתו התחייבות להקמת חברה להפעלת מערכת סליקה (להלן – **החברה**) בתוך 30 ימים ממועד הזכייה, אשר תעמוד בכלל

דרישות פרק ה'1 לחוק הייעוץ הפנסיוני, וזאת ככל שיוכרז כזוכה במכרז.

1.3.1.3. ההתחייבות תכלול פירוט רשימת בעלי המניות (כולל בעלי השליטה) וחברי הדירקטוריון המוצעים. בנוסף לכך, המציע יצרף להצעתו "הסכם מייסדים" הכולל התייחסות, לכל הפחות, לחלוקת המניות המוצעת ואופן הצבעה בדירקטוריון.

1.3.1.4. החברה לא תעסוק בכל עיסוק אחר, לרבות עיסוקים מסחריים נוספים שאינם קשורים ישירות לביצוע התחייבויות המציע הזוכה במסגרת המכרז.

1.3.1.5. המציע הזוכה מתחייב להעביר לידי המזמין בתוך 45 ימים ממועד הזכייה את המסמכים הבאים:

- תעודת התאגדות ואישור רשם החברות המעידים על הקמת החברה;
- תקנון חברה הכולל סעיף ייחוד עיסוק בהתאם להוראות סעיף זה.

1.3.1.6. כל שינוי בסעיף ייחוד העיסוק של החברה יחייב אישור מראש ובכתב מאת המזמין.

1.3.2. **תכנית עסקית ופתרון טכנולוגי**

1.3.2.1. על המציע לצרף להצעתו את התכנית העסקית לניהול הפרוייקט כמפורט בסעיף 1.7.2.3 להלן.

1.3.2.2. על המציע לצרף להצעתו את הפתרון הטכנולוגי ליישום הוראות מכרז זה כמפורט בנספח ג.9. יובהר כי על הפתרון הטכנולוגי לכלול התייחסות לאיכות הפתרון הטכנולוגי, לרבות התייחסות לקריטריונים שנקבעו בסעיף 1.7.2.2 להלן.

1.4. בעלות על המערכת והעברתה

1.4.1. הספק יהא הבעלים הבלעדי של כל רכיבי מערכת הסליקה, ובכלל זה רכיבי תוכנה, חומרה, תשתיות, גיבוי, קוד מקור, סיסמאות, רשימת רישיונות, רשימת ספקי המשנה, פרטים אודות מוקד התמיכה, פרטים אודות הפעלת פורטל האינטרנט, כללי ונהלי המערכת וכל מידע נוסף הנחוץ לשם הפעלת המערכת (להלן – **רכיבי המערכת**).

1.4.2. על הספק לרכוש "שם מתחם" (דומיין) באנגלית ובעברית למערכת, אשר יאושר עם המזמין מראש ובכתב, ולדאוג לחידוש הדומיין לכל אורך תקופת ההתקשרות והאופציות, ככל שימומשו. על הספק הזוכה להעביר את הבעלות בדומיין במועד סיום ההתקשרות למי שייקבע על ידי המזמין. יובהר כי הבעלות על שם המתחם (דומיין) יהיה של הרשות.

1.4.3. על אף האמור בסעיף זה, הספק יהיה רשאי לעשות שימוש מקביל ברכיבי המערכת, למעט המידע השמור בה והמועבר בה, לאחר קבלת אישור הממונה מראש ובכתב בתום תקופת ההתקשרות.

1.4.4. בתום תקופת ההתקשרות, הספק יעביר את כל רכיבי המערכת, למעט חומרה וציוד פיזי אחר, לידי מי שיקבע המזמין, וזאת ללא קבלת כל תמורה.

1.5. העדר ניגודי עניינים

1.5.1. המציע יצהיר כי אינו מחזיק בקשרי בעלות לגוף מוסדי או לבעל רישיון או לתאגיד בנקאי, כהגדרתם בחוק הייעוץ הפנסיוני.

1.5.2. על כל אחד מחברי המציע או מבעלי מניותיו להגיש פירוט של קשרים נוכחיים, ישירים ועקיפים, לרבות רשימת צדדים קשורים ובעלי עניין, עם גופים מוסדיים, בעלי רישיון וכן לענפי החיסכון הפנסיוני והבנקאות בכלל.

1.5.3. עבור כל אחד מבעלי התפקידים המנויים בסעיף 1.2.3.4 יצרף המציע להצעתו תצהיר לפיו אין לבעל התפקיד המוצע כל קשרי בעלות, קשרי עסקים או קשרים אחרים עם גופים כאמור בסעיף 1.5.1, וכן על כל קשר העלול ליצור מצב של ניגוד עניינים פוטנציאלי, קרבה היוצרת חשש לתלות או חשש לפגיעה אפשרית ביישום תפקידו או במטרות מערכת הסליקה.

1.5.4. ועדת המכרזים תוכל לאשר בעל תפקיד שיציג פעילות שכזו, אם תשוכנע שאין בפעילות זו משום ניגוד עניינים או במקרים בהם האפשרות לניגוד עניינים בפעילות נושא המכרז זניחה.

1.5.5. בנוסף להצהרות לעיל, המציע ועובדיו ימלאו הצהרה לעניין העדר ניגוד עניינים, בנוסח המצורף בנספח XX ה1 להסכם ההתקשרות.

1.6. ערבות הצעה

1.6.1. כל מציע שהגיש הצעה, יידרש להגיש ערבות הצעה אוטונומית ובלתי מותנית כבטוחה לקיום הצעתו במכרז בסך של 1,000,000 ₪ (מיליון שקלים חדשים), תוך 7 ימי עבודה מיום קבלת דרישה מעורך המכרז.

1.6.2. הגשת הערבות תהיה תנאי מקדים לבדיקת ההצעה. אין להגיש ערבות כחלק מההצעה אלא רק לאחר קבלת דרישה בדואר אלקטרוני מעורך המכרז המאשרת את הגשת ההצעה ומפרטת את קוד הערבות ותוקף הערבות הנדרשים.

1.6.3. תוקפה של הערבות יפורט בדרישת עורך המכרז להגשתה, ויהיה 120 יום ממועד יצירת דרישת הערבות או עד למועד בחירת הספק הזוכה.

1.6.4. הערבות תהיה דיגיטלית ותונפק ממנפיק ערבות מורשה, בהתאם לנוסח המופיע כנספח "תדפיס ערבות דיגיטלית" להוראת תכ"ם 7.3.3 "ערבויות וביטחונות" ועל

פי ההוראות המפורטות בהוראה זו. להנחיות אודות הגשת ערבות דיגיטלית ראה:

https://govextra.gov.il/digital-guarantee/homepage/

1.6.5. חלף הגשת ערבות דיגיטלית כאמור, גוף סטטוטורי, חברה ממשלתית ומוסד להשכלה גבוהה שהמדינה משתתפת בתקציבו רשאים להגיש הוראת קיזוז בהתאם לנוסח המפורט בהוראת תכ"ם 7.3.3 "ערבויות".

1.7. ניקוד ההצעות

1.7.1. אמות מידה לניקוד הצעות במכרז

הניקוד של כל הצעה במכרז יהיה בהתאם לאמות המידה הבאות:

- איכות – 80%;
- מחיר – 20%;

1.7.2. מדדי איכות

מובהר כי רק מציעים שעמדו בכלל תנאי הסף, יעברו לשלב בדיקת האיכות.

הערכת איכות ההצעות תיעשה לפי המשקלות הבאים:

מס'	רכיב	משקל
1	ניסיון מקצועי של המציע והצוות הניהולי	20%
2	איכות הפתרון הטכנולוגי	35%
3	תכנית עסקית	25%
4	התרשמות כללית וראיון	20%
	סה"כ	**100%**

יודגש כי מעבר לשלב בדיקת הצעות המחיר מותנה בקבלת ציון איכות כולל (רכיבים 1-4) של 70 לפחות. להלן פירוט אופן ניקוד הרכיבים:

1.7.2.1. ניסיון מקצועי של המציע והצוות הניהולי:

ניסיון מקצועי		
קריטריון	**רכיב**	**ציון רכיב**

ניסיון המציע	ניסיון במתן שירותי הפעלה של מערכות מידע מורכבות בתחום הפנסיוני ו/או בתחום פיננסיים ו/או שוק ההון (מעל 10 שנים- ניקוד מלא, 8-10 שנים - 10 נקודות, 4-7 שנים - 5 נקודות, 3 שנים ומטה- ציון 0)	15.00
	ניסיון בהפעלה פיתוח ותחזוקה של מערכת המאפשרת לקיים פעולות (ממשקים אוטומטיים להעברת מידע ומסרים) בין גופים מוסדיים ו/או פיננסיים (מעל 5 גופים מוסדיים/פיננסיים – יינתן ציון מלא, 4 או פחות- ציון 0)	10.00
	ניסיון ביישום תהליכים בפרוטוקולים של API (ניסיון של מעל 3 שנים – 10 נקודות, שנתיים עד 3 שנים – 7 נקודות, שנה עד שנתיים – 3.5 נקודות, מתחת לשנה – 0)	10.00
	ניסיון בהקמה ותפעול פורטלים אינטרנטיים (ניסיון של מעל 3 שנים – 10 נקודות, שנתיים עד 3 שנים – 7 נקודות, שנה עד שנתיים – 3.5 נקודות, מתחת לשנה – 0)	10.00
	ניסיון של שלוש שנים בהפעלת מערך שירות ותמיכה (מעל 3 שנות ניסיון- ציון מלא, אחרת- ציון 0)	5.00
	סה"כ ניקוד מקסימאלי לקריטריון	**50**
ניסיון אנשי המקצוע	**מנכ"ל החברה המוצע:** (תנאי סף - 5 שנות ניסיון ניהולי של לפחות 20 עובדים) ניסיון כמנכ"ל ו/או בניהול יחידה עסקית בת 50 עובדים לפחות. כל שנה מעל תנאי הסף מקנה 2.5 נקודות עד הניקוד המקסימלי	12.50
	מנהל הפרויקט: (5 שנות ניסיון ניהולי של לפחות 20 עובדים ו-5 שנים ניסיון בפרויקטים טכנולוגים - תנאי סף) ניסיון מקצועי בפרויקטים טכנולוגים בתחומי הפיננסיים : מעל 10 שנים – ציון מלא, 8-10 שנים – 10 נקודות, 6-8 שנים – ציון של 5 נקודות.	12.50
	מנהל פיתוח טכנולוגי: (תנאי סף – 5 שנות ניסיון בפיתוח) בעל ניסיון מקצועי של למעלה מ- 15 שנים – ציון מלא, 13-15 שנות ניסיון – 10 נקודות, 11-12 שנות ניסיון – 5 נקודות. 9-10 שנות ניסיון -4 נקודות, 8 שנות ניסיון- 3 נקודות. 7 שנות ניסיון- 2 נקודות, 6 שנות ניסיון- נקודה אחת.	12.50
	ממונה אבטחת מידע (תנאי סף - 5 שנות ניסיון) בעל ניסיון מקצועי של למעלה מ-10 שנים - ציון מלא, 8-10 שנות ניסיון - 10 נקודות, 6-8 שנות ניסיון - 5 נקודות	12.50
	סה"כ ניקוד מקסימאלי לקריטריון	**50**
	סה"כ ניקוד (לשני הקריטריונים)	**100**
	סה"כ משקל רכיב זה במפ"ל –	**20**

1.7.2.2. <u>איכות הפתרון הטכנולוגי:</u>

על המציע להגיש את הפתרון הטכנולוגי המוצע על ידו עבור מערכת הסליקה, ובפרט למעבר העתידי לטכנולוגיית API, כמפורט **בנספח ג.9 – מענה המציע** בחלקים מענה לפרק 2 ומענה לפרקים 3- 4.

איכות הפתרון הטכנולוגי		
קריטריון	רכיב	ציון רכיב
ארכיטקטורת מערכות מידע מוצעת	גמישות/מודולריות הפתרון הטכנולוגי לשינויים עתידיים לרבות היבטי ניידות (Portability) של הפתרון בין סביבות.	10
	הפתרון הטכנולוגי המוצע מבוסס על טכנולוגיות עדכניות (מיקרו שירותים, API פתוחים) ומאפשר גמישות, אינטגרציה והרחבה עתידית בהתאם לצרכים משתנים.	10
	יכולת מוכחת של הספק בפריסה ותפעול של המערכת בסביבת ענן (ככל ויידרש בעתיד ובכפוף לתנאי המכרז), כולל שימוש בטכנולוגיות ענן מתקדמות (כגון קונטיינרים, מיקרו-שירותים, שירותים מנוהלים ואוטומציה)	10
	סה"כ קריטריון	30
אינטגרציה וממשקים	תמיכה בפרוטוקולים מקובלים- –תמיכה מלאה בסטנדרטים נפוצים (REST/JSON, XML,) וחיבור למערכות חיצוניות	5
	רמת פתיחות וניהול ממשקי API (תיעוד, sandbox, versioning)	5
	סה"כ קריטריון	10
רשת, תקשורת ופרוטוקולים	מבנה הרשת ותתי-רשתות המוצעים וכן מידת הגמישות בהגדרת ארכיטקטורת תקשורת (מודולריות, אבטחה פנימית)	10
	סה"כ קריטריון	10
חווית משתמש	ממשק משתמש נוח ומודרני (אפליקציה/אתר)	5
	סה"כ קריטריון	5
אוטומציה וניהול תפעולי	רמת אוטומציה מוצעת בתפעול המערכת	2
	תמיכה בכלי בדיקות אוטומטיים	2
	תפעול ותמיכה פרואקטיביים	1
	סה"כ קריטריון	5
יתירות והמשכיות עסקית	איכות תוכנית BCP ו-DRP	5
	איכות מנגנוני RTO	5
	סה"כ קריטריון	10
אבטחת מידע והגנת הפרטיות	נאותות מערך אבטחת המידע המוצע	5
	חסינות ספקים חיצוניים ושרשרת אספקה	5
	סה"כ קריטריון	10
ניהול וניטור אירועי אבטחת מידע	יכולות ניטור מתקדמות - ניתוח אנומליות-AI , based Detection, SIEM	5
	נאותות מערך תגובה לאירועים המוצע	5
	סה"כ קריטריון	10
	תהליכי זיהוי ואימות משתמשים מוצעים	5

איכות הפתרון הטכנולוגי		
תהליכי זיהוי, אימות וניהול משתמשים	תהליך זיהוי ואימות לקוחות מוצע	5
	סה"כ קריטריון	10
	סה"כ ניקוד	**100**
	סה"כ משקל רכיב זה במפ"ל –	**35**

1.7.2.3. **<u>תכנית עסקית</u>**

על הספק להוכיח איתנות פיננסית ויכולת לממן את הפרויקט במסגרת ההצעה. על המציע לספק תכנית עסקית ריאלית שתתייחס לתקופת החפיפה ול-8 השנים הראשונות של מתן השירותים (ברמה השנתית), התוכנית תכלול לכל הפחות התייחסות למרכיבים שלהלן:

1.7.2.3.1. **דוח רווח והפסד פרופורמה הכולל הערכה של המציע לגבי:**

א. הכנסות, בפילוח לפי מקורות הכנסה;

ב. הוצאות, בפילוח לפי מרכיבי הוצאה – כ"א, קבלני משנה, ציוד ושירותים, הוצאות הנהלה וכלליות וכד';

ג. תרומה לרווח.

1.7.2.3.2. **תזרים מזומנים צפוי.**

האמצעים ההוניים העומדים לרשותו, כולל הון עצמי ונכונות לתת ערבויות ובטחונות וכן נכונות לספק אמצעים הוניים מספקים או יכולת מוכחת לגייס אמצעים הוניים להקמת המאגר ותפעולו.

1.7.2.3.3. **הערכה לגבי היקפי כוח אדם בפילוח ל:**

א. הנהלה;

ב. פיתוח ותפעול;

ג. שירות.

<u>סה"כ משקל רכיב זה במפ"ל – 25 נקודות.</u>

הניקוד ברכיב זה יינתן בהתאם לרמת הריאליות וההיתכנות המעשית של התכנית העסקית שתוגש על ידי המציע, על פי החלוקה לסעיפים לעיל.

1.7.2.4. **<u>ראיון, התרשמות כללית והמלצות מלקוחות קודמים</u>**

ראיון, התרשמות כללית והמלצות מלקוחות קודמים	
רכיב	ציון רכיב
ראיון – דיון ומענה על שאלות בנוגע לפתרון הטכנולוגי המוצע על ידי הספק	20.00

ראיון – ידע מקצועי רלוונטי של צוות ניהול הפרויקט	20.00
ראיון – בקיאות בתחום החיסכון הפנסיוני	15.00
התרשמות כללית לגבי היכולת של המציע לספק את השירותים (בנוסף, תינתן התייחסות למענה המציע בנספח ג.9, באשר לפורטל האינטרנטי ומערך השירות ותמיכה המוצעים על ידו)	25.00
ממליצים – שביעות רצון של לקוחות קודמים- פניה לשני לקוחות קודמים לפחות להם ניתן שירות ע"י המציע תוך התייחסות ביו היתר לפרמטרים הבאים: 1. מקצועיות- 5 נקודות 2. זמינות- 5 נקודות 3.עמידה בלוחות זמנים- 5 נקודות 4. שביעות רצון כללית של הלקוח – 5 נקודות	20.00
סה"כ ניקוד	**100.0**
סה"כ משקל רכיב זה במפ"ל –	**20**

.1.7.3 מדדי האיכות (A)

הניקוד על חלק האיכות יהיה הניקוד המצטבר המשוקלל של הרכיבים המפורטים בטבלת המשקלות. הניקוד המשוקלל יהיה סכום הניקוד שיתקבל עבור כל רכיב, בהתאם לשיקול דעת ועדת המכרזים ובהתאם לאמות המידה להערכות המפורטות בטבלה. שקלול ניקוד האיכות בציון הכולל יעשה לפי הנוסחה הבאה:

$$\mathbf{A} = \sum \boldsymbol{ai} * \boldsymbol{pi}$$

כאשר **a** הוא הניקוד שיינתן עבור כל אחד מהרכיבים המנויים בטבלת המשקולות ו-p הוא המשקל של כל אחד מהרכיבים.

.1.7.4 מדדי מחיר (B)

.1.7.4.1 מציע במכרז נדרש לתת הצעת מחיר בהתאם למפורט ב"טופס הצעת המחיר" (ראה **נספח ג.1 בחלק ג' של המכרז**).

.1.7.4.2 הצעת המחיר למכרז, הכוללת את העלויות עבור כלל השירותים הנדרשים, תנוקד כך שאחוז ההנחה המקסימלי (30%) יקנה את הציון המקסימלי (100 נקודות) ואחוז הנחה מינימאלי (0%) יקנה את הציון המינימאלי (0 נקודות). בין טווחים אלה יינתן ניקוד יחסי;

1.7.5. כך למשל, הצעת מחיר עם הנחה בשיעור של 15% – תקנה ציון של 50 נקודות. אופן חישוב הניקוד המשוקלל:

1.7.5.1. כל הצעה תקבל ציון משוקלל, על פי הנוסחה שלהלן:

A = הניקוד בגין איכות המענה;

B = הניקוד בגין הצעת המחיר;

C = הציון המשוקלל, אשר יחושב על ידי הנוסחה הבאה:

$$\mathbf{C} = 0.8\mathbf{A} + 0.2\mathbf{B}$$

1.8. בחירת זוכה

1.8.1. דירוג ההצעות

1.8.1.1. ההצעות ידורגו בהתאם לציון שהתקבל לאחר שיקלול אמות המידה הקבועות במכרז, כאשר ההצעה בעלת הציון הגבוה ביותר תדורג ראשונה, לאחריה ההצעה עם הניקוד השני בטיבו, וכן הלאה.

1.8.1.2. אם לאחר שקלול ההצעות כמפורט לעיל, ההצעות בעלות הציון המשוקלל הגבוה ביותר קיבלו ציון זהה, יפעל המזמין לפי סדר הפעולות הבא עד לבחירת זוכה:

1.8.1.2.1. יפעל בהתאם להוראות סעיפים 2ב ו-2ד לחוק חובת המכרזים, התשנ"ב-1992, בדבר "עסק בשליטת אישה" ובדבר "עידוד משרתי מילואים בעסקים זעירים, קטנים או בינוניים" כהגדרתם שם, וזאת בתנאי שהמציע עומד בדרישות החוק.

1.8.1.2.2. אם עדיין אין הכרעה, ההצעה בעלת ציון האיכות הגבוה ביותר תדורג ראשונה.

1.8.1.2.3. אם עדיין אין הכרעה, יבצע המזמין הליך תיחור נוסף, בין אותן הצעות, במסגרתו כל אחד מהמציעים יוכל להגיש הצעת מחיר מטיבה ביחס להצעתו המקורית.

1.8.2. בחירת זוכה

בתום דירוג ההצעות כמפורט לעיל, המזמין יכריז על המציע שהצעתו דורגה ראשונה, כזוכה במכרז, בכפוף לביצוע הפעולות המפורטות בסעיף 1.8.4 להלן, וכן יודיע למציעים האחרים על ההכרזה כאמור. אין בהודעה על זכייה כדי ליצור יחסים חוזיים בין הצדדים, אלה ייווצרו רק עם חתימת מורשי החתימה מטעם הרשות על הסכם ההתקשרות בין הצדדים, ובכפוף לעמידת הספק במפורט בסעיף 1.8.4 להלן.

1.8.3. **כשירים לזכייה**

המזמין יהיה רשאי לבחור כשירים במכרז ("**הכשיר**"), וזאת בהתאם לסדר דירוג ההצעות במכרז. אם תבוטל זכייתו של זוכה במכרז, מכל סיבה שהיא, בתקופה שעד תום שנה מיום בחירתו כזוכה, רשאי המזמין להכריז על הכשיר הבא אחריו כזוכה בכפוף לעמידה בדרישות המנויות להלן בנוגע לזוכה במכרז.

1.8.4. **תנאים לחתימה על הסכם ההתקשרות עם הזוכה**

1.8.4.1. כתנאי לחתימת המזמין על הסכם ההתקשרות, על הזוכה לבצע את הפעולות הבאות, בפרק זמן שיוגדר על ידי המזמין:

1.8.4.1.1. אם הזוכה הוא חברה, עליו להעביר אישור מעודכן כי החברה אינה רשומה כמפרת חוק ואינה מצויה בהתראה לפני רישום כחברה מפרת חוק. לצורך זה ניתן להיעזר באתר הגיידסטאר.

1.8.4.1.2. להגיש את הסכם ההתקשרות שבחלק ד' למכרז, על נספחיו (לדוג' נספח ביטוח, נספח ערבות בנקאית לטובת ביצוע ההתקשרות ("ערבות ביצוע"), נספח סודיות והיעדר ניגוד עניינים וכדו') כשהוא חתום על ידי הזוכה.

1.8.4.2. להגיש את הסכם ההתקשרות שבחלק ד, על נספחיו (לדוג' נספח ביטוח, נספח סודיות והיעדר ניגוד עניינים וכדו') כשהוא חתום על ידי הזוכה.

1.8.4.3. על הזוכה להירשם כספק (ככל שאינו רשום) בפורטל הספקים הממשלתי לשם הגשת דיווחים וחשבוניות. לצורך כך, הזוכה יידרש לשאת בכל העלויות, ככל שישנן, ולאשר את תנאי השימוש בפורטל (ראה הוראת תכ"ם 7.12.5 "פורטל הספקים").

1.8.4.4. אם הזוכה לא הצליח לבצע את הפעולות המנויות לעיל בסד הזמנים שהוגדר על ידי המזמין, יוכל המזמין, בהתאם לשיקול דעתו הבלעדי, לתת לו ארכה להשלים את ביצוע הפעולות, לפסול את הצעתו ולבטל את המכרז, או להכריז על המדורג הבא כזוכה במכרז. כמו כן יוכל המזמין לחלט את ערבות ההצעה של הזוכה.

1.8.5. **תחילת מתן השירותים**

1.8.5.1. לאחר שימלא הזוכה את כל התנאים הנקובים יוסיף המזמין את חתימת מורשי החתימה מטעמו על גבי הסכם ההתקשרות (להלן - **מועד החתימה על הסכם ההתקשרות**).

1.8.5.2. על הזוכה להיות מוכן לתחילת העבודה, בזמנים המוגדרים בתכנית העבודה.

1.9. מופעים ומועדים במכרז

1.9.1. מועדי המכרז

1.9.1.1. <u>הליך המכרז יתבצע, בהתאם ללוח הזמנים המפורט להלן:</u>

נושא	תאריך
מועד פרסום המכרז	30/11/2025
מועד אחרון לרישום לכנס ספקים	14/12/2025
מועד כנס הספקים	16/12/2025
מועד אחרון להגשת שאלות הבהרה	05/01/2026
מועד אחרון להעברת תשובות המזמין	17/03/2026
מועד תחילת הגשת הצעות	18/03/2026
מועד אחרון להגשת הצעות	30/04/2026
תוקף ההצעה וערבות הצעה	30/08/2026
ראיון	השעה תימסר למציעים הרלוונטיים בסמוך למועד הריאיון

1.9.1.2. הזמנים המפורטים בטבלה מחייבים את כל מי שמעוניין להתמודד במכרז. שינוי לוחות הזמנים יתבצע על ידי המזמין בלבד, ובהתאם לשיקול דעתו הבלעדי.

1.9.1.3. כל שינוי במועדי המכרז או עדכונים הנוגעים להם יפורסמו באתר האינטרנט של מינהל הרכש הממשלתי בכתובת: www.mr.gov.il תחת שם המכרז – מכרז 5/2025 – למערכת סליקה פנסיונית מרכזית - הפעלה, תחזוקה ופיתוח ("**דף המכרז**").

1.9.2. כנס ספקים

1.9.3. השתתפות בכנס המציעים <u>אינה</u> מהווה תנאי להשתתפות במכרז, אולם מציע אשר לא ישתתף בכנס, יהיה מנוע מלטעון כי הוא לא קיבל מידע שניתן במהלך הכנס. כנס הספקים יהיה מקוון וחסוי כך שפרטי המציעים יהיו ידועים למזמין בלבד.

1.9.4. ההשתתפות בכנס והרישום באחריות המציע ועליו לוודא את רישומו ברשימת המשתתפים בכנס באמצעות קבלת אישור השתתפות מהמזמין.

1.9.5. יש להירשם מראש לכנס באמצעות שליחת שם הנציג שישתתף מטעם המציע בכנס לכתובת המייל Pension2025@mof.gov.il. כל נציג שישתתף בכנס יוכל לייצג מציע אחד בלבד.

1.9.6. כנס המציעים יתקיים באופן מקוון. קישור לכנס יישלח למי שנרשם מראש, כמפורט לעיל. כנס המציעים המקוון יתנהל בהתאם לכללים שיקבע המזמין.

1.9.7. תשובות שיינתנו בכנס המציעים יחייבו את המזמין רק אם ניתנו בכתב והועברו לכלל המציעים בהתאם למפורט להלן.

1.9.7.1. **<u>שאלות הבהרה בנוגע למכרז</u>**

1.9.1.4.1 בכל מקרה של אי בהירות או הערות בנוגע למכרז, מועדיו או לתנאיו ניתן לפנות למזמין בשאלות הבהרה, וזאת עד למועד האחרון להגשת שאלות הבהרה הנקוב לעיל.

1.9.1.4.2 שאלות הבהרה יוגשו באמצעות מערכת יהלום. מציע אשר מעוניין לשאול שאלות הבהרה, נדרש ללחוץ על הקישור המתאים בדף המכרז ולפעול בהתאם להנחיות במערכת. שאלות שיועברו לאחר המועד הנקוב לעיל, או שיועברו שלא באמצעות מערכת יהלום, לא יחייבו מענה מאת המזמין.

1.9.1.4.3 המזמין רשאי לאפשר סבבים נוספים של שאלות הבהרה, בהודעה שתפורסם בדף המכרז, וזאת בהתאם לשיקול דעתו הבלעדי.

1.9.1.4.4 מציע שלא יפנה למזמין בשאלות הבהרה על המכרז, בהתאם לכללי המכרז, יהיה מנוע מלהעלות בעתיד כל טענה, דרישה או תביעה כנגד המכרז.

1.9.7.2. <u>מענה המזמין לשאלות ההבהרה</u>

1.9.1.5.1 תשובות והבהרות תינתנה בכתב בלבד, נוסחן הוא הנוסח המחייב והן יהיו חלק בלתי נפרד ממסמכי המכרז.

1.9.1.5.2 תשובות והבהרות של המזמין, יפורסמו בדף המכרז. באחריות מציע במכרז להתעדכן בתשובות המזמין וכן בעדכונים שוטפים אשר יפורסמו בנוגע למכרז זה.

1.9.1.5.3 המזמין רשאי לבצע כל שינוי במסמכי המכרז, וכן ליתן פרשנות או הבהרה להוראות מסמכי המכרז.

1.9.1.5.4 המזמין אינו מחויב לנוסח שאלה שהוגשה, ובכלל זה רשאי המזמין, בעת ניסוח מענה לשאלות ההבהרה, לקצר נוסח שאלה או לנסחה מחדש.

1.9.1.5.5 תשובות המזמין יפורסמו ללא שמות הפונים.

1.9.1.5.6 המזמין אינו מתחייב לענות או להתייחס לכל השאלות והבקשות שיועברו אליו באיחור.

1.9.8. הגשת הצעות במכרז

1.9.8.1. הגשת ההצעות למכרז תבוצע באופן מקוון, באמצעות מערכת יהלום, אלא אם כן קבע המזמין.

1.9.8.2. על המציע להגיש במסגרת הצעתו למכרז את חוברת ההצעה בלבד, יחד עם המסמכים שיש לצרפם, כמפורט בחלק ג'.

1.9.8.3. יובהר כי המציע לא נדרש לצרף את כל מסמכי המכרז ולא נדרש להשיב לסעיפים ספציפיים במסגרת מסמכי המכרז, שלא בהתאם לנדרש בחלק ג' למכרז – חוברת ההצעה.

1.9.8.4. ההצעה תוגש כהצעה סרוקה בקובץ PDF, ובנוסף בקובץ Word, אלא אם נקבע מפורשות אחרת.

1.9.8.5. הצעת המחיר (ראה נספח ג.1 בחלק ג' של המכרז) <u>תוגש כקובץ נפרד</u> מחוברת ההצעה בהתאם להוראות המפורטות במערכת להגשת הצעות בקשר עם מכרז זה. מודגש בזה שפרטי הצעת המחיר או העתק ממנה לא יופיעו בחוברת ההצעה בשום דרך שהיא.

1.9.8.6. קישור למערכת יהלום לצורך הגשת הצעות במכרז יפורסם בדף המכרז. מציע המעוניין להגיש את הצעתו במכרז נדרש ללחוץ על הקישור "להגשת הצעות", אשר יעביר אותו למערכת.

1.9.8.7. הליך הגשת ההצעות במערכת כולל 2 שלבים: 1) הזדהות מגיש ההצעה באמצעות מערכת ההזדהות הממשלתית; 2) הגשת ההצעה בתיבת המכרזים במערכת יהלום ("התיבה").

1.9.9. פעולות במערכת ההזדהות:

1.9.9.1. מגיש הצעה אשר טרם נרשם למערכת ההזדהות הממשלתית יידרש להירשם למערכת, ולאחר השלמת ההרשמה לערוך אימות של ההזדהות לצורך מעבר לשלב הגשת ההצעות.

1.9.9.2. מגיש הצעה אשר רשום למערכת ההזדהות הממשלתית, יידרש לאמת את זהותו לצורך מעבר לשלב הגשת ההצעה.

1.9.9.3. בכל תקלה בהליך ההרשמה להזדהות הממשלתית, או בתהליך ההזדהות יש לפנות למוקד התמיכה של המערכת (טלפון - 1299, כתובת דואר אלקטרוני moked@mail.gov.il, טלפון נוסף 08-6863100).

1.9.9.4. לפרטים נוספים אודות הליך ההרשמה ראו בקישור זה.

1.9.9.5. לאחר השלמת ההזדהות, המערכת תעביר את מגיש ההצעה באופן אוטומטי לתיבת המכרז הרלוונטית. על המציע לוודא כי במערכת להגשת ההצעות מופיע שם ומספר המכרז המבוקש על ידו.

1.9.10. **פעולות במערכת יהלום:**

1.9.10.1. במסגרת הגשת ההצעה על המציע לפעול בהתאם להנחיות שיופיעו במערכת יהלום, למלא את כלל השדות שנדרש באופן ברור ובהתאם להנחיות המערכת, ולהעלות למערכת את הקבצים הנדרשים בהתאם להוראות המכרז.

1.9.10.2. מציע יוכל לעדכן את הצעתו כל עוד לא חלף המועד האחרון להגשות הצעות.

1.9.10.3. לאחר השלמת הגשת ההצעה במערכת תתקבל הודעה "הצעתך נשלחה בהצלחה" ומציע יוכל להוריד את מסמך ההצעה. מסמך ההצעה הינו מסמך חתום דיגיטלית של ההצעה ומהווה אסמכתא להצעה שהוגשה. המסמך ישלח למציע גם בדואר האלקטרוני. מסמך ההצעה האחרון שנשלח יוצג גם במערכת בדף הבית של המכרזים באזור "הצעות שנשלחו".

1.9.10.4. לא ניתן יהיה להגיש הצעות במערכת לאחר המועד האחרון להגשת הצעות.

1.9.10.5. במסגרת הגשת ההצעות במערכת, ישנן מגבלות טכניות שונות, כגון:

1.9.10.5.1. ניתן להעלות עד 10 קבצים כאשר הגודל המקסימלי של כל קובץ הוא עד 15MB. ניתן לעלות קבצים מהסוגים הבאים: jiff, pjpeg, pjp, tiff, tif, doc, docx, xls, xlsx, ppt, pptx, pdf, png, jpg, jpeg. לא ניתן לעלות קבצים עם שמות זהים, מומלץ לתת לכל קובץ שם קצר בהתאם לתכולה שלו.

1.9.10.5.2. פרק הזמן שבו המערכת מתנתקת בהיעדר פעולה של משתמש הוא עשרים דקות.

1.9.10.6. על מנת להכיר את יתר מגבלות המערכת, באחריות מגיש ההצעה לקרוא מבעוד מועד את המדריך להגשת הצעות בתיבה הדיגיטלית.

1.9.10.7. לסיוע טכני במקרה של תקלה או שאלה ניתן לפנות למוקד התמיכה בימים א'-ה' בין השעות 8:30-17:00 באמצעות הצ'אט האנושי. יש לציין בפניה את שם המכרז, המועד האחרון להגשת ההצעות ובמידת הצורך לצרף צילומי מסך.

1.9.10.8. זמן ההמתנה מרגע משלוח הפניה ועד לחזרת נציג שירות לא יעלה על 4 שעות בטווח שעות פעילות המוקד. מוקד התמיכה אינו מתחייב לספק מענה לפניות אשר יתקבלו בזמן קצר מ-4 שעות מהמועד האחרון להגשת הצעות. מציע אשר מגיש את הצעתו כאשר ישנן פחות מ-4 שעות להגשת הצעות במכרז לוקח על עצמו את הסיכון שבמקרה של תקלה נציג השירות לא יספיק לפתור את הבעיה הטכנית שלו או לענות על שאלה שיש לו.

1.9.10.9. על מציע במכרז האחריות הבלעדית להגיש את ההצעה לפני המועד האחרון להגשת הצעות. על המציע להביא בחשבון כי בסמוך למועד האחרון להגשת הצעות ייתכן עומס על מערכת ההגשה או תקלות טכניות אחרות אשר ימנעו מהמציע להגיש את הצעתו. על המציע להיערך לכך, ולהגיש את הצעתו מבעוד מועד. למציע לא תהיה כל טענה למזמין באשר לתקלה שהתגלתה במערכת ההזדהות או במערכת הגשת ההצעות סמוך למועד האחרון להגשת הצעות, גם אם כתוצאה מכך הוא לא הצליח להגיש את הצעתו במכרז.

1.9.11. **ביטול אוטומטי של הצעה שהוגשה – תיקונים במסמכי המכרז**

1.9.11.1. כמפורט לעיל, שינויים במסמכי המכרז יתכנו עד למועד האחרון להגשת הצעות ואף לאחר המועד ממנו ניתן להתחיל להגיש הצעות למכרז. אם לאחר שהוגשה הצעה לתיבה, ערך המזמין שינוי במסמכי המכרז, למעט שינוי במועדי המכרז, הצעה שהיתה בתיבה תבוטל באופן אוטומטי ותעבור למצב טיוטה. מציע אשר יהיה מעוניין להגיש את הצעתו בהתאם לתנאי המכרז המעודכנים יידרש לבצע הגשה מחדש.

1.9.11.2. באחריותו הבלעדית של המציע להתעדכן בסטאטוס הצעתו במערכת הגשת ההצעות.

1.9.12. **ריאיון**

1.9.12.1. הודעה בדבר מועד הריאיון תשלח לכל מציע שעומד בדרישות המפורטות במכרז. המזמין רשאי על פי שיקול דעתו לשנות את מועד הריאיון, ובלבד שיודיע למציע על המועד החלופי מראש.

1.9.12.2. המזמין יהיה רשאי לפסול את הצעתו של מציע אשר לא יגיע לריאיון במועד שנקבע לו, או לחלופין לאפשר לו ראיון במועד חלופי, וזאת בהתאם לשיקול דעתו הבלעדי, ולנסיבות המכרז.

1.9.12.3. על המציע להגיע לריאיון יחד עם בעלי התפקידים הנכללים בתנאי הסף או בתבחיני האיכות שפורטו במכרז, אלא אם כן בהזמנה לריאיון המזמין הודיע אחרת.

1.9.12.4. במסגרת הריאיון המזמין יהיה רשאי לדרוש מהמציע או מנציגיו בריאיון להציג בפניו כל מידע או מסמכים או אישורים או רישיונות וכיוצ״ב, אשר לדעת המזמין נחוצים לצורך הוכחת עמידה בדרישות המכרז.

1.9.12.5. במסגרת הריאיון המזמין יהיה רשאי לבחון את הבנתו ובקיאותו של המציע או של נציגיו בתחום השירותים נושא ההליך וכן לבחון את יכולתו של המציע לעמוד בכל התחייבויותיו על פי הסכם ההתקשרות.

1.9.12.6. המזמין יהיה רשאי לזמן יועצים מקצועיים או משקיפים נוספים מטעמו שישתתפו בריאיונות.

1.10. כללי המכרז

1.10.1. בדיקת ההצעות

1.10.1.1. המזמין יבדוק כי המציע הגיש את ההצעה בהתאם להנחיות המכרז וצירף את כל המסמכים כנדרש בחוברת ההצעה (חלק ג'), וינקד את ההצעות בהתאם לאמות המידה המפורטות במכרז.

1.10.1.2. באם המציע, כאישיות משפטית עצמאית, אינו עומד בתנאי הסף המפורטים לעיל, או בתנאים אחרים הקבועים במכרז, ובעברו של המציע התרחש שינוי ארגוני (לדוגמה רכישת פעילות, התאגדות כחברה, רה-ארגון או איחוד של חברות בדרך אחרת), שמאפשר לו עמידה בתנאי המכרז לאחר ההשתלבות בו, יוכל המציע לבקש מהמזמין בכתב ובאופן מנומק לצרף לנתוניו את נתוני הגוף שבו התקיימה הפעילות לפני השינוי הארגוני. החלטה בדבר הכרה כאמור תהיה בכפוף לשיקול דעת המזמין.

1.10.1.3. לצורך בדיקת ההצעות וניקודן רשאי המזמין לעשות שימוש בצוות מקצועי אשר יכול ויכלול גם יועצים חיצוניים.

1.10.1.4. המזמין רשאי לבקש ממציע לבאר פרט מסוים מתוך הצעתו, להשלים בה פרט חסר, או להמציא מסמך נוסף או חלופי המוכיח את עמידתו בתנאי המכרז, ובפרט בתנאי הסף של המכרז, וזאת בתוך פרק זמן קצוב. אי מענה לפניה כאמור, או מענה שלא בפרק הזמן שהוגדר עלול לגרום לפסילת ההצעה, בהתאם לשיקול הדעת של המזמין.

1.10.1.5. אם הוחלט על מתן אפשרות למציע לבצע השלמה של הצעתו, המזמין רשאי לפסול הצעה שעדיין אינה עונה על דרישות המכרז או, בהתאם לשיקול דעתו לבקש השלמה נוספת.

1.10.1.6. אם ימצא בעת בחינת ההצעות כי ההצעה כוללת התנאה או הסתייגות על תנאי המכרז, התנאה או הסתייגות זו לא תזכה להכרה מצד המזמין ועשויה אף להביא לפסילת ההצעה בהתאם לשיקול דעתו הבלעדי של המזמין.

1.10.1.7. לצורך בדיקה ומתן ניקוד להצעות יעשה המזמין שימוש במידע המפורט בהצעה שהגיש המציע וכן הוא רשאי לעשות שימוש במקורות מידע מהימנים אחרים וביניהם הידע המקצועי העומד לרשותו של המזמין, וכן לעשות שימוש בניסיון העבר של המזמין עם המציע או של גוף ממשלתי אחר עם המציע, אם קיים ניסיון כאמור, במידע ציבורי על

המציע, בחוות דעת יועצים מקצועיים וכיוצא באלה. יודגש, לצורך ניקוד ההצעות, המזמין יהיה רשאי להתחשב בניסיון שלו עם המציע או של גוף ממשלתי אחר, וזאת במקום או בנוסף ללקוחות אחרים שפורטו בהצעה, אם פורטו או במסגרת כל אמת מידה רלוונטית אחרת.

1.10.1.8. בדיקת ההצעות במכרז תתבצע באופן הבא – בשלב ראשון יבדקו ההצעות ללא הצעת המחיר. רק לאחר סיום שלב זה יפתח המזמין את מעטפות הצעת המחיר.

1.10.2. **כללים ביחס לערבות ההצעה**

1.10.2.1. לצורך סיום הליך בדיקת ההצעות במכרז, יוכל המזמין כאמור, להאריך את תוקף ההצעות. אם המזמין יחליט על הארכת תוקף ההצעות, יידרש המציע להאריך את תוקף הערבות בהתאמה. אם הערבות לא תוארך כנדרש, יהיה רשאי המזמין לפסול את ההצעה ולחלט את ערבות ההצעה.

1.10.2.2. מבלי לגרוע מהאמור בכל מקום אחר במכרז, חילוט ערבות הצעה יתבצע בהתאם לשיקול דעתו הבלעדי של המזמין, ומהסיבות המנויות בתקנה 16ב(ב) לתקנות חובת המכרזים.

1.10.2.3. טרם חילוט הערבות יתן המזמין למציע הזדמנות להשמיע את טענותיו בנוגע לחילוט האמור. השמעת הטענות כאמור תתבצע בכתב או בעל פה, בהתאם לשיקול דעתו הבלעדי של המזמין.

1.10.2.4. היה ותוקף ההצעה כהגדרתו במכרז זה הסתיים לפני מועד פקיעת תוקף הערבות, יחזיר המזמין את הערבות למציע ובלבד שאין עילה לחלטה.

1.10.3. **ניהול מו"מ עם מציעים**

1.10.3.1. המזמין יהיה רשאי, בהתאם לשיקול דעתו הבלעדי, לנהל משא ומתן עם המציעים או הספק הזוכה במכרז לצורך קבלת הצעה אשר מטיבה עם המזמין.

1.10.3.2. משא ומתן עם מציעים, אם יתקיים, ינוהל בהתאם לתקנה 7 לתקנות חובת המכרזים.

1.10.4. **הצעה יחידה**

1.10.4.1. אם הוגשה במכרז הצעה יחידה או שלאחר בדיקת ההצעות נותרה הצעה אחת בלבד, המזמין, בהתאם לשיקול דעתו הבלעדי יהיה רשאי:

1.10.4.1.1. להכריז על המציע שנותר כזוכה;

1.10.4.1.2. לבטל את המכרז, ולצאת למכרז חדש.

1.10.5. פסילת הצעות

1.10.5.1. המזמין יהיה רשאי לפסול הצעה שהוגשה במכרז, לפי שיקול דעתו, ובמקרים המתאימים לאחר שנתן למציע זכות טיעון (בכתב או בע"פ, בהתאם לקביעתו הבלעדית של המזמין), בין היתר, אם מתקיים אחד מהתנאים הבאים:

1.10.5.2. הצעה הפסדית – אם ההצעה הינה בלתי כלכלית למציע במידה המטילה בספק את יכולתו לעמוד בהתחייבויותיו היה ויזכה במכרז. הצעה תכסיסנית או הצעה המוגשת בחוסר תום לב – אם ההצעה כוללת מחירים או הנחות חריגותסבסוד צולב, dumping וכל מקרה אחר שבו ההצעה נגועה בחוסר תום לב, ובכלל זה במקרה של פעולה או התנהגות של המציע, במסגרת המכרז, שלא בתום לב.

1.10.5.3. התנהגות במכרזים ובהתקשרויות קודמות – המציע, במסגרת מכרז או התקשרות קודמת של המזמין, או של משרד ממשלתי או יחידת סמך אחרים, נהג בחוסר תום לב, בערמה, בתכסיסנות או בחוסר ניקיון כפיים, מסר מידע מטעה או מידע מהותי בלתי מדויק או התנהל בחוסר מקצועיות קיצונית, באופן שלדעת המזמין מצדיק את פסילתו.

1.10.5.4. מצב כלכלי של המציע – אם עקב מצבו הכלכלי הנוכחי או הצפוי של המציע, לרבות הליכי פשיטת רגל או פירוק או תביעות מהותיות הקיימות נגדו, קיים חשש לתיפקודו באם יזכה במכרז.

1.10.5.5. ניגוד עניינים – אם קיים ניגוד עניינים, ישיר או עקיף, או חשש לניגוד עניינים בין ענייני המציע, ההצעה שהוא הגיש, או בעלי העניין בו, לבין השתתפות וזכיה במכרז או ביצוע השירותים על ידי המציע, באופן שלדעת המזמין, בהתאם לשיקול דעתו הבלעדי, אינו ניתן להסדרה.

1.10.5.6. תיאום הצעות - אם קיים חשד סביר לתיאום בין המציע להצעות אחרות במכרז, או בין המציע לבין מציע פוטנציאלי.

1.10.6. מינוי נציג מטעם המציע

1.10.6.1. לצורך המכרז ימנה המציע נציג מטעמו (כמפורט בהסכם ההתקשרות) אשר יהווה את הכתובת הבלעדית לכל פניה בנושא המכרז.

1.10.6.2. כל מענה והתייחסות שתישלח מנציג המציע למזמין, או מהמזמין לנציג המציע תחייב את המציע.

1.10.7. **תוקף הצעות**

1.10.7.1. תוקף ההצעה הוא 120 יום לאחר המועד האחרון להגשת הצעות. המזמין רשאי להודיע על הארכת תוקף ההצעה לתקופה נוספת של עד 120 ימים, זאת לצורך בחירת זוכה במכרז.

1.10.7.2. מציע אינו רשאי לחזור בו מהצעתו בתקופה שבה הצעתו בתוקף.

1.10.8. **ביטול או שינוי המכרז**

1.10.8.1. המזמין רשאי מיוזמתו ועל פי שיקול דעתו הבלעדי, לבטל את המכרז, לשנותו ולעדכנו, לרבות עדכוני מועדים הנקובים בו ופרסום הבהרות על האמור בו.

1.10.8.2. הודעה על ביצוע שינויים כאמור תפורסם בדף המכרז. על מציע האחריות להתעדכן באופן עצמאי בהודעות ועדכונים אשר יפורסמו כאמור בנוגע למכרז זה.

1.10.8.3. ההתקשרות עם הזוכה במכרז מותנית בקיומו של תקציב זמין. אם מסיבות תקציביות לא ניתן יהיה להתקשר עם הזוכה במכרז, רשאי המזמין לבטל את המכרז.

1.10.8.4. המזמין לא יהיה חייב לפצות את המציעים במקרה של ביטול המכרז.

1.10.9. **יועצים שסייעו למזמין בכתיבת המכרז**

1.10.9.1. לצורך כתיבת המכרז המזמין עשה שימוש ביועצים הבאים:

1.10.9.1.1. KPMG

1.10.9.2. יועצים אלו מנועים מלקחת חלק במכרז <u>זה</u>, ולא יכולים לתת ייעוץ למציעים בשלב מכרז זה.

1.10.9.3. מציעים אשר יסתייעו ביועצים אלו לצורך הגשת הצעות במכרז, בין בתשלום ובין ללא תשלום, הצעתם תיפסל, בכפוף לשימוע.

1.10.10. **הוצאות**

1.10.10.1. מציעים הבוחרים להגיש הצעה במכרז יישאו בכל עלות כספית הנדרשת לצורך השתתפותם במכרז, ולא יהיו זכאים להחזר כלשהו מהמזמין בגין עלויות אלו.

1.10.10.2. המציעים לא יהיו זכאים להחזר הוצאות או לפיצוי כלשהו בקשר עם המכרז, לרבות במקרה של הפסקתו, עיכובו, שינוי תנאיו או ביטולו.

1.10.11. **סמכות השיפוט**

1.10.11.1. סמכות השיפוט בכל הקשור לנושאים וענייניים הנוגעים למכרז, או בכל תביעה הנובעת מהמכרז ומניהולו, תהיה אך ורק בבתי המשפט במקום בו יושבת ועדת המכרזים של המזמין.

1.10.12. **סודיות ההצעה וזכות העיון**

1.10.12.1. בכפוף לחובות המזמין על פי דין, המזמין מתחייב שלא לגלות תוכן ההצעה לצד שלישי שאינו מעובדי המזמין או יועצים המועסקים על ידו ונותנים לו שירות לצורך המכרז, אשר גם עליהם תחול חובת הסודיות ואי השימוש בהצעות שהוגשו במכרז אלא לצורכי המכרז בלבד.

1.10.12.2. יחד עם זאת, בהתאם לתקנה 21(ה) לתקנות חוק חובת המכרזים, מציעים במכרז רשאים לבקש לעיין בהצעה זוכה, וכן בפרוטוקולים של ועדת המכרזים ובמסמכים נוספים הקשורים במכרז (או חלקם), מלבד החריגים המנוים בתקנה, ובכלל זה במסמכים שהם בגדר סוד מסחרי או מקצועי, או שעלולים לפגוע בביטחון המדינה, יחסי החוץ שלה, כלכלתה וביטחון הציבור.

1.10.12.3. בהתאם לאמור בתקנות המידע הפלילי ותקנת השבים (מסירת מידע מהמרשם הפלילי לשם התקשרות בחוזה לביצוע עסקה במסגרת מכרז), התשפ"ה-2025 ("תקנות מידע פלילי במכרזים"), אשר הותקנו מכוח חוק המידע הפלילי ותקנת השבים, תשע"ט-2019, מובהר כי ועדת המכרזים לא תחשוף מידע פלילי של מציע במסגרת בקשה לעיון בהצעות במכרז, לרבות את עצם קיומו.

1.10.12.4. בהתאם לאופי המכרז, החלק מההצעה שהוא מוגדר על ידי המזמין כסוד מסחרי או מקצועי ועל כן לא תתאפשר זכות עיון בחלק זה של ההצעה הזוכה.

1.10.12.5. אם ברצון מציע למנוע עיון בסעיפים נוספים של הצעתו בשל טענה לסוד מסחרי, סוד מקצועי, או כל טעם אחר המוזכר בתקנות חובת המכרזים, עליו לציין זאת באופן מפורש בחוברת ההצעה (חלק ג'), במקום המיועד לכך. מובהר כי לא יהא בעצם הבקשה כדי למנוע עיון בסעיפים הרלוונטיים, והחלטה בנושא תתקבל על ידי ועדת המכרזים של המזמין. מובהר כי מחיר ההצעה אינו בגדר סוד מסחרי או מקצועי.

1.10.12.6. מציע שטען שחלק מסוים מהצעתו הוא סוד מסחרי או מקצועי, יהיה מנוע מלדרוש לעיין בחלק זה של ההצעה הזוכה במכרז.

1.10.12.7. בכפוף לאמור לעיל, בהשתתפותו במכרז מסכים המציע, כי במקרה של זכיה במכרז הצעתו תועמד לעיונם של יתר המציעים במכרז בהתאם להוראות הדין ולא יהיו לו כל טענות בקשר לגילוי פרטי הצעתו בהתאם להוראות סעיף זה.

1.10.12.8. במקרה בו ועדת המכרזים של המזמין תדחה את טענת המציע הזוכה בדבר היות חלקים מהצעתו סוד מסחרי או מקצועי, המזמין יודיע לו על כך טרם מימוש זכות העיון בפועל.

1.10.13. **מיצוי הליכים מול הוועדה**

1.10.13.1. אם לאחר מימוש זכות העיון, מציע במכרז סבור שנפלה טעות בהחלטה של ועדת המכרזים, עליו לפנות לוועדה בכתב ולפרט את טענותיו באופן מנומק וזאת לא יאוחר מ-10 ימי עסקים ממועד מימוש זכות העיון.

1.10.13.2. במהלך בירור טענות מציע במכרז, אם ישנן, המזמין לא יעכב את מימוש ההתקשרות עם הזוכה, למעט מקרים חריגים, בהתאם לשיקול דעתו הבלעדי.

1.10.13.3. אם לאחר בירור טענות המציע, ועדת המכרזים, תסבור כי נפלה טעות בהחלטה שקיבלה, לא יהיה במימוש ההתקשרות עם הזוכה כדי למנוע ממנה לקבל כל החלטה נדרשת לצורך תיקון הטעות, ובכלל זה, במקרים חריגים, ביטול הזכייה.

חלק ב' –
תוכן השירותים ופירוט ההתקשרות עם הספק הזוכה

פרק 2 – מפרט השירותים הנדרשים

2.1 רקע

2.1.1. פרק זה מתאר את השירותים הנדרשים ובכלל זה השירות המרכזי של הפעלה, תחזוקה ופיתוח של מערכת סליקה פנסיונית מרכזית בישראל המבוססת על השירותים הניתנים על ידי מערכת הסליקה הקיימת נכון למועד פרסום מכרז זה ומתן שירותים חדשים בהתאם לתנאים המפורטים במכרז זה. מערכת סליקה כאמור תאפשר העברת מידע וכספים בין השחקנים השונים בשוק החיסכון הפנסיוני באמצעות מערכת מרכזית אחת באופן ממוכן ואחיד, בהתאם לפירוט שלהלן.

2.1.2. הספק יידרש לספק את השירותים המפורטים בפרק זה בהקדם האפשרי ולא מאוחר ממסגרת הזמן המפורטת בתכנית העבודה.

2.1.3. מערכת הסליקה לא תשמור מידע המועבר אליה או חלק ממנו, אלא בהתאם להוראות הדין ולאמור בפרק 4 - אבטחת מידע. יודגש כי מערכת הסליקה לא תיזום פעולות, ותבצע אך ורק את הפעולות שהתבקשה על ידי הלקוחות והמשתמשים, בכפוף להרשאה על פי כל דין, למעט משלוח תזכורות לגוף מוסדי אשר לא פעל בהתאם למסר שנשלח אליו במסגרת הזמן שהוקצבה לכך.

2.1.4. מערכת הסליקה תחויב לעמוד בהסכם רמת שירות (**SLA**), לרבות זמינות גבוהה בהתאם לפירוט בסעיף 6.3.1 להלן.

2.1.5. הספק יגבש כללים להפעלת מערכת סליקה, להתחברות ולשימוש במערכת הסליקה וליישום ממשקי המבנה האחיד כמשמעותם בסעיף 31י לחוק הייעוץ הפנסיוני, כמפורט בסעיף 5.6 להלן.

2.1.6. הספק לא יהיה רשאי להציע ללקוחות ולמשתמשי המערכת שירותים נוספים הנוגעים למערכת הסליקה הפנסיונית ולכל הקשור לה, בתשלום או שלא בתשלום, אלא באישור הממונה.

2.1.7. כל השירותים המפורטים בפרק זה מהווים חלק בלתי נפרד מההצעה ועל הספק להביאם בחשבון במסגרת הצעת המחיר.

2.2. לקוחות ומשתמשי המערכת

2.2.1. מערכת הסליקה נדרשת לתת שירות ללקוחות ומשתמשי המערכת, או מי מטעמם:

2.2.1.1. "**לקוח**";

2.2.1.2. "**משתמש**";

"**גורם אחר**" – מערכת מידע אשר קיבלה ייפוי כוח ממשתמש שהוא מעסיק או בעל רישיון לפעול בשמם מול גוף מוסדי בהתאם להוראות החוק.

2.2.2. המזמין יהיה רשאי להרחיב את היקף וסוגי הלקוחות, הגורמים האחרים והמשתמשים במערכת הסליקה מעת לעת.

2.3. המוצרים

2.3.1. מערכת הסליקה תעביר מידע וכספים לגבי מוצר פנסיוני או תכנית ביטוח, מכלל הגופים המוסדיים בהתאם להגדרתם ובכפוף למסגרת החוקית שנקבעה בחוק הייעוץ הפנסיוני, ולגביהם בלבד:

2.3.1.1. סוג מוצר פנסיוני כהגדרתו בחוק הייעוץ הפנסיוני;

2.3.1.2. תכנית ביטוח מפני סיכון מוות או מפני סיכון אובדן כושר עבודה, שהממונה נתן לגביה היתר לפי הוראות סעיף 40(ב) לחוק הפיקוח על הביטוח בשים לב שיועבר רק מידע על עצם קיומה ותוקפה של תכנית הביטוח;

2.3.1.3. תכנית ביטוח מפני סיכון מוות מתאונה, נכות מתאונה, נכות מקצועית, נכות רגילה, שחרור מתשלום פרמיה באבדן כושר עבודה, פיצוי חודשי באבדן כושר עבודה, ביטוח למקרה מוות של בן או בת הזוג או מחלות קשות או קטלניות או ביטוח בריאות או סיעוד אחר, או תכנית ביטוח אחרת שקבע השר, והכל בלבד שהתכנית הייתה כלולה במוצר פנסיוני, ולמעט תכנית ביטוח שהמוטב היחיד בה הוא גוף עסקי, שנכרתה אגב רכישת מוצר ממנו. בשים לב שיועבר רק מידע על עצם קיומה ותוקפה של תכנית הביטוח.

2.3.2. המזמין יהיה רשאי להרחיב את סוגי המוצרים לגביהם תעביר מערכת הסליקה מידע וכספים.

2.4. מצב קיים

מערכת הסליקה מהווה תשתית טכנולוגית המאפשרת מתן שירותים - העוסקים בהעברת מידע, בקשות לקבלת מידע וביצוע פעולות לרבות קבלת המענה עליהן, בין השחקנים השונים בשוק החיסכון הפנסיוני (לקוחות, משתמשים וגורמים אחרים) סליקת כספים באמצעות מס"ב ומתן שירותים נלווים נוספים, כפי שמפורט בנספח ב.4 לחלק ב' של המכרז.

2.5. השירותים המבוקשים

השירות המבוקש הוא הפעלה של מערכת סליקה פנסיונית מרכזית בישראל, המבוססת על השירותים הניתנים על ידי מערכת הסליקה הקיימת, כמפורט בסעיף 1.2 לנספח ב.4 לחלק ב' במכרז זה והקמת שירותים חדשים בהתאם לתנאים והמועדים המפורטים במכרז זה.

יובהר כי השירותים הניתנים ללקוחות ולמשתמשים על ידי הספק הזוכה יהיו לכל הפחות השירותים אותם מספק הספק הקיים וכפי שמפורט בנספח מצב קיים המצורף כנספח ב.4 לחלק ב' במכרז זה.

במסגרת תנאי מכרז זה, מערכת הסליקה תשמש גם כגורם מרכז (מתכלל) להנפקת סרטיפיקטים למשתמשי המערכת וגורמים אחרים המבקשים להתחבר למערכת הסליקה או לבצע פעילות אחרת מול גופים מוסדיים בהתאם לסטנדרט שיוגדר על ידי הממונה.

הספק יידרש לספק את השירותים המפורטים בפרק זה.

השירותים המבוקשים, ובכלל זה הציוד הנדרש לצורך הפעלת מערכת הסליקה וחיבורה ללקוחות השונים, צריכים לענות על דרישות תקניות, איכותיות ומקצועיות המקובלות בשוק החיסכון הפנסיוני ובתחום מערכות המידע וסליקת הכספים, בארץ ובעולם, על הוראות הממונה, וכן על הדרישות המפורטות בסטנדרטים המקצועיים במכרז זה. כל השירותים המפורטים בפרק זה מהווים חלק בלתי נפרד מההצעה ועל הספק להביאם בחשבון במסגרת הצעת המחיר, אלא אם נאמר במפורש אחרת.

מערכת הסליקה תספק פתרון המבטיח סנכרון ותיאום מלא בין כל הלקוחות והמשתמשים הפועלים במערכת. מערכת הסליקה תהיה ערוכה לבצע תהליך המורכב ממספר בקשות לקבלת מידע ולביצוע פעולות בין מספר לקוחות (שניים או יותר), ולבצע תיאום בין אותן הבקשות ובין הלקוחות אליהם נוגעות הבקשות, עד להשלמתן, וזאת על מנת לתמוך בכל סוגי הפעולות השכיחות בשוק החיסכון הפנסיוני.

2.5.1. **<u>שירותים כלליים</u>**

2.5.1.1. הספק יידרש להפעלת מערכת הסליקה הקיימת על כלל שירותיה בטכנולוגיה הקיימת. בנוסף, הספק הזוכה יידרש בהקמה ותפעול תשתית טכנולוגית מותאמת לטכנולוגיית API לשם העברת מידע וביצוע פעולות באופן ממוכן ואחיד בשוק החיסכון הפנסיוני וכן הקמה ותפעול של תשתית טכנולוגית להנפקת סרטיפיקטים.

2.5.1.2. הקמה ותפעול של מנגנוני אבטחת מידע המאפשרים לקבל את המידע ממוסר המידע, לבקר את איכות המידע, לשמור את הנתונים הנדרשים ולהעבירו לנמען המידע, תוך מזעור הסיכונים לפגיעה בפרטיות החוסכים שהמידע על אודותם מועבר באמצעות מערכת הסליקה, והכל כמפורט בפרק 4 אבטחת מידע להלן.

2.5.1.3. חיבור לקוחות ומשתמשים אל מערכת הסליקה, לרבות קיום בחינת מוכנות של המשתמש לשימוש במערכת בסביבת הניסוי (להלן - **אינטגרציה**).

2.5.1.4. מתן שירות שיאפשר הקמת הרשאות לייפוי כוח של לקוח לבעל רישיון.

2.5.1.5. עריכת תיעוד נלווה לגבי השימוש והתמיכה במערכת כמפורט בפרק זה.

2.5.1.6. הדרכה והכשרה של לקוחות ומשתמשים קיימים וחדשים של מערכת הסליקה לשימוש במערכת, בעת הקמתה ולאורך כל תקופת ההתקשרות, לרבות בעת העלאת שירותים חדשים ובעת שינויים בשירותים.

2.5.1.7. הקמה והפעלת מערך שירות ותמיכה ללקוחות ומשתמשי מערכת הסליקה, הכולל מוקד טלפוני ואמצעים אלקטרונים נוספים.

2.5.1.8. הספק ינגיש ויתאים את השירותים שניתנים על ידו בהתאם לחוק שוויון זכויות לאנשים עם מוגבלות, תשנ"ח-1998.

2.5.1.9. קיום ממשקי תקשורת עם גורמים נוספים, מלבד לקוחות ומשתמשי המערכת, בהתאם לצרכי מערכת הסליקה לשם קבלת מידע או מסירת מידע לגורמים אלה במסגרת מתן השירותים הכלולים במכרז זה. בין גורמים אלה ניתן למנות את הרשות, מערכת זה"ב בבנק ישראל, שב"א, מרשם האוכלוסין וכדומה. באחריות הספק לעמוד בדרישות השונות שעשוי לקבוע כל אחד מהגורמים אליהם נדרשת מערכת הסליקה להתממשק, על מנת לעמוד בדרישות מכרז זה ובהוראות הדין, על חשבונו.

2.5.1.10. קיום ממשקי תקשורת עם גורם אחר שהספק יידרש להתקשר מולו לאחר שאושר על ידי הממונה ובאופן שיורה, לרבות הקמת ממשק ייעודי, לשם קבלת מידע, מסירת מידע או סליקת כספים.

2.5.1.11. העברת מידע ודיווחים על פעילות המערכת והמידע המועבר במערכת על פי כל דין ולפי דרישת הממונה.

2.5.1.12. הספק יגבש כללי מערכת להפעלת מערכת סליקה, להתחברות ושימוש במערכת הסליקה וליישום ממשקי המבנה האחיד. אופן כתיבת כללי המערכת, תיעודם, פרסומם והצגתם לציבור ייקבעו על ידי הספק באישור הממונה.

2.5.1.13. הרשות רשאית להורות בכל עת על פיתוחים לצורך שינויים או הרחבות למערכת הסליקה, ובכלל זה לשירותים הניתנים, לסוגי הממשקים, לסוגי המוצרים, או ביחס ללקוחות או משתמשים או גורמים אחרים, והספק יידרש לבצע התאמות לצורך יישום השינויים, ובכלל זה אפיון, פיתוח והעמדת צוות מקצועי לביצוע השיפורים והשינויים. התאמות אלו ייעשו במתכונת ובלוחות זמנים שייקבעו על ידי הממונה ובכפוף לסעיף 2.5.11 לעיל.

2.5.2. **<u>הקמה ותפעול של תשתית טכנולוגית להנפקת סרטיפיקטים</u>**

2.5.2.1 הקמה ותפעול של תשתית טכנולוגית להנפקת סרטיפיקטים למשתמשי המערכת וגורמים אחרים המבקשים להעביר מידע ולבצע פעולות באמצעות מערכת הסליקה או באופן ישיר מול הגופים המוסדיים בהתאם להוראות חוזר

מבנה אחיד ולסטנדרט שיוגדר על ידי הממונה. במסגרת זו, תשמש המערכת כגורם מאשר המוסמך להנפיק סרטיפיקטים ולאמתם בגין כל פעולה המבוצעת באמצעות הסטנדרט לרבות במסגרת פעולות ישירות בין המשתמשים לגופים המוסדיים או הגורמים האחרים שמערכת הסליקה אינה צד להם (פרט לאימות כאמור).

2.5.2.2 השימוש בסרטיפיקט נועד על מנת לאמת את הגורמים המעורבים בתעבורת המידע. גוף מוסדי המהווה כמקור מידע, מערכת הסליקה או מערכת מידע של משתמש או גורם אחר, המהווים הגורמים הפונים לשם קבלת מידע או ביצוע פעולה בגוף המוסדי. פעולה של משתמש הנעשית באמצעות גורם אנושי ישירות מול פורטל האינטרנט אינה מצריכה שימוש בסרטיפיקט והגורם האנושי יעבור תהליך זיהוי ואימות בהתאם לאמור בסעיף 256 להלן.

2.5.2.3 במסגרת תהליך הצירוף של גורמים אחרים, המערכת תערוך בדיקות לווידוא כי הגורם האחר עומד בדרישות אבטחת המידע והגנת הסייבר וכן כי הגורם האחר פועל באמצעות הסטנדרט וכל זאת בהתאם לכללים שייקבעו על ידי הממונה.

2.5.2.4 אחת ל-24 חודשים מערכת הסליקה תדרוש מהגורמים האחרים להמציא אישור על עמידה בהצלחה של סקר אבטחת מידע ומבדקי חדירה אשר יבוצעו ביחד אליהם על ידי גורם מקצועי, עצמאי, חיצוני ובלתי תלוי שאינו מעורב בפיתוח והטמעת מערכות אצל הגורם האחר.

2.5.2.5 מערכת הסליקה תנהל מחזור חיים לסרטיפיקטים ותוכל לחדש, לתקף ולחסום או לבטל סרטיפיקטים לפי העניין

2.5.2.6 יובהר כי, ביטול או חסימה של סרטיפיקט יתאפשר לבקשת בעל הסרטיפיקט או על ידי מערכת הסליקה באישור הממונה.

2.5.2.7 בעת גישה של משתמש באמצעות גורם אחר, המערכת תוודא כי הפעולה או הבקשה למידע בוצעה על ידי המשתמש. ווידוא כאמור עשוי להיערך באמצעות מנגנון זיהוי ואימות המשתמש שיספק למערכת הסליקה וודאות לגבי זהות יוזם הפעולה.

2.5.2.8 כחלק מתפעול תשתית הנפקת הסרטיפיקטים ומבלי לגרוע מהאמור בסעיף 2.5.1 לעיל, תידרש מערכת הסליקה ליתן לכל משתמש או גורם אחר המבקש להשתמש בשירות הנפקת סרטיפיקט, שירותי הדרכה, תמיכה וטיפול בתקלות.

2.5.3. **<u>שירות העברת מידע, בקשה לקבלת מידע, בקשה לביצוע פעולה ואגרגציה</u>**

2.5.3.1. הספק יספק שירותי העברת מידע והעברת מידע אגב ביצוע פעולה לרבות היזונים חוזרים בהתאם להוראות חוזר מבנה אחיד או כל חוזר שיהיה במקומו. ככל שלא יוגדר מבנה אחיד במסגרת הוראות החוזר יוכל הספק להגדיר מבנה שונה להעברת מידע באישור הממונה.

2.5.3.2. הספק יספק שירותי אגרגציה ברמת לקוח למידע (איסוף מידע באופן מרוכז) שהתקבל אצלו במסגרת המענים לבקשות המידע השונות ויציג אותם ללקוחות ולמשתמשי המערכת לפי העניין. אופן הצגת המידע האגרגטיבי על ידי הספק לרבות אופן העברתו ללקוחות ולמשתמשים במערכת יהיו בכפוף לאישור הממונה.

2.5.3.3. מערכת הסליקה תקבל בקשות ותעביר מידע בין ואל הלקוחות באמצעות קבצים או שדרים מסוג JSON ,Word, Excel, XML, PDF, לכל הפחות, בהתאם להוראות הממונה לפי העניין, או סוג קובץ אחר שיוצע על ידי הספק ויאושר על ידי הממונה במהלך תקופת ההתקשרות.

2.5.3.4. מערכת הסליקה תאפשר קבלת מידע באופן רציף, כך שכל מידע המועבר אל המערכת במענה לבקשת מידע, לבקשה לביצוע פעולה או לבקשת העברת כספים של לקוח יימסר לנמען מיד עם קבלתו במערכת, אלא אם כן הוגדר אחרת בבקשת הלקוח.

2.5.3.5. מערכת הסליקה תעביר מידע, לרבות היזון חוזר, ללקוח הנמען רק לאחר שביצעה בקרת איכות המידע כמפורט בסעיף 2.5.4 להלן ובדיקת התאמה לבקשה שהועברה, ובאופן שהמידע יישמר במערכת הסליקה לפרק זמן קצר ככל הניתן.

2.5.3.6. **<u>אופן מתן השירותים ללקוחות ומשתמשי מערכת הסליקה</u>**

2.5.3.6.1. הטיפול בבקשת מידע אשר הועברה במסגרת מערכת הסליקה יסתיים רק לאחר קבלת מידע ו/או היזון חוזר מהלקוח שאליו נשלח המידע על השלמת הטיפול בבקשה. ככל שהמענה לבקשה לא הועבר לשביעות רצונו של הלקוח, הספק יאפשר ללקוח להגיש פניה בנוגע לאיכות מידע כמפורט בסעיף 2.5.6 להלן ובהתאם לחוזר פניות איכות מידע, יימשך הטיפול בבקשה עד לסיום הטיפול בפנייה, בהתאם להוראות החוזר כאמור.

2.5.3.6.2. מערכת הסליקה תחויב לעמוד במדדי רמת השירות (SLA), בהתאם למפורט בפרק 6 למכרז זה.

2.5.3.6.3. מערכת הסליקה תציג ותמסור ללקוח הודעות והתראות בנוגע לסטטוס הטיפול בבקשתו לקבלת מידע או לביצוע פעולה וכן תציג ותמסור ללקוח הודעות והתראות במידה ונדרש להשלים מידע או מסמך לצורך השלמת הגשת הבקשה כמפורט בסעיף 2.5.6 להלן.

2.5.4. <u>בקרת איכות המידע במערכת הסליקה</u>

2.5.4.1. מערכת הסליקה אינה אחראית לתוכן המידע המועבר באמצעותה מגוף מוסדי ללקוח במענה לבקשת מידע ובכפוף לכך שהמידע שהועבר באמצעותה תואם למידע שהעביר הגוף המוסדי.

2.5.4.2. אף על פי כן, המערכת תבצע בקרות ובדיקות להבטחת איכות המידע המועבר במערכת ומהימנותו. הבקרות יהיו מובנות בתהליכי העבודה של המערכת.

2.5.4.3. מערכת הסליקה תבצע באופן יזום ושוטף בדיקות ופעולות להבטחת איכות המידע המועבר במערכת, שלמותו, תקינותו ומהימנותו, בהתאם לסעיפים הבאים לכל הפחות. הבקרות יהיו מובנות בתהליכי העבודה של המערכת, לרבות חיווי למעביר המסר על שגיאה, במידה שקיימת, בזמן אמת. הבקרות והבדיקות יאושרו על ידי הממונה. הספק יידרש לשכלל את הבקרות והבדיקות המבוצעות על ידו מעת לעת. כמו כן, רשאי הממונה להגדיר בקרות ובדיקות נוספות שיבוצעו על ידי הספק לאורך תקופת ההתקשרות.

2.5.4.4. בדיקות איכות המידע ייעשו ללא תלות בזהות הלקוח.

2.5.4.5. הספק יקבע נוהל אשר יפרט את הבקרות והבדיקות שיבוצעו על ידו, לרבות בקרות חכמות שיבוצעו באופן אוטומטי לצורך בקרת איכות המידע ודיווח לממונה במקרים שיוגדרו (להלן – **נוהל בקרת איכות המידע**). נוהל זה יאושר על ידי הממונה, שיהיה רשאי בכל שלב להורות לספק על קיום בקרות ובדיקות נוספות, על פי שיקול דעתו הבלעדי.

2.5.4.6. הבדיקות והבקרות יתבצעו באמצעות מנגנון אוטומטי שמתחשב במאפייני סוגי המוצרים והמשתמשים השונים.

2.5.4.7. מערכת הסליקה לא תבצע תיקונים במידע שהועבר באמצעותה בעקבות ביצוע בקרת איכות המידע.

2.5.4.8. המערכת תעביר למוסר המידע חיווי ייעודי על מידע שיימצא לא תקין, לרבות מהות השגיאה בזמן אמת.

2.5.4.9. מערכת הסליקה תבצע בדיקות כי המידע מועבר בהתאם להוראות שנקבעו בחוזר מבנה אחיד או כל חוזר אחר שבו ייקבעו הוראות לתקינות שלמות וסבירות המידע, כללי המערכת ובקרות מובנות נוספות שהספק יידרש להציע במסגרת נוהל בקרות איכות המידע על מנת לבקר את תקינות שלמות וסבירות המידע, ושאושרו על ידי הממונה. כמו כן, רשאי הממונה להגדיר בקרות ובדיקות נוספות שעל הספק יהיה ליישם. בכלל זה, ומבלי לגרוע מהאמור בכל הנוגע לבדיקות ובקרות שמערכת הסליקה נדרשת לבצע, המערכת תבצע את הבדיקות הבאות לכל הפחות:

2.5.4.9.1. מערכת הסליקה תבצע בדיקת התאמה בין פרטי הזיהוי של הלקוח אשר לגביו הועברה בקשה או פעולה לבין פרטי הזיהוי של הלקוח הכלולים במידע שנמסר לנמען ובהיזון החוזר לגבי מענה לבקשה או לפעולה.

2.5.4.9.2. מערכת הסליקה תבצע בדיקות לשלמות המענה המועבר באמצעות המערכת בהתאם לאופן שבו הוגדרה הבקשה והתהליך לבקשה או ביצוע פעולה.

2.5.4.9.3. מערכת הסליקה תבצע בדיקות בנוגע כל אחד מהשדות הכלולים בדיווח, לגבי נכונות וסבירות הפרטים המופיעים בבקשה לקבלת מידע או ביצוע פעולה וכן בדיקת נכונות וסבירות לגבי המידע והמענה שהתקבל.

2.5.5. **<u>שירות סליקת כספים</u>**

2.5.5.1. נכון למועד זה, מפעיל מערכת הסליקה אינו מבצע באופן עצמאי סליקה ישירה של הוראות תשלום (להלן – **סליקה ישירה**) אלא מבצע סליקה של הפקדות מעסיק שבחר בכך למוצרים הפנסיוניים עבור עובדיו באמצעות מס״ב כספק משנה והמערכת מרכזת את קבצי המידע הנלווים להוראות התשלום לצורך שיוך הכספים לחשבונות העובדים. הספק יידרש לספק שירותי סליקה של כספים במתכונת המבוצעת כיום ובהתאם לנוהל שיקבע אשר יובא לאישור הממונה ויעודכן בהתאם לדרישתו (להלן – **נוהל סליקת כספים**).

2.5.5.2. הממונה רשאי לקבוע הוראות נוספות לעניין אופן סליקת הכספים, ובכלל זה לאפשרות של העברת הוראות התשלום באמצעות גורמים נוספים שאינם תאגידים בנקאיים או להוספת אפשרות לשירות של כתיבה של הוראות תשלום באמצעות מערכת הסליקה (ייזום תשלומים), והספק יידרש להתאים את השירות שיינתן על ידו למתכונת עליה יורה הממונה ובהתאם ללוחות הזמנים שיוסכמו על ידי הספק והממונה ויקבעו מראש ובכתב.

2.5.5.3. נוסף על האמור לעיל וככל שהממונה יורה כי מתן שירות של סליקת כספים יתבצע בדרך של סליקה ישירה באמצעות המערכת (ולא באמצעות ספק משנה) – יינתן לספק פרק זמן של שנה, אותו ניתן יהיה להאריך בהתאם לשיקול דעת הממונה ככל שנדרש, לצורך היערכות למתן השירות. תמחור עלות השירות שתיגבה מלקוחות ומשתמשי המערכת (או מי מהם) עבור מתן השירותים בסליקה ישירה ייקבע מראש ובכתב באישור הממונה. בהקשר זה יצוין ששירות של סליקה ישירה נעשה, נכון למועד זה, באמצעות חיבור למערכת זה״ב בלבד.

נספח ב.1 - סליקה ישירה של כספים, מפרט את הדרישות המרכזיות הרלוונטיות לסליקה ישירה של כספים באמצעות חיבור למערכת זה"ב נכון למועד פרסום מכרז זה. יחד עם זאת, מתן שירות של סליקה ישירה, ככל שיורה על כך הממונה במהלך תקופת ההתקשרות, עשוי להתבקש כך שיינתן באמצעות פלטפורמות וטכנולוגיות תשלום אחרות, ולא בהכרח באמצעות חיבור למערכת זה"ב.

2.5.6. **שירות פורטל ללקוחות ולמשתמשי המערכת**

2.5.6.1. הספק יספק שירותי פורטל למשתמשי המערכת וללקוחותיה. שירותי הפורטל יינתנו ללקוחות ולמשתמשים לצורך מתן השירותים על ידי מערכת הסליקה, וביצוע פעולות באמצעותה כמפורט בפרק זה. כמו כן, הפורטל ישמש להעברת בקשות מידע למסירה והצגה של מידע שהתקבל, ביצוע פעולות ללקוחות ולמשתמשי המערכת ובפרט אלו המוגדרים במסגרת הוראות חוזר מבנה אחיד.

2.5.6.2. מתן השירותים באמצעות הפורטל ייעשה בדרך פשוטה, נגישה, זמינה ואחידה, לשם פניה וגישה למערכת הסליקה.

2.5.6.3. הפורטלים השונים ישרתו את כלל לקוחות ומשתמשי המערכת בסטנדרט המקובל בשוק ובדרכים הבאות לכל הפחות: פורטל אינטרנטי, פורטל אינטרנטי מותאם למובייל ואפליקציה (יישומון) למובייל למי שהוא אחד מאלה: לקוח, מעסיק או בעל רישיון.

2.5.6.4. האפליקציה למכשירים ניידים של מערכת הסליקה תפותח ותהיה זמינה להורדה, ללא תשלום, בכל מערכות ההפעלה הקיימות לאפליקציות.

2.5.6.5. שירותי הפורטל יידרשו לתמוך בלקוחות ובסוגי המשתמשים השונים, ויותאמו לכל הפחות ללקוחות, בעלי רישיון, מעסיקים וגופים מוסדיים, על פי מאפייניהם הייחודיים, צרכיהם ויכולותיהם הטכנולוגיות. כמו כן, הספק יתמוך בפורטל ייעודי עבור רשות שוק ההון.

2.5.6.6. הספק יתמוך בכלל השירותים והממשקים שניתנים באמצעות הפורטל, ללא יוצא מן הכלל, וזאת החל ממועד קבלת האחריות על המערכת ובמשך כל תקופת ההתקשרות;

2.5.6.7. אפיון ותפעול פורטל האינטרנט, לרבות השירותים והמיידעים המוצגים באמצעותו, יינתנו באמצעות תשתית מאובטחת ויהיו כפופים לתקנים ולסטנדרטים בנושא אבטחת מידע והגנת הפרטיות המפורטים בפרק 4 אבטחת מידע ולהוראות כל דין;

2.5.6.8. פורטל האינטרנט יאופיין ויפותח על פי סטנדרטים ותקנים טכנולוגיים מקובלים וישמור על עדכניותו הטכנולוגית הנדרשת בהתאם לאמור בפרק 3 הטכנולוגיה;

2.5.6.9. באחריות הספק לוודא כי הפורטל יעמוד בהוראות הדין ובכלל זה עמידה בהוראות הנגישות לפי חוק שוויון זכויות לאנשים עם מוגבלות, תשנ"ח-1998;

2.5.6.10. הספק יעביר לאישור הממונה נוהל לעניין הפעלה של פורטל האינטרנט בהתאם לדרישות פרק זה והוראות הממונה (להלן – **נוהל פורטל האינטרנט**).

2.5.6.11. ממשקי המשתמש בפורטל יאופיינו ויפותחו על פי סטנדרט, ויעמדו בתקני UI/UX כמקובל לפיתוח אפליקציות ואתרים וישמרו על עדכניותם הטכנולוגית. הפורטל יהיה ידידותי למשתמש, פשוט לתפעול ולהבנה. לשם עמידה בדרישות אלה, יערוך הספק טרם הפעלת הפורטל סקרי שימוש בפורטל אשר יבוצעו על ידי הספק ועל חשבונו, באמצעות גורם המתמחה לעריכת סקרים.

2.5.6.12. הממונה רשאי להנחות את הספק מעת לעת לבצע שיפורים ועדכונים בפורטל, לפי שיקול דעתו הבלעדי.

2.5.6.13. התנאים והמאפיינים הנדרשים במסגרת שירות הפעלת פורטל האינטרנט של מערכת הסליקה:

2.5.6.13.1. ביצוע רישום ראשוני והתחברות למערכת הסליקה לאחר ביצוע זיהוי ואימות הלקוחות ומשתמשי המערכת; הספק יאפשר ללקוחות ולמשתמשים להזדהות באמצעות מספר אמצעי זיהוי ואימות דיגיטליים, לרבות באמצעים לא דיגיטליים על מנת להבטיח גישה לכלל הלקוחות והמשתמשים לשירותי מערכת הסליקה.

2.5.6.13.2. אופן זיהוי ואימות הלקוחות והמשתמשים, ביצוע רישום ראשוני וההתחברות למערכת הסליקה יעשו בהתאם לפרק 4 להלן ובהתאם להוראות הדין ויוגדרו בנוהל פורטל האינטרנט. הנוהל יכיל בין השאר התייחסות לאופן הזיהוי והאימות בהתאם לסוג הלקוח או המשתמש.

2.5.6.13.3. הפורטל יאפשר ללקוח ולמשתמש להגדיר ולנהל הרשאות כניסה לפורטל לביצוע השירותים הניתנים על ידי מערכת הסליקה ולצפייה במידע, ובכלל זה הגדרת הרשאות לפורטל לקבוצות משתמשים מטעם המשתמש (כגון עובדים מורשים מטעם גוף מוסדי או מעסיק או מי מטעמו), והגדרות אלו יובאו לאישור הממונה במסגרת נוהל פורטל האינטרנט.

2.5.6.13.4. הפורטל יאפשר ללקוח לצפות במשתמשים שביקשו מידע לגביו או ביצעו פעולות בשמו אגב ייפוי כוח שנתן לקוח לבעל רישיון וכן יאפשר לו לבטל ייפוי כוח למשתמש מסוים לקבל מידע לגביו באמצעות המערכת, לרבות האפשרות לקבוע שלא תבוצע כל פעולה או בקשה, אלא ביוזמתו בלבדובהתאם לקבוע בהוראות חוזר מבנה אחיד .

2.5.6.13.5. הפעלת הפורטל תהיה באמצעות דפדפנים מקובלים, שיתמכו בשפה העברית והערבית, לכל הפחות. על אף האמור, דוחות ללקוח שיסופקו על ידי מערכת הסליקה יוצגו לכל הפחות בשפה העברית או בשפה הערבית בהתאם לבחירת הלקוח.

2.5.6.13.6. הפורטל יאפשר הורדה של המידע שהועבר באמצעותו, לרבות דוחות ייעודיים בפורמט של קובץ אקסל, XML ו-PDF לפחות, והדפסתם ;

2.5.6.13.7. פורטל האינטרנט יציג מידע שהועבר למערכת, ללקוחות ולמשתמשים לאחר שבוצעה בקרת איכות למידע המוצג ;

2.5.6.13.8. פורטל האינטרנט יאפשר מתן השירותים באמצעותו לכל הלקוחות ומשתתפי מערכת הסליקה באופן רציף ובהתאם להגדרות זמינות המערכת בסעיף 6.3.1 להלן ;

2.5.6.13.9. הממונה יהיה רשאי לדרוש מהספק לבצע התאמות למידע המוצג בפורטל האינטרנט ובכלל זה האפשרות להורות על הסרה או הוספה של תכנים או קישורים לדוגמה לאתרי אינטרנט של הרשות או אתרים ממשלתיים אחרים ;

2.5.6.13.10. הספק יאפשר למשתמשים ולגורמים אחרים באישור הממונה, להוסיף קישורים לפורטל מערכת הסליקה או לעמודים מסוימים בפורטל זה, באתרי אינטרנט המנוהלים על ידם. ואולם, הספק יהא רשאי להתנות הצגת קישורים לעמודים מסוימים בפורטל בדרישות אבטחת מידע על מנת לעמוד בהוראות מכרז זה ובהוראות כל דין.

2.5.6.13.11. מילוי והגשת בקשות באמצעות מערכת הסליקה תעשה באופן מקוון, לרבות צירוף או מילוי של טפסים נלווים במתכונת שקבועה בהוראות הממונה ובנוהל הפעלת הפורטל ושיפורסם על ידי הספק הזוכה, באישור הממונה ויהיו זמינים להורדה בפורטל בכל עת, ובכלל זה טפסים החתומים באמצעות חתימה גרפית ממוחשבת או חתימה אלקטרונית. מילוי בקשות על ידי בעל רישיון יוכל להיעשות באמצעות טופס מקוון בפורטל האינטרנט או באמצעות ממשק אחר שאותו יציע הספק למשתמשים. יובהר כי מערכת הסליקה תידרש לבצע בקרת איכות מידע לבקשות כאמור ולטפסים שהוגשו במסגרתן. יחד עם זאת, ייתכן שבצירוף לטפסים שונים יהיה צורך בהעברת אישורים ומסמכים נלווים אשר נוצרו על ידי צד ג' והמשתמש או הלקוח יוזם

הפעולה יצרפם כקובץ סרוק נלווה לבקשה (למשל אישורים רפואיים או תצלום מסמך מזהה). מובן כי מערכת הסליקה תוכל לבצע בקרת איכות המידע חלקית בלבד לגבי קבצים סרוקים אלה, ככל שניתן.

2.5.6.13.12. הפורטל יאפשר ללקוחות ולמשתמשים ביצוע מעקב אחר סטטוס הבקשה שהוגשה והמענה הנדרש בגינה על כל שלביה ממועד הגשתה ועד לקבלת המענה הנדרש, תוך מעקב אחר לוחות הזמנים המוגדרים בהוראות הרגולציה, לפי העניין.

2.5.6.13.13. הפורטל יאפשר ללקוחות ולמשתמשים הגשת פניית איכות מידע, בהתאם להגדרתה בחוזר פניות איכות מידע וביצוע מעקב על שלבי טיפולה עד לסיום הטיפול בה, לרבות מעקב אחר סטטוס פניות איכות המידע שהופנו אל הגוף המוסדי לפי סוג הלקוח או המשתמש הפונה, סוג הפניה, והתראה על לוחות הזמנים הנדרשים למענה מצד הגוף המוסדי. פורטל האינטרנט יציג לכל גוף מוסדי נתונים לעניין טיפול בפניות איכות מידע שהופנו אל הגוף המוסדי ויאפשר לגוף המוסדי להעביר באמצעות הפורטל מענה בהתאם להוראות חוזר טיפול בפניות איכות מידע.

2.5.6.13.14. הפורטל יאפשר הגשת פנייה למוקדי מערך השירות והתמיכה כמפורט בסעיף 2.5.8 להלן בהתאם לסוג השירות, וקבלת הודעות והתראות בנוגע לטיפול בפנייה ומעקב אחר סטאטוס הטיפול בה, לרבות מידע על הגורם המטפל בבקשה, הגורם שנדרשת תגובתו, פרק הזמן שהוגדר לטיפול בפנייה וצפייה בפירוט ההתראות והודעות שהועברו ביחס לפנייה. הצפייה וההצגה של סטטוס הטיפול בפנייה של הלקוח תתאפשר באמצעות הפורטל, ואופן קבלת ההודעות וההתראות תתבצע בהתאם לבחירת הלקוח לכל הפחות באמצעות דוא״ל או מסרון.

2.5.6.13.15. הפורטל יאפשר ביצוע פעולה של תשלום דמי שימוש באמצעות מערכת ייעודית לביצוע תשלומים (Billing), בהתאם למתכונת ואופן הצגת המידע הקבועים בסעיף 2.5.7 להלן (מערכת הגבייה).

2.5.6.13.16. הפורטל יאפשר ללקוחות ולמשתמשים לבקשתם, לקבל נתונים על אודות המידע וכן נתונים על כספים שהועברו באמצעות מערכת הסליקה בכפוף לפרק הזמן המוגדר בתקנות אבטחת המידע ולהוראות סעיף 31טז׳ לחוק הייעוץ.

2.5.6.13.17. הפורטל יאפשר הצגת דוחות תפעוליים ללקוח או למשתמש לפי העניין לגבי סטטיסטיקת השימוש של הלקוח או המשתמש במערכת הסליקה, תוך הצגת כלל הנתונים והמידע הניתנים להצגה כאמור באמצעות ממשקי המשתמש. הדוחות יהיו ניתנים להורדה.

2.5.6.13.18. בנוסף למפורט לעיל, בפורטל האינטרנט לגוף המוסדי יוצגו דוחות בקרה תפעוליים שיכללו מידע והתראות אודות תהליכי העברת מידע וביצוע פעולות, בין השאר ככל שהגוף המוסדי לא מסר מידע, לא ביצע פעולה או לא העביר היזון חוזר בפרק הזמן שהוגדר עבור כל שירות, כפי שהוגדר בהוראות הממונה ו/או בנוהל פורטל האינטרנט.

2.5.6.14. <u>מידעים כלליים המוצגים בפורטל</u>

הספק יפרסם לציבור בפורטל האינטרנט את המידע הכללי המפורט להלן, לפחות:

2.5.6.14.1. מידע לציבור על פעילות מערכת הסליקה, כגון שעות פעילות, מוקדי תמיכה ודרכי התקשרות עמם, וכן מידע סטטיסטי על פעילות מערכת הסליקה; יובהר כי הממונה רשאי לפרסם באתר האינטרנט שלו מידע סטטיסטי לגבי הפעולות אשר בוצעו באמצעות מערכת הסליקה והתקבלו מאת הספק.

2.5.6.14.2. מידע שמיועד ללקוחות מערכת הסליקה ומשתמשיה, הכולל למשל, פירוט השירותים הזמינים לכל אחד מסוגי לקוחות המערכת או משתמשיה, מדריכים לשימוש במערכת הסליקה, נהלי שימוש וחיבור למערכת (לרבות סוגי החיבורים הזמינים ללקוחות והמשתתפים למערכת הסליקה ועלותם), טופסי מערכת הסליקה וכו';

2.5.6.14.3. כללי מערכת הסליקה לרבות פרסום כללי מערכת קודמים שבוטלו או שעודכנו, לצרכי תיעוד ובקרה;

2.5.6.14.4. הצהרה של הספק בנוגע לאמצעי אבטחת המידע שבהם הוא נוקט על מנת למנוע גישה בלתי מורשית למידע המועבר במערכת הסליקה ולמניעת התממשות של סיכון תפעולי;

2.5.6.14.5. גרסאות ממשקי המידע והפעולות לרבות עדכונים;

2.5.6.14.6. נהלי עבודה של מערכת הסליקה מול הלקוח והמשתמשים בנושאים השונים ובכלל זה נהלים המתייחסים להתחברות למערכת;

2.5.6.14.7. מסמכים כלליים לכלל הלקוחות והמשתתפים, לרבות נהלי אבטחת מידע והגנת פרטיות;

2.5.6.14.8. מידע כללי אודות הספק:

2.5.6.14.8.1. שמות חברי הנהלה הבכירה ונושאי משרה בכירים בחברה ופירוט תפקידיהם;

2.5.6.14.8.2. שמות חברי הדירקטוריון;

2.5.6.14.8.3. בעלי מניות עיקריים;

2.5.6.14.8.4. בעלי שליטה;

2.5.6.14.8.5. תרשים מבנה אחזקות של החברה ככל שהמבנה כולל יותר מחברה אחת.

2.5.6.14.8.6. מידע נוסף בהתאם להוראות המכרז, לדרישות הממונה או בכפוף להוראות כל דין;

2.5.6.15. פורטל ייעודי לרשות שוק ההון, ביטוח וחיסכון

2.5.6.15.1. הספק יקים פורטל אינטרנט ייעודי לדיווח שוטף לרשות שוק ההון אשר יכלול גם הצגת נתונים סטטיסטיים אודות תקלות לקוחות ומשתמשים, פניות איכות מידע , בקשות מידע או כספים שהועברו באמצעות מערכת הסליקה ויספק לרשות כלים לניתוח איכותי של המידע ויאפשר ניתוח אגרגטיבי וסטטיסטי של מגמות ושינויים.

2.5.6.15.2. האופן, התדירות והגדרת המידע, שיועברו בפורטל הייעודי לרשות יוגדרו על ידי הספק ויאושרו על ידי הממונה בנוהל פורטל אינטרנט.

2.5.6.15.3. הפורטל כאמור יכלול לכל הפחות את המידעים הבאים:

א. מידע אודות תקלות (תקלות פתוחות ותקלות סגורות, תוך פירוט עמידה ב-FCR), כפי שמפורטות בפרק SLA 6. המידע יכלול את כלל התקלות הקיימות המתקבלות מכלל הערוצים שבהם מדווחות תקלות במערך התמיכה, סטטוס הטיפול בהן עד לסיומן ופרק הזמן שנדרש לצורך הטיפול בהן, לרבות, תקלות חוזרות;

ב. דוחות בקרה על פעילות מערך השירות והתמיכה;

ג. פירוט אירועי אבטחת מידע והגנת הפרטיות, לרבות פעולות של שחזור מידע, וליקויים שנתגלו בסקרי הסיכונים כמפורט בפרק 4 אבטחת מידע;

ד. נתונים על היקפי הכספים שנסלקו באמצעות מערכת הסליקה לפי תאריכים, גופים מוסדיים וסוג פעולה, נתונים אודות היקף פעילות המערכת המתייחסים לתאריכים, היקף לקוחות ומשתמשים, לרבות דיווחים על היקפי שימוש חריגים, חשד לניצול לרעה של המערכת על ידי לקוח או משתמש לרבות פעולות של לקוח בהיקף חריג או בעלות מאפיינים חריגים;

ה. מידע בנוגע לקצב גידול מספר הלקוחות וכן לגבי כמות נטישת לקוחות;

ו. מידע על דמי השימוש שנגבים מלקוחות ומשתמשי המערכת לפי סוגם ;

ז. עמידה בלוחות הזמנים במענה לבקשות המועברות לגופים המוסדיים ;

ח. נתונים על עמידה במדדי איכות ורמת השירות ובכלל זה תוצאות סקרי שביעות רצון הלקוחות והמשתמשים, כמפורט בפרק SLA 6 ;

ט. נתונים על ליקויים חוזרים ומערכתיים על איכות המידע המועבר בחלוקה לסוגי משתמשים ;

י. כל דיווח אחר שיידרש על ידי הרשות.

2.5.6.15.4. הפורטל הייעודי לרשות יאפשר הפקת דוחות באופן עצמאי על פי פילוח המידע המבוקש ומתן אפשרות להורדת הדוחות כקובץ.

2.5.6.15.5. הפורטל הייעודי לרשות יכלול אפשרות להגדרה של הפרמטרים והמידע שביחס אליהם יועברו חיוויים והתראות אוטומטיים. חיוויים אלו יכולים להתייחס, בין השאר, גם לקבלת התראות על העברת מידע באמצעות מערכת הסליקה שנעשתה בחריגה מהוראות הממונה.

2.5.6.15.6. הפורטל הייעודי לרשות יאפשר לרשות לנהל הרשאות לעובדיה, בכפוף להוראות אבטחת המידע והגנת הפרטיות החלות על הרשות ועל מערכת הסליקה.

2.5.6.15.7. לרשות תישמר הזכות להנחות את הספק לבצע שיפורים ועדכונים בפורטל הייעודי לרשות, בתיאום עם הספק.

2.5.6.15.8. הספק יאפשר לרשות להגיש בקשות לקבלת מידע באמצעות הפורטל הייעודי לרשות בהתאם לדרישות שיעלו על ידי הרשות. בכלל זה, הספק יאפשר לרשות לקבל מידע המועבר באמצעות מערכת הסליקה לשם פיקוח הממונה לפי כל דין, כמפורט להלן :

א. מידע על פעילות של לקוחות או משתמשים המועבר באמצעות מערכת הסליקה בכפוף להוראות החוק לעניין זה.

ב. קבלת נתונים על אודות המידע ונתונים על הכספים המועברים באמצעות מערכת הסליקה.

2.5.7. **<u>שירות גביה במערכת הסליקה</u>**

2.5.7.1. הסכום לתשלום עבור השירותים שניתנים על ידי מערכת הסליקה ללקוחותיה ומועדיהם - תוך הבחנה בין תשלום אשר נדרש מגוף מוסדי (המורכב מדמי שימוש קבועים ודמי שימוש עבור פעולות) ולקוח או משתמש שאינו גוף מוסדי (תשלום דמי שימוש עבור פעולות בלבד), ייקבע בחוזר תשלומים כמפורט בפרק 7 מודל תמחור.

2.5.7.2. להלן יפורט האופן שבו ייגבה תשלום דמי השימוש מהלקוחות.

2.5.7.3. הספק יעביר **לאישור** הממונה נוהל לעניין גבייה וטיפול בחייבים ובפיגורים (להלן – **נוהל הגביה**) - אשר יישם את הוראות סעיף זה, פרק 7 מודל התמחור, הוראות חוזר תשלומים ויתר הוראות הממונה.

2.5.7.4. גביית דמי השימוש של מערכת הסליקה מלקוחותיה תבוצע באמצעות כרטיס אשראי, הרשאה לחיוב חשבון, העברה בנקאית, או תשלום באמצעות אמצעי תשלום דיגיטלי אחר שעומד בסטנדרטים המקובלים הנדרשים בין השאר בהיבט של אבטחת מידע, והכל בהתאם לנוהל הגביה.

2.5.7.5. חיוב הלקוחות בדמי שימוש עבור פעולות, יבוצע מראש עבור כל פעולה שיבקשו לבצע באמצעות מערכת הסליקה וכתנאי לביצוע הפעולה כפי שייקבע בנוהל גביה, אשר יוגדר מראש ויפורסם לידיעת הלקוחות.

2.5.7.6. חיוב משתמשים בגין דמי שימוש עבור פעולות, יכול שיבוצע בחיוב מראש כאמור, בתדירות חודשית או במועד קבוע אחר כפי שייקבע בנוהל גביה, אשר יוגדר מראש ויפורסם לידיעת המשתמשים.

2.5.7.7. חיוב של גופים מוסדיים בגין דמי שימוש קבועים יהיה במועד שיוגדר בנוהל גביה ושיפורסם מראש לגופים המוסדיים.

2.5.7.8. הספק יידרש לאפשר ללקוחות ומשתמשי המערכת לבצע את התשלומים למערכת ולקבל את המידע, באמצעות מערכת ייעודית לביצוע תשלומים (Billing) שתוצג ללקוחות ולמשתמשים בפורטל האינטרנט, כמפורט להלן:

2.5.7.8.1. הצגת דמי השימוש שמערכת הסליקה גובה עבור השירותים השונים, פירוט השירותים שניתנו בפועל ללקוחות והמשתמשים והחיובים בגינם;

2.5.7.8.2. צפיה בהיסטוריית החיובים של הלקוח והמשתמשים לתקופה שתוגדר בנוהל, והפקת דוח ביצוע תשלומים שבוצעו

על ידי הלקוח, שיעודכנו באופן שוטף. הורדה והפצה של הדוח תתאפשר בפורמט של קובץ אקסל ו-PDF לפחות;

2.5.7.8.3. בגין כל תשלום שבוצע עבור שימוש במערכת הסליקה, יופקו עבור הלקוח והמשתמש חשבונית מס וקבלה, אשר יישלחו ללקוח כקובץ באמצעות ערוץ התקשורת של אותו לקוח או משתמש עם מערכת הסליקה (למשל בדוא"ל או במסרון), ואף יוצגו בפורטל האינטרנט ויהיו זמינים לשחזור, להורדה והפצה בפורמט של קובץ PDF לפחות. לקוח או משתמש יהיו רשאים לערער בפני הספק על גובה החיוב בתוך 90 ימים מיום קבלת חשבונית המס והקבלה, ולקבל תגובה על הערעור בתוך שני ימי עסקים, והכל במתכונת שתפורט בנוהל הגביה;

2.5.7.8.4. ככל שמערכת הסליקה תספק ללקוח או למשתמש חבילה של שירותים עבור בקשות שיבוצעו על ידו באמצעות המערכת, יוצג מידע בנוגע למחיר חבילת השירותים, היקף וכמות השירותים שנרכשו באמצעות חבילת השירותים, היקף השירותים שנותרו למימוש ומועד סיום חבילת השירותים ככל שקיים, והכל לפי התנאים שפורטו על ידי מערכת הסליקה בעת רכישת חבילת השירותים, בהתאם לנוהל הגביה ובלבד שתיגבה תמורה אחידה בגין החבילות, כמפורט בפרק 7 מודל התמחור.

2.5.7.9. הספק יהא האחראי הבלעדי לטיפול בחייבים ובפיגורים בתשלום, בהתאם לאפשרויות העומדות בפניו לפי הוראות כל דין.

2.5.7.10. המזמין לא ישפה או יפצה את הספק בגין חיובים שלא שולמו או פיגורים בגבייה מכל סוג שהוא.

2.5.7.11. הממונה עשוי להפעיל את סמכותו לפי כל דין, לפי שיקול דעתו, לגבי לקוחות או משתמשים אשר פועלים בניגוד להוראות הממונה בנוגע לחיבור ושימוש במערכת הסליקה, לרבות אי תשלום.

2.5.8. **<u>מערך שירות ותמיכה ללקוחות</u>**

2.5.8.1. הספק יעמיד לרשות הלקוחות והמשתמשים מערך שירות ותמיכה שיורכב ממספר מוקדי שירות ותמיכה ומערכי תמיכה אחוריים בהתאם לסוגי הלקוחות השונים של מערכת הסליקה (להלן – **מערך שירות**) לטיפול בפניות של לקוחות משתמשים, <u>גופים מוסדיים</u> וגורמים אחרים.

2.5.8.2. בין היתר, מערך השירות יעניק מענה בנושאי רישום וחיבור אל מערכת הסליקה, שימוש ותפעול המערכת, זמינות ממשקי המשתמש, גביית תשלום עבור שירותים המסופקים על ידי מערכת

הסליקה, טיפול בתקלות חומרה ותוכנה וטיפול בפניות איכות מידע המופנות אל מערכת הסליקה.

.2.5.8.3 מוקדי השירות והתמיכה יתנו שירות, לכל הפחות, לאלה: (1) לקוחות (2) בעלי רישיון, (3) מעסיקים ומתפעלים, (4) גופים מוסדיים (5) גורמים נוספים שיתממשקו על המערכת, ככל ויהיו כאלה בהתאם להוראות הממונה (להלן - **המוקדים**).

.2.5.8.4 מערך השירות יכלול לכל הפחות את המוקדים הבאים:

מוקדים ללקוחות ומשתמשים:

.2.5.8.4.1 מערך תמיכה ושירות ללקוחות;

.2.5.8.4.2 מערך תמיכה ושירות לבעלי רישיון;

.2.5.8.4.3 מערך תמיכה ושירות למעסיקים;

.2.5.8.4.4 מערך תמיכה ושירות לגופים מוסדיים וגורמים אחרים;

.2.5.8.4.5 מערך תמיכה ושירות לסליקה כספית;

.2.5.8.4.6 מערך תמיכה ושירות למפתחים ומתכנתים.

.2.5.8.5 הספק יהיה רשאי להציע חלוקת מוקדים שונה מהמפורט לעיל, ולהביאה לאישור הממונה.

.2.5.8.6 מערך השירות והתמיכה יתמוך במתן שירות בערוצים הבאים: טלפון, דוא"ל, פנייה מפורטל האינטרנט ואפליקציית WhatsApp או אפליקציית תקשורת אחרת שתהיה מקובלת בשוק, ויהיה זמין להגשת פניות של לקוחות המערכת במשך 24 שעות ביממה, 365 ימים בשנה.

.2.5.8.7 מערך השירות יהווה נקודת קשר וריכוז לפניות הלקוחות. ככל שבוצעה פנייה מלקוח ישירות למי מעובדי מערכת הסליקה שלא באמצעות מערך התמיכה, היא תועבר למערך התמיכה לשם תיעוד וטיפול בה.

.2.5.8.8 הספק יפעיל מערכת ניהול פניות ממוחשבת לצורך הפעלת מערך השירות והתמיכה וכן מנגנוני שליטה ובקרה, אשר יאפשרו רישום וריכוז של כל הפניות מכל סוגי הלקוחות והמשתמשים במסד הנתונים של מערך השירות והתמיכה ותחזוקת בסיס ידע אירגוני לטיפול בפניות.

.2.5.8.9 כל פנייה לאחד ממוקדי מערך השירות והתמיכה תירשם במערכת ניהול הפניות, תסווג בהתאם לסוג הפנייה ויוקצה לה מספר מזהה ייחודי, אשר יימסר ללקוח או המשתמש הפונה מיד עם קבלת

פנייתו. המזהה של כל פנייה ילווה אותה לכל אורך הליך הטיפול בפנייה עד לסגירתה, וישמש את הספק והלקוח או המשתמש לאורך כל הטיפול בפנייה.

2.5.8.10. מערכת ניהול הפניות תתעד את תהליך הטיפול בפנייה בכל אחד ממוקדי מערך השירות והתמיכה משלב הפתיחה, דרך אבחון וסיווג הפנייה, מעקב אחר דרגי הטיפול השונים אצל הספק, דיווח לגורמים שונים אצל הספק והממונה, ככל ויידרש, ועד לסגירת הפנייה. מערכת ניהול הפניות תאפשר צפייה ועדכון כל הגורמים המעורבים במעגלי התמיכה השונים, וכן תאפשר פתיחת פניה ובירור מצב הטיפול בה מצד לקוחות המערכת ומשתמשיה.

2.5.8.11. יובהר בהתאם לאמור לעיל, כי ככל שהפנייה של לקוח או משתמש היא תקלה או פניית איכות מידע הנוגעת למספר לקוחות או משתמשים מאותו הסוג, או למספר סוגי לקוחות או משתמשים, סגירת הפנייה לא תיחשב כסגירת התקלה או סגירת פניית איכות המידע, אלא לאחר שהתקלה או פניית איכות המידע יטופלו באופן רוחבי ומלא לגבי כל הלקוחות או המשתתפים שאליהם היא נוגעת.

2.5.8.12. כמו כן, יובהר כי על הספק להתחבר למערכת בירור פניות הציבור שהוגשו לממונה וכי מערך השירות יתן מענה לפניות אלו באמצעות מערכת פניות הציבור שמפעילה הרשות ובכפוף להוראות חוזר גופים מוסדיים 2-9-2022 שעניינו "בירור ויישוב תביעות וטיפול בפניות ציבור" (2.1.22) כפי שישתנה מעת לעת ובשינויים המחוייבים.

2.5.8.13. מדדים לעניין טיפול בפניות ובתקלות הוגדרו בפרק 6 SLA.

2.5.8.14. הספק יקבע נוהל תמיכה וטיפול בפניות לקוחות ומשתמשים (להלן – **נוהל שירות ותמיכה**) במסגרת מערך שירות ותמיכה אשר יעודכן אחת לתקופה, ביוזמת הספק או בהתאם לדרישות הממונה. הנוהל יכלול התייחסות , בין היתר, לטיפול בתקלות ובפניות איכות מידע, אשר יוגש לממונה. הנוהל יכלול את אופן סיווג הפניות ואופן הטיפול בהן בכל אחד ממוקדי מערך השירות והתמיכה, בהתחשב באופי הפניות והתקלות שיכולות לעלות באותו מוקד.

2.5.8.15. הספק יערוך סקרי שביעות רצון ללקוחות ולמשתמשים במערכת שיתייחסו לכלל שירותי מערכת הסליקה, אשר יבוצעו על ידי הספק ועל חשבונו אחת לרבעון, באמצעות גורם המתמחה בעריכת סקרים. הסקרים, כאמור, יכללו מדגם מייצג של סוגי הלקוחות השונים. הספק יפעל לתיקון ליקויים שיתגלו כתוצאה מהסקרים כאמור ויפעל לשיפור השירות ללקוחות.

2.5.8.16. נוהל שירות ותמיכה יתייחס לאופן עריכת הסקרים (על ידי שיחות טלפוניות ו/או הודעות סמס), לרבות אופן קביעת הניקוד לסקרים, תדירות ביצוע, סוגי הפניות שייסקרו וכו' הערוצים שבאמצעותם יינתן השירות וכו'. יובהר, כי הספק יישא בכלל העלויות הקשורות לגורם המתמחה בעריכת סקרים אלה.

2.5.8.17. הספק ידווח באמצעות הפורטל הייעודי לרשות את תוצאות הסקר, לרבות הפעולות לתיקון הליקויים.

2.5.8.18. <u>אופן ניהול מוקדי התמיכה והשירות:</u>

2.5.8.18.1. הספק יקים ויתפעל את מערך המוקדים, הכולל מענה אנושי לטיפול בפניות לקוחות. כל מוקד יכלול צוות קבוע של אנשי תמיכה מקצועיים.

2.5.8.18.2. השירות יכלול מתן תמיכה אפליקטיבית, לזיהוי ואפיון תקלות ופניות, ומתן תמיכה מרחוק; צוות המוקד יאויש בהתאם לצרכי כל מוקד לפי העניין על מנת לתת שירות ותמיכה יעילים אשר יבטיחו עמידה במדדי השירות כמפורט בפרק 6 SLA.

2.5.8.18.3. המוקד יענה לפניות על ידי נציג אנושי, לכל הפחות, בשעות העבודה המקובלות, בימים א'-ה' בשעות 08:30-17:00. הגשת פנייה לאחר שעות העבודה המקובלות שלעיל תתאפשר באמצעים אוטומטיים בלבד, תיחשב כהגשת פנייה לכל דבר ועניין ותחילת הטיפול בה יחל ביום העסקים הבא. על אף האמור לעיל, על הספק לוודא קיומו של גורם מקצועי מטעמו אשר יהיה זמין לקבלת דיווח ולטיפול בנוגע לנושאים דחופים, כגון תקלה משביתה, בשעות שאינן שעות העובדה באופן שיאפשר טיפול מידי.

2.5.8.18.4. המוקד ייתן מענה לפניית הלקוח במהירות האפשרית ויפעל לטיפול רצוף בתקלה עד להשלמת הטיפול בה, בכפוף לזמני הטיפול בתקלות, לפי חומרת התקלה, כמפורט בפרק 6 SLA.

2.5.8.18.5. הספק ינתח באופן שוטף את פניות הלקוחות למוקד ואת תהליכי הטיפול בהן במטרה לזהות מגמות, תקלות חוזרות או כשלים בתפקוד המוקד, וינקוט בפעולות מתקנות יזומות למניעת תקלות חוזרות ולשיפור תפקוד המוקד.

2.5.8.18.6. עובדי המוקד יעברו הדרכות והכשרות תקופתיות מתאימות, וזאת על מנת לספק מענה מתאים, יעיל ומקצועי לפניות למוקד.

2.5.8.19. <u>מערך תמיכה אחורי (back office) לסליקה כספית וגבייה</u>

2.5.8.19.1. מערך התמיכה האחורי יטפל בפניות לקוחות המערכת בנושא בירורים בנוגע לסליקת כספים וגבייה.

2.5.8.19.2. מערך התמיכה האחורי יתמוך באופן מלא בכל שלבי תהליך סליקת הכספים והגבייה, ויהווה הגורם המקשר בין מערכת הסליקה לבין הגוף הסולק, תאגידים בנקאיים, גופים מוסדיים ולקוחות אחרים.

2.5.8.20. <u>מערך תמיכה למתכנתים ולמפתחים</u>

המערך יספק תמיכה טכנית למתכנתים ולמפתחים מטעם משתמשי המערכת בכל הקשור להעברת מידע וביצוע פעולות באמצעות מערכת הסליקה, בפרט התממשקות עם מערכת הסליקה בטכנולוגיית כספות או API, תמיכה בסביבת ניסוי ואינטגרציה, הנפקת סרטיפיקטים וכו'.

2.5.9. **<u>תיעוד הפעילות</u>**

2.5.9.1. <u>אחריות כוללת לתיעוד</u>

הספק יישא באחריות ובעלויות להפקת התיעוד מהמערכת. הספק אחראי לעדכון שוטף של התיעוד בכל עת, ובפרט לאחר הפעלת שלבים נוספים בתכנית העבודה או ביצוע שינויים בפעילות המערכת. יובהר כי הספק לא יהיה זכאי לתמורה נוספת בגין התיעוד.

2.5.9.2. <u>עריכת התיעוד</u>

2.5.9.2.1. התיעוד יהיה ערוך בצורה מסודרת ובהירה מבחינה גרפית, תוך ניצול עזרים גרפיים מתקדמים על מנת להקל על עין הקורא ועל הבנת התכנים.

2.5.9.2.2. התיעוד ייערך בהתאם לסטנדרטים מקובלים, ובכפוף להוראות רלוונטיות לנושא המתועד.

2.5.9.2.3. שפת התיעוד תהיה עברית, לפחות.

2.5.9.2.4. התיעוד יסופק בפורמט Word, Excel או PDF לפי העניין, ובעקוב אחר שינויים ממהדורות קודמות.

2.5.9.3. התיעוד ייעשה באופן שוטף, כך שהמהדורות הקודמות והשינויים יתועדו והמסמכים יופיעו בנוסח המלא והמעודכן ביותר. שינויים יופיעו על המסמך האחרון.

2.5.9.4. <u>תיעוד טכנולוגי של המערכת</u>

2.5.9.4.1. התיעוד של המערכת במתכונת מקובלת, ובכלל זה המערכת במבט-על, הגדרת מושגים, תיאור ישויות, תהליכים, זרימת מידע, סכימה לוגית, מבנה נתונים וכו' ;

2.5.9.4.2. כלל הפעילות המתבצעת במערכת, לרבות LOG אירועים מרכזיים של המערכת, הממשקים, הפעולות, השירותים וכו' ;

2.5.9.4.3. היסטורית עלייה והורדה של המערכת, חיבורים חדשים למערכות חיצוניות, ניסיונות פריצה\אירועי אבטחה וכו' ;

2.5.9.4.4. במקרה של העלאת גרסאות חדשות במערכת, תיעוד באופן שניתן להתחקות אחר המצב טרם העלאת הגרסה ולאחריה, והתרשמות מהשינויים והשיפורים במערכת ;

2.5.9.4.5. התיעוד יכלול כל התייחסות נוספת שתידרש על ידי הממונה.

2.5.9.5. <u>תיעוד מקצועי של המערכת</u>

הספק יערוך וישמור תיעוד מפורט ומלא של הנושאים הבאים לפחות ולמשך כל תקופת ההתקשרות :

2.5.9.5.1. תכנית העבודה ;

2.5.9.5.2. תיק אפיון מפורט, לרבות תהליכים, ממשקים, הפעולות המבוצעות במערכת הסליקה וכו' ;

2.5.9.5.3. תיק עיצוב, לרבות ארכיטקטורה, בסיס הנתונים, מסכים, דוחות וכדומה ;

2.5.9.5.4. תיק פריסת המערכת (תכנון מפורט של פריסת רכיבי המערכת ושל תשתיות סביבתיות וכדומה) ;

2.5.9.5.5. תכניות בדיקה ותיקי תפעול, לרבות נהלי תפעול למרכיבי תשתית, נהלי גיבוי, נהלי התאוששות מתקלות ואסון, תכנית ניהול סיכונים, נהלים לשדרוג עמדות עבודה ומרכיבי תשתית וכדומה ;

2.5.9.5.6. תיקי תחזוקה, לרבות הוראות תחזוקת תכנה, חומרה, תקשורת וכדומה, רשימת שינויים ושיפורים שבוצעו ושינויים ושיפורים שנתבקשו מהספק ומצב הטיפול בהם, וכן רשימת תקלות ומצב הטיפול בהן ;

2.5.9.5.7. תיק אבטחה, לרבות נוהל אבטחת נתונים, נוהל מתן הרשאות, נוהל אבטחה פיזית וכדומה ;

2.5.9.5.8. פרוטוקולים וסיכומי דיונים של ישיבות המנהלת וכן של ישיבות אחרות עם נציגי הממונה ;

2.5.9.5.9. תיעוד של כלל הפעילות של הלקוח או המשתמש לרבות בקשות שהוגשו וסטטוס הטיפול בהן, היזון חוזר, מסמכים שהועלו על ידם וכדומה והכל בכפוף לכל דין;

2.5.9.5.10. עדכוני גרסאות טכנולוגיים אשר משפיעים על פעילות הלקוח או המשתמש מול המערכת;

2.5.9.5.11. נהלי עבודה של מערכת הסליקה מול הלקוח והמשתמשים בנושאים השונים ובכלל זה נהלים המתייחסים להתחברות למערכת;

2.5.9.5.12. מסמכים כלליים לכלל הלקוחות, לרבות נהלי אבטחת מידע והגנת פרטיות, מדריכים ללקוחות ולמשתמשים וכללי המערכת.

2.5.10. **<u>שירותים נלווים שיינתנו על ידי הספק הזוכה</u>**

2.5.10.1. <u>שירותי הדרכה והטמעה</u>

2.5.10.1.1. הספק הזוכה יקים מערך הדרכה מתאים, הכולל תוכניות הדרכה מפורטות ומדריכים מקצועיים לשימוש במערכת הן ללקוחות ולמשתמשים חדשים והן ללקוחות ומשתמשים קיימים הנדרשים מעת לעת להדרכות נוספות.

2.5.10.1.2. הספק יכשיר את אנשיו לרמת מומחיות גבוהה בעבודה עם המערכת, ויעמיד לרשות הלקוחות והמשתמשים מומחים לטובת סיוע בכל הנדרש לשם שימוש והכרה של מערכת הסליקה על שירותיה והן לצורך חיבור מערכת הסליקה למערכות הלקוחות והמשתמשים.

2.5.10.1.3. הספק ייתן למשתמשים שירותי הדרכה והטמעה בפרט החל ממועד תחילת המעבר לטכנולוגיית API. על הספק יהיה לסייע ביישום והטמעת השינויים אצל הלקוחות והמשתמשים.

2.5.10.1.4. הספק יערוך תכנית הכשרה מקיפה לכל סוגי המשתמשים במערכת הסליקה, אשר תוגש לאישורו של הממונה. תכנית ההכשרה תתחשב באוכלוסיות השונות של המשתמשים והגורמים האחרים, ובשלבי תכנית העבודה. תכנית ההכשרה תוכל להתבצע בקבוצות של משתמשים בעלי מאפיינים דומים.

2.5.10.1.5. יובהר כי תכנית ההכשרה תתייחס למשתמשים וגורמים אחרים (אין צורך בתכנית הכשרה ללקוחות).

2.5.10.1.6. הספק יפרסם בפורטל האינטרנט עבור לקוחות ומשתמשי המערכת, בהתאמה לפי סוגים, מצגות סרטוני הדגמה והדרכה והסבר כתוב על אופן השימוש במערכת וסוגי השירותים השונים. המצגות, סרטונים וההסברים הכתובים ייערכו בשפה פשוטה, בהירה ומובנת, ויהיו זמינים להצגה או להורדה

באמצעות תוכנות מקובלות לכל אורך תקופת ההתקשרות. המסמכים יעודכנו על פי צורך על ידי הספק ודרישות הרשות.

2.5.10.1.7. **<u>כללים הנוגעים למדריכים הכתובים ללקוחות ומשתמשי המערכת:</u>**

א. שפת המדריך תהיה עברית וערבית לכל הפחות.

ב. המדריך יהיה קריא, בהיר וכתוב בשפה פשוטה, תוך שימוש בעזרים גרפיים ומתן דוגמאות, על מנת שלקוחות ומשתמשים ברמות שונות ובעלי רקעים שונים יוכלו להבין את החומר כראוי.

2.5.11. <u>הרחבות ושינויים לבקשת המזמין</u>

2.5.11.1. המזמין רשאי לדרוש מהספק להרחיב את סל השירותים, סוג המוצרים שלגביהם ניתנים השירותים וסוג הלקוחות שלהם יסופקו השירותים, במהלך תקופת ההתקשרות בהתאם להוראות הדין, במתכונת שתיקבע על ידי הממונה ובהתאם ליכולתו של הספק סביר לספק את השירותים. במידת הצורך, יקבע הממונה תעריף עבור שירות חדש, אשר יתווסף למחירון הסופי.

2.5.11.2. הספק יעמיד צוות, ברמה שאינה נופלת מרמתו של צוות הפיתוח וניהול הפרויקט המשמש למתן השירותים בהתאם לתכנית העבודה לפי מכרז זה, לצורך שיפורים או שדרוגים במערכת ופיתוחים חדשים מעבר לפיתוחים הנדרשים לשם יישום מכרז זה (כגון שירות/מוצר/לקוח חדש) (להלן – **שירותי שדרוג**), על חשבונו וללא כל תמורה נוספת לאמור בפרק 7 מודל התמור.

2.5.11.3. היקף השעות הנדרש מצוות הספק לצורך שירותי השדרוג יעמוד על 4,000 שעות עבור כל 12 חודשים קלנדריים במהלך תקופת ההתקשרות (לרבות בתקופות האופציה). שעות שלא נוצלו במסגרת שירותי השדרוג ייצברו משנה לשנה ללא הגבלה עד תום תקופת ההתקשרות. בנוסף המזמין יהיה רשאי להגדיל את כמות שעות הפיתוח בשנה מסוימת על חשבון שנה אחרת. יודגש כי שעות שירותי שדרוג אלה לא ישמשו לצורך יישום של כל שירות שנכלל במסגרת השירותים המוגדרים לפי מכרז זה, ובכלל זה התאמה של התשתית הטכנולוגית של מערכת הסליקה להוראות הממונה, שמירה על העדכניות הטכנולוגית, תיקון תקלות, פגמים או שגיאות במערכת וכו'. לעניין זה זכות ההכרעה בנוגע להגדרת שירות שדרוג במובחן מהתאמת התשתית הטכנולוגית שמורה לממונה.

2.5.12. <u>שירותי אינטגרציה (סביבת ניסוי)</u>

הספק יספק שירותי אינטגרציה בהתאם לקבוע בסעיף 3.16.5 להלן.

פרק 3 – טכנולוגיה

3.1. רקע

הספק נדרש להבטיח את המשך הפעילות התקינה של מערכת הסליקה בתצורתה הנוכחית, תוך שמירה על תמיכה מלאה בשירותים הקיימים המבוססים על טכנולוגית העברת קבצים באמצעות כספות ובמבנה המוגדר על פי הרשות. במקביל, הספק נדרש להיערך ולתמוך באופן מדורג במעבר לטכנולוגיה מתקדמת מבוססת API ופיתוח ותפעול כלל השירותים המפורטים בפרק 2 השירותים, בהתאם לתכנית העבודה והוראות הממונה.

על הספק לוודא שעד למעבר לטכנולוגית API, התשתית הקיימת לא צוברת "חוב טכנולוגי" ומתוחזקת בהתאם לנדרש במכרז זה וכן כי יתקיים מעבר חלק בין שתי הטכנולוגיות, אשר לא יפגע בביצועי המערכת.

הספק מתחייב לעמוד בכל התקנים הקבועים בפרק זה ולעדכן אותם בהתאם למקובל בשוק כפי שיהיה מעת לעת וכפי שיורה הממונה לעניין מועד העדכון כאמור.

3.2. עקרונות מרכזיים

3.2.1. **מעבר מדורג**: על הספק לתכנן תהליך מעבר מהמצב הקיים למצב עתידי באופן מבוקר והדרגתי, תוך מזעור סיכונים ושמירה על המשכיות תפעולית.

3.2.2. **עמידה ברגולציות**: על הספק להבטיח עמידה בדרישות רגולטוריות ובתקנים מקומיים ובינלאומיים, כולל התאמה לחוקי הגנת הפרטיות והוראות אבטחת מידע כמפורט בפרק 4 אבטחת המידע.

3.2.3. **אבטחה תחילה והגנת הפרטיות**: על הספק לתכנן את הפתרון מתוך גישה של הגנת הפרטיות (Privacy First) ואבטחה תחילה (Security First) כערך מרכזי, כולל מנגנוני הגנה מונעים ומנגנוני זיהוי מתקדמים.

3.2.4. **עקרון ההפרדה**: על הספק ליישם הפרדה פיזית בין רכיבי המערכת למערכות אחרות או ללקוחות נוספים של הספק ככל וקיימים, לשיפור האבטחה והביצועים.

3.2.5. **בחירת ספקי טכנולוגיה**: על הספק להשתמש בטכנולוגיות ובמוצרים של ספקים מוכרים ובעלי מוניטין, המתאפיינים בוותק, חוסן ותמיכת קהילה רחבה.

3.2.6. **יכולת התרחבות וגמישות**: על הספק לתכנן מערכת שיכולה לגדול ולהתאים עצמה לדרישות ולשינויים לרבות ממשקים נוספים ועדכונים טכנולוגיים מהותיים.

3.2.7. **תפעוליות הדדית (אינטרופרביליות)**: הספק נדרש להפשטה במימוש אינטגרציה ותקשורת חלקה בין מערכות וטכנולוגיות שונות.

3.2.8. **שלמות ודיוק נתונים**: על הספק ליישם שיטות ומנגנונים המבטיחים את שלמות ודיוק הנתונים ומספקים איכות ואמינות גבוהה של הנתונים.

3.2.9. **מודולריות**: הספק נדרש לבצע תכנון מודולרי הכולל הפרדה לרכיבים בלתי תלויים ברמת התשתית והקוד, להקלת תחזוקה ושדרוגים.

3.2.10. **פרוטוקולים**: על הספק לאמץ פרוטוקולים נפוצים וסטנדרטיים לתקשורת ולהחלפת מידע, להבטחת תאימות ואינטרופרביליות.

3.2.11. **תשתיות**: על הספק להשתמש בגישת "תשתיות כקוד" (Infrastructure as Code) לניהול תשתיות באופן מתועד, אוטומטי וחוזר.

3.2.12. **אוטומציה**: על הספק להטמיע אוטומציה בתהליכי DevOps ותפעול, לשיפור היעילות והפחתת טעויות אנוש לרבות DevSecOps לעניין תהליכי אבטחת מידע.

3.2.13. **בדיקות אוטומטיות**: על הספק לשלב בדיקות אוטומטיות בכל רכיבי המערכת, להבטחת יציבות ואיכות לאורך כל מחזור החיים של הפתרון.

3.2.14. **כתיבת קוד**: Clean Code, Clean Architecture- על הספק להשתמש במתודולוגיות מוכרות של קוד ותכנון ארכיטקטוני, להבטחת קריאות, תחזוקה ושימושיות של הקוד.

3.2.15. **מניעת נעילה לספק**: על הספק לנקוט אמצעים המונעים תלות מהותית בספקים או מוצרים צד ג' ספציפיים, לטובת גמישות עתידית.

3.2.16. **מוכנות לענן**: על הספק לתכנן מערכות באופן שיאפשר התאמה למודלים של ענן ציבורי, פרטי או היברידי.

3.2.17. **אופטימיזציה ביצועים**: על הספק להתמקד ביעילות ומהירות תגובה בעיצוב המערכת לשיפור חוויית המשתמש.

3.2.18. **זמינות גבוהה:** על הספק לתכנן פתרון המספק זמינות גבוהה עם מינימום זמני השבתה, לשמירה על רציפות עסקית ותכנון ויישום ארכיטקטורת חסינה לכישלון (Design to Fail), הכל בהתאם לסעיף 6.3.1. להלן.

3.2.19. **חוסן ושרידות**: על הספק לעצב את המערכת כך שתוכל להתמודד עם תקלות, שינויים פתאומיים ותנאים בלתי צפויים.

3.2.20. **חוויית משתמש**: על הספק לתכנן את המערכת כך שיהיה מיקוד בחוויית משתמש חדשנית ונגישה, המותאמת למגוון רחב של צרכים ויכולות.

3.2.21. **קיימות**: על הספק לשלב שיקולים ושיטות ידידותיים לסביבה בתכנון וביישום טכנולוגי.

3.2.22. **תיעוד והעברת ידע**: על הספק להבטיח תיעוד מקיף והדרכה לשימוש ותחזוקה יעילים של הטכנולוגיה.

3.3. ארכיטקטורה כללית

הספק יקים את המערך הטכנולוגי הדרוש לשם תפעול מערכת הסליקה, לרבות חומרה, תוכנה ותשתיות, בהתאם לדרישות פרק זה והמכרז בכללותו. המערך יוקם באתר קיים של הספק או באתר שיקים הספק לצורך הקמת המערכת בפריסה מקומית או בענן בכפוף להוראות פרק זה ולהנחיות פרק 4 אבטחת מידע בהקשר זה.

בהתאם לתכנית העבודה, הספק הזוכה יספק את השירותים הניתנים כיום על ידי מערכת הסליקה באמצעים טכנולוגיים כפי שמפורט בנספח מצב קיים המצורף כנספח ב.4 לחלק ב׳ במכרז זה.

3.4. אתר מערכת הסליקה

3.4.1. דרישות כלליות

3.4.1.1. כללי

הספק יקים שני חדרי מחשב נפרדים בתקן **Tier3** כל אחד, לפחות. חדרי המחשב ימוקמו במרחק של כ-40 ק״מ זה מזה לפחות, כאשר אחד מהם משמש כאתר הגיבוי המרוחק (**DRP**) כמפורט בפרק 4 אבטחת מידע במכרז זה. באתרים אלו תותקן המערכת.

הספק יבטיח שמקום הקמת המערכת יאפשר הפעלה של תשתיות מודרניות, מאובטחת ויעילה תפעולית. במענה, הספק יציע את האתר שבו הוא מתכוון להקים את המערכת, ענן ציבורי, פרטי או היברידי, או המשך שימוש במתקנים פיזיים משודרגים לפי הצורך.

ככל והספק בחר בתצורה מבוססת ענן, וסעיפי המשנה המפורטים בסעיף זה להלן אינם רלוונטיים, יציין הספק כי סעיף זה יבוצע על ידי ספק הענן, וספק המערכת מתחייב לוודא עמידה בתקנים נדרשים של ספק הענן.

התקנים המופעים בפרק זה הינם מחייבים, עם זאת, הספק יכול להציע תקן אחר הנותן כיסוי והבטחת איכות דומה.

3.4.1.2. תוכנית מעבר לאתר אחר

על הספק להציג תוכנית מפורטת למבנה האתרים לפי החלופה שיבחר לממש, הכוללת:

3.4.1.2.1. תוכנית למעבר מלא או חלקי לענן, תוך פירוט תצורת הפריסה וספקי הענן המוצעים.

3.4.1.2.2. תוכנית לתחזוקת התשתיות הפיזיות הקיימות או הקמת תשתיות פיזיות חדשות.

3.4.1.2.3. התוכנית תציג כיצד מובטחת מדרגיות, זמינות גבוהה ואבטחה פיזית של האתרים במהלך המעבר ואחריו.

3.4.1.3. תרשים מבנה

הספק הזוכה נדרש לספק תרשים מפורט של מבנה האתרים, הכולל את השינויים הצפויים ואת הטכנולוגיות המיועדות לשימוש.

3.4.1.4. מודל תחזוקה ותפעול

הספק הזוכה יציג מודל תחזוקה ברור, הכולל ניטור, בקרה וניהול סיכונים של אתר המחשב בין אם מדובר באתר פיזי או בספק ענן.

3.4.2. דרישות מבנה ותכנון פיזי

3.4.2.1. על המבנה לעמוד בדרישות התקן **ANSI/BICSI 002** או תקן מקביל, המספק הנחיות לתכנון ובנייה של מרכזי מחשוב.

3.4.2.2. הקירות, הרצפה והתקרה של חדר המחשב יהיו חסיני אש ברמת **Class A**, בהתאם לתקן **NFPA 75**.

3.4.2.3. רצפת החדר תהיה מוגבהת ותעמוד בדרישות התקן **ISO/IEC 22237**, כולל יכולת נשיאת עומס של לפחות 1500 ק״ג למ״ר. יש לכלול מיגון מפני רעידות אדמה במבנים הממוקמים באזורי סיכון, בהתאם לתקן **IBC 2018** (**International Building Code**) או תקן מקביל.

3.4.3. דרישות תשתית חשמל

תשתית החשמל תתוכנן ותותקן בהתאם לתקן **NFPA 70 National Electrical Code** או תקן מקביל, ותכלול מערכת הגנה מפני קצרים ותקלות.

יש להתקין מערכת גיבוי **UPS Uninterruptible Power Supply** המספקת תמיכה למינימום 30 דקות של פעילות רציפה בזמן הפסקת חשמל, בהתאם לתקן **IEC 62040**.

תכנון החשמל יכלול מנגנון יתירות **N+1** לפחות, לצורך שמירה על זמינות גבוהה בהתאם לדרישות **Tier III** של **Uptime Institute**.

מערכת הארקה תעמוד בדרישות התקן **IEEE 1100** ותספק הגנה מקסימלית מפני קפיצות מתח.

3.4.4. דרישות מיזוג אוויר ובקרת אקלים

3.4.4.1. מערכת המיזוג תעמוד בדרישת התקן **ASHRAE TC 9.9**.

3.4.4.2. יש להתקין מערכות קירור יתירות ברמת **N+1**, כולל מנגנוני **Failover** במקרה של כשל במערכת עיקרית.

3.4.4.3. יש לכלול מערכות קירור ייעודיות מסוג **In-row cooling** או **Hot/Cold aisle containment**, בהתאם להנחיות **EU Code of Conduct for Data Centres** לשיפור יעילות אנרגטית.

3.4.4.4. כל מערכות המיזוג ייבחנו לאמינות בזמן עומס חום קיצוני, כולל בדיקות תפקוד בתנאי כשל של מערכת אחת לפחות.

3.4.5. דרישות אבטחה פיזית

חדר המחשב יהיה מוגן בהתאם לתקן **ISO/IEC 27001** או תקן מקביל, עם דגש על הגנה פיזית מתקדמת.

יש להתקין מערכת בקרת גישה עם תיעוד מלא, הכוללת:

3.4.5.1. כרטיסי זיהוי מגנטיים.

3.4.5.2. זיהוי ביומטרי.

3.4.5.3. מערכת תיעוד גישה.

המתקן יכלול מצלמות אבטחה עם הקלטה רציפה למשך 90 יום לפחות.

המתקן יכלול חיישנים לזיהוי פריצה, רעידות, ותנועה לא מורשית במרחב החיצוני והפנימי של חדר המחשב.

כל הדלתות והפתחים לחדר המחשב יכללו מנגנוני נעילה אוטומטיים ואיטום מתקדם.

3.4.6. דרישות בטיחות וגיבוי

יש להתקין מערכות גילוי אש ועשן מתקדמות מסוג **VESDA** (**Very Early Smoke Detection Apparatus**), התואמות את התקן **NFPA 72**.

יש לכלול מערכת גיבוי אוטומטית לאספקת מים, חשמל, ומיזוג, שתאפשר פעילות תקינה למשך 72 שעות לפחות במקרה של כשל תשתיתי מלא.

תכנון הבטיחות יכלול יציאות חירום ברורות, מסומנות, ומאושרות.

3.4.7. דרישות יעילות אנרגטית

תכנון המבנה יבוצע בהתאם לתקן **ISO 50001** לניהול אנרגיה ויפעל להפחתת צריכת החשמל הכוללת.

מדדי ה- **Power Usage Effectiveness PUE** של המתקן לא יעלו על 1.5 בתנאי עומס מלא, עם עדיפות למתקנים בעלי **PUE** נמוך יותר.

יש להתקין מערכות ניטור אנרגיה מתקדמות המאפשרות בקרה בזמן אמת ושיפור מתמיד בצריכת האנרגיה.

3.4.8. בדיקות ואישורים

עם השלמת בניית האתרים בהתאם לפרק זה, הספק יידרש להציג תיעוד מלא של עמידה בדרישות התקנים המצוינים, כולל אישורי צד שלישי ממעבדות או גופים מורשים.

כל המערכות ייבדקו בצורה מלאה לפני הפעלה בייצור, ויופעלו מבחני עמידות בתנאים מדומים כדי להבטיח עמידה בדרישות.

על הספק להציג לוחות זמנים מדויקים לתחזוקה שוטפת, בדיקות תקופתיות, והחלפת רכיבים קריטיים.

3.5. רשת, תקשורת ופרוטוקולים

3.5.1. מבנה הרשת ותתי-רשתות

הספק נדרש לתכנן רשת מבודדת ומאובטחת הכוללת חלוקה לתתי-רשתות (**Subnets**) בהתאמה לתקני תעשייה מובילים, כגון **ISO/IEC 11801** לתשתיות רשת ותקשורת, ובכפוף לדרישות אבטחת המידע המפורטות בפרק 4 אבטחת מידע.

3.5.1.1. על הספק לתכנן ולהקים את הרשתות המוצעות להלן:

3.5.1.1.1. רשת פנימית: לשימוש רכיבי המערכת בלבד, ללא גישה חיצונית.

3.5.1.1.2. רשת לממשקים ממשלתיים: תאפשר גישה ישירה ומאובטחת למערכות ממשלתיות רלוונטיות.

3.5.1.1.3. רשת אינטגרציה: לצורך חיבור לקוחות ושותפים חיצוניים למערכת בממשקי **API**.

3.5.1.1.4. רשת דיגיטל: לצורך חשיפה של פורטל האינטרנט והפעלת אתרי מידע והכל כמפורט בפרק 2 השירותים.

3.5.1.1.5. רשת לשותפים וספקי צד ג': לצורך אינטגרציה עם שירותים ותשתיות חיצוניות .

הספק יוודא שתצורת הרשתות בייצור תשוקף גם בסביבות הנמוכות.

3.5.1.2. על הרשת להיבנות בתצורה שתתמוך בהתרחבות עתידית, הן בהיבטי קיבולת והן בהיבטי טכנולוגיה, תוך עמידה בהנחיות תקן **TIA-942** לתכנון מרכזי מחשוב.

3.5.1.3. כל פתרונות התקשורת שיוצעו יעמדו בסטנדרטים מוכרים בתעשייה ולא יגבילו שילוב עתידי של טכנולוגיות חדשות או הרחבות.

3.5.2. תקנים להקמת תשתית תקשורת פיזית

3.5.2.1. יש לתכנן את הרשת עם תמיכה בקצבי העברה מתקדמים של לפחות 100**Gbps**, תוך שמירה על תאימות לעדכוני תקן עתידיים, כגון תקני **IEEE 802.3** לסביבת **Ethernet**.

3.5.2.2. תשתיות הכבילה יעמדו בדרישות התקן **ISO/IEC 11801**. הכבילה תיבחר כך שתאפשר תמיכה בטכנולוגיות תקשורת מתקדמות, כגון סיבים אופטיים או טכנולוגיות מקבילות התואמות לתקני התעשייה המובילים.

3.5.2.3. תכנון תשתית התקשורת יתבצע בהתאם לתקן **IEC 61754** להבטחת תאימות בחיבורים אופטיים, ויתמוך בשדרוג עתידי ללא צורך בהחלפת רכיבים קריטיים.

3.5.3. חלוקת תתי-רשתות (**Subnets**)

3.5.3.1. הרשת תכלול חלוקה לתתי-רשתות (**Subnets**) בהתאם לסטנדרטים המוכרים, תוך שמירה על הפרדה לוגית ופיזית בין תתי-הרשתות, כמתואר בפרק 4 אבטחת מידע.

3.5.3.2. תתי-הרשתות יתוכננו כך שיאפשרו בידוד אפליקטיבי, ניהול עומסים, ותמיכה בפרוטוקולים מתקדמים כגון **IPv6**.

3.5.3.3. כל תת-רשת תתמוך בשילוב עתידי של שירותים חדשים ובביצוע התאמות קלות לצרכים משתנים.

3.5.4. סטנדרטים וטכנולוגיות רשת

כל רכיבי הרשת יתמכו בפרוטוקולים תקניים לתעשייה, כגון:

3.5.4.1. **IEEE 802.1Q** לניהול **VLAN** והפרדה לוגית.

3.5.4.2. **BGP**, **OSPF** ו- **EIGRP** לניתוב דינמי ותמיכה ברשתות מבוזרות.

הספק יוכל להציע רשת המבוססת על טכנולוגיות **SDN Software-Defined Networking**, להבטחת גמישות בהקצאת משאבים ולניהול מרכזי. ראה פירוט בסעיף 3.5.9 להלן.

פתרונות החומרה יהיו מבוססים על טכנולוגיות מוכרות בשוק, מתוצרת ספקים בעלי מוניטין, עם יכולת שדרוג לתמיכה בקצבים גבוהים יותר ופרוטוקולים חדשים.

יש לתכנן את תשתית התקשורת כך שתתמוך בטכנולוגיות עתידיות כמו 802.3**bs** (**GbE**400) או גבוהות יותר.

3.5.5. יתירות וניהול תקלות

3.5.5.1. הספק יתקשר עם לפחות שני ספקי תקשורת מקומיים בלתי תלויים לצורך יתירות וזמינות גבוהה.

3.5.5.2. על הרשת לתמוך במנגנוני יתירות מלאים ברמת רכיבי החומרה והקישורים, בהתאם לתקן **Uptime Institute Tier III**.

3.5.5.3. מערכות הניטור והניהול של הרשת יאפשרו ניטור ביצועים בזמן אמת ותיעוד תקלות.

3.5.6. בדיקות ואישורים

3.5.6.1. עם השלמת בניית תשתית התקשורת בהתאם לסעיף זה, על הספק להמציא אישור עמידה בתקנים המפורטים לעיל מרשויות או גופים מוסמכים, וכן לספק דוחות בדיקה של צד שלישי המאשרים את איכות והיתכנות פתרון הרשת.

3.5.6.2. בדיקות חדירה ובדיקות עומס יבוצעו לאחר ההקמה, תוך שמירה על התאמה לדרישות המפורטות בפרק 4 אבטחת מידע.

3.5.6.3. כחלק מבדיקות התוכנה כמפורט בתכנית העבודה, יבצע הספק דוח מסכם המפרט את כלל רכיבי הרשת, קצביהם, ותאימותם לדרישות המכרז ולתקנים הנדרשים.

3.5.6.4. הספק נדרש להבטיח זמינות רשת של 99.5% לפחות, תוך ניטור מתמיד של ביצועי התקשורת.

3.5.7. ניהול ותפעול עתידי

3.5.7.1. פתרונות הרשת יכללו תשתיות ניהול ותפעול גמישות, המאפשרות הרחבה ושדרוג ללא צורך בשינויים משמעותיים בתשתית הפיזית.

3.5.7.2. יש להבטיח התאמה מלאה של רכיבי הרשת לניהול מרכזי (**NMS**) ולמערכות ניטור ביצועים, כך שניתן יהיה לשלבם עם מערכות קיימות או עתידיות.

3.5.7.3. כל רכיבי החומרה והתוכנה יהיו בעלי תמיכה טכנית מעודכנת ותאימות להנחיות יצרן לפחות למשך 5 שנים מיום ההקמה.

3.5.8. פתרונות למיקרו-סגמנטציה (אופציונלי)

3.5.8.1. הספק רשאי ליישם מיקרו-סגמנטציה (**Micro-Segmentation**) לשיפור אבטחת הרשת והבידוד הלוגי בין תתי-רשתות (**Subnets**).

3.5.8.2. ככל והספק יבחר להציע פתרון מיקרו-סגמנטציה, עליו להבטיח תאימות לטכנולוגיות תקניות בתעשייה כגון **VMware NSX**, **Cisco ACI**, או פתרונות מקבילים בעלי מוניטין.

3.5.8.3. יישום המיקרו-סגמנטציה יהיה מבוסס על מדיניות אבטחת מידע המפורטת בפרק 4 אבטחת מידה ויתמוך בתעבורה מוצפנת, מניעת תנועה רוחבית (**Lateral Movement**), וניהול גמיש של הרשאות גישה.

3.5.8.4. הספק יידרש לוודא שהפתרון אינו מגביל שדרוגים או הרחבות עתידיות של תשתיות הרשת.

3.5.9. שימוש ברשת מוגדרת תוכנה (**SDN**) – אופציונלי

3.5.9.1. הספק רשאי להציע יישום טכנולוגיית **Software-Defined Networking (SDN)** לניהול דינמי וגמיש של תשתיות הרשת.

3.5.9.2. כל פתרון **SDN** שיוצע יתבסס על פרוטוקולים תקניים כגון **OpenFlow**, **NetConf**, או פתרונות תעשייתיים מוכרים, ויתמוך באינטגרציה עם מערכות קיימות.

3.5.9.3. אם ייבחר פתרון **SDN**, עליו לאפשר:

3.5.9.3.1. ניהול מרכזי של מדיניות רשת ותעבורה.

3.5.9.3.2. אוטומציה של הקצאת משאבים (**Resource Allocation**).

3.5.9.3.3. תמיכה בהתאמות לצרכים עסקיים משתנים ללא שינוי פיזי בתשתית הרשת.

3.5.9.4. הספק יבטיח שהפתרון יתמוך בשדרוגים עתידיים של קצבי תעבורה וטכנולוגיות מתקדמות, כגון **GbE**400 ויותר.

3.5.10. בדיקות והתאמות לפתרונות אופציונליים

3.5.10.1. במקרה של הצעת פתרונות מיקרו-סגמנטציה או **SDN**, על הספק לספק תיעוד מפורט של אופן הפעולה, התאמת הפתרון לתקנים המקובלים בתעשייה, ואופן האינטגרציה שלו עם הרשת המוצעת.

3.5.10.2. הפתרונות האופציונליים לא יפגעו בדרישות הבסיסיות של המכרז או בגמישות תשתיות הרשת להתפתחויות עתידיות.

3.5.10.3. בדיקות תאימות יתבצעו לאחר ההקמה, וכוללות בחינה של גמישות הניהול, הבידוד הלוגי, וביצועי הרשת תחת עומס.

3.6. מערכות הפעלה ווירטואליזציה

3.6.1. דרישות כלליות למערכות הפעלה ותשתיות

3.6.1.1. על הספק להציע תכנון והקמה של תשתית שרתים, בין אם באתר פיזי או בענן, בהתבסס על נוהגים מקצועיים מקובלים וסטנדרטים בתעשייה הפיננסית.

3.6.1.2. תשתית השרתים תיבנה עם מוכנות לשילוב עתידי בטכנולוגיות ענן, תוך שמירה על גמישות, מדרגיות ותאימות לשדרוגים עתידיים.

3.6.1.3. על הספק להבטיח שכל רכיבי התשתית, כולל חומרה ותוכנה, יתמכו בעדכוני גרסה שוטפים ותהיה להם תמיכה פעילה מצד היצרן.

3.6.2. בחירת מערכות הפעלה ותקני תשתית

3.6.2.1. מערכות ההפעלה שייבחרו על ידי הספק יעמדו בסטנדרטים מוכרים בתעשייה ויהיו **Certified** על ידי היצרנים ונתמכות לאורך זמן עם עדכוני גרסה שוטפים**.**

3.6.2.2. דוגמאות למערכות הפעלה מקובלות כוללות, אך לא מוגבלות ל:

3.6.2.2.1. **Red Hat Enterprise Linux (RHEL)**

3.6.2.2.2. **Ubuntu Server (LTS versions)**

3.6.2.2.3. **SUSE Linux Enterprise Server**

3.6.2.3. על מערכות ההפעלה לעמוד בכל דרישות התאימות ואבטחת המידע כפי שמפורט בפרק 4 אבטחת מידע.

3.6.3. תחזוקה ושדרוגים

על הספק להציע תוכנית תחזוקה למערכות ההפעלה והחומרה הכוללת:

3.6.3.1. התקנה של עדכונים ותיקוני אבטחה באופן שוטף.

3.6.3.2. ניטור ביצועים וזמינות של המערכות.

3.6.3.3. שדרוגים מתוכננים לציוד החומרה ומערכות ההפעלה בהתאם להנחיות היצרנים.

3.6.4. תאימות לפלטפורמות וירטואליזציה

3.6.4.1. על התשתית לתמוך בטכנולוגיות וירטואליזציה מקובלות בתעשייה, כגון **VMware, KVM**, או **Hyper-V**, בהתאם לצרכים התפעוליים של המערכת.

3.6.4.2. על הספק להבטיח קשר ישיר ותאימות מלאה בין תשתיות הווירטואליזציה לבין מערכות ההפעלה, כך שיובטח תפקוד תקין גם לאחר שדרוגים עתידיים.

3.6.5. זמינות ותאימות לגרסאות

3.6.5.1. מערכות ההפעלה שיוצעו יפעלו על גרסאות עדכניות בלבד, הנתמכות לאורך זמן על ידי היצרנים.

3.6.5.2. על הספק לוודא שמערכות ההפעלה יישארו מעודכנות לכל היותר תוך שנתיים ממועד יציאת גרסה חדשה, בהתאם להמלצות היצרן.

3.6.6. פתרונות קונטיינרים (אופציונלי)

3.6.6.1. ככל והספק בוחר להציע פתרונות מבוססי קונטיינרים, עליהם לכלול פתרונות לניהול סביבות מבוזרות המבוססים על סטנדרטים מוכרים בתעשייה (לדוגמה: **Kubernetes, OpenShift**).

3.6.6.2. פתרונות קונטיינרים, ככל יוצעו, יעמדו בדרישות אבטחת המידע המפורטות בפרק 4 אבטחת מידע.

3.6.7. ביצועים ויכולת מדרגיות

3.6.7.1. התשתית שתוצע על ידי הספק תעמוד בדרישות עומס נוכחיות ותתמוך בגידול שנתי של לפחות 35% בעומסים לאורך חיי המערכת.

3.6.7.2. הספק ינהל ניטור בזמן אמת על מדדים כמותיים להערכת ביצועי המערכת, כגון:

3.6.7.2.1. זמן תגובה ממוצע (**Response Time**).

3.6.7.2.2. ניצול משאבים (**CPU**, זיכרון, **IOPS**).

3.6.7.3. תכנון התשתית יאפשר הרחבה פשוטה של משאבים (**Scaling**), הן אופקית (**Horizontal Scaling**) והן אנכית (**Vertical Scaling**).

3.6.8. דרישות סביבתיות ואנרגטיות

התשתית תיבנה תוך עמידה בסטנדרטים מובילים של יעילות אנרגטית, כגון **Energy Star for Servers** או תקן מקביל.

3.7. מאגרי מידע, אחסון ובסיסי נתונים

3.7.1. עקרונות כלליים

3.7.1.1. בסעיף זה, יפורטו הדרישות לגבי האמצעים הטכנולוגיים למימוש הדרישות הפונקציונליות המבוקשות.

3.7.1.2. פתרון האחסון יתמוך במגוון סוגי נתונים, לרבות נתונים מובנים, מובנים למחצה, נתונים לא מובנים, נתוני ארכיון ולוגים, ואימג׳ים לצורכי פריסה, תוך הבטחת זמינות גבוהה ויכולת מדרגית.

3.7.1.3. פתרון האחסון יותאם לאופי הנתונים, לדרישות הביצועים, ולמאפיינים השונים של המידע, בהתאם לסטנדרטים מקצועיים מוכרים.

3.7.2. תכנון מערכות האחסון

3.7.2.1. מערכות האחסון יתוכננו כך שיתמכו בשכבות אחסון (**Storage Tiers**) על פי הצרכים:

3.7.2.1.1. אחסון מהיר עבור מידע קריטי הנדרש לעיבוד בזמן אמת או לגישה תדירה.

3.7.2.1.2. אחסון בינוני עבור מידע הנדרש לעיתים קרובות, שאינו דורש ביצועים מקסימליים.

3.7.2.1.3. אחסון ארכיון עבור מידע שהגישה אליו אינה שכיחה, הכולל נתוני לוגים וגיבויים.

3.7.2.2. סוגי פתרונות האחסון ייבחרו בהתאם לדרישות העסקיות, תוך שימוש בטכנולוגיות מקובלות בתעשייה כגון אחסון מבוסס **Flash** עבור ביצועים גבוהים ואחסון מבוזר או מבוסס ענן עבור מידע ארכיב.

3.7.3. דרישות לתכונות אחסון

3.7.3.1. על פתרון האחסון לכלול ניהול מחזור חיי נתונים (**Data Lifecycle Management**) באופן המאפשר ניהול והזזה של נתונים בין שכבות אחסון לפי צורכי ביצועים ועלויות.

3.7.3.2. המערכת תבטיח זמינות נתונים ברמה של 99.5% לפחות, תוך שמירה על יתירות מלאה והגנה מפני אובדן נתונים, בהתאם לסטנדרטים מוכרים.

3.7.3.3. פתרון האחסון יהיה מדרגי (**Scalable**), הן ברמה האופקית והן ברמה האנכית, כך שיתמוך בגידול רציף של נפחי המידע.

3.7.3.4. אבטחת המידע באחסון תתבצע בהתאם לדרישות בפרק 4 אבטחת מידע, לרבות הצפנת נתונים וניהול הרשאות גישה.

3.7.3.5. טכנולוגיית הגיבוי תותאם לאופי המשאב המגובה, ותכלול מנגנונים המאפשרים שחזור מהיר וזמינות גבוהה של הנתונים המגובים.

3.7.4. ביצועים ומדדים לאיכות מערכות האחסון

3.7.4.1. על הספק להפעיל מערכות אחסון שיבטיחו ביצועים נדרשים תוך מדידה מבוססת של:

3.7.4.1.1. זמן תגובה ממוצע (**Latency**) בהתאם לדרישות הביצועים לכל שכבת אחסון.

3.7.4.1.2. מהירות קריאה וכתיבה (**IOPS**) בהתאם לסוג הנתונים והשימושים.

3.7.4.1.3. ניצול נפחי אחסון, כולל מדדים לתפוסה מרבית (**Utilization Rate**).

3.7.4.2. על הספק לכלול פתרונות המאפשרים ניטור רציף ודיווח על ביצועי מערכות האחסון.

3.7.5. פתרונות אחסון אפשריים

3.7.5.1. על הספק ליישם פתרונות אחסון מבוססי אתר פיזי (**On-Premise**), אחסון בענן, או שילוב היברידי, תוך עמידה בסטנדרטים מקובלים.

3.7.5.2. פתרונות האחסון יכללו תמיכה במערכות **NAS/SAN** לניהול נתונים מובנים, ובמערכות **Object Storage** לנתונים לא מובנים.

3.7.5.3. שילוב פתרונות היברידיים יתבצע באופן המאפשר אופטימיזציה של ביצועים וניהול עלויות.

3.7.6. ייעוד האחסון לפי סוג מידע

3.7.6.1. אחסון נתונים מבניים יתמוך במערכות רלציוניות מבוססות **SQL**, בהתאם לסטנדרטים מקצועיים מקובלים.

3.7.6.2. אחסון נתונים מובנים למחצה יתבצע באמצעות מערכות **NoSQL** או **Object Storage** מותאמות לגישה מהירה.

3.7.6.3. אחסון נתונים לא מובנים ייתמך באמצעות מערכות לניהול מסמכים ופתרונות **Object Storage**.

3.7.6.4. פתרונות ארכיון וגיבויים יתוכננו בקיבולת גבוהה ובעלות מופחתת, תוך התאמה לסטנדרטים בתעשייה.

3.7.6.5. פתרונות האחסון יתמכו בניהול ואחסון של אימג׳ים מערכתיים (**System Images**) וקבצי קונטיינרים (**Container Files**) לצורך פריסה ושחזור מערכות.

3.7.6.6. על הספק להבטיח:

3.7.6.6.1. זמינות גבוהה של האימג'ים והקבצים, כך שניתן יהיה לפרוס או לשחזר מערכות בזמן קצר, עם זמן השהיה מינימלי (**Low Latency**).

3.7.6.6.2. שימוש בטכנולוגיות אחסון התומכות בניהול משאבים מסוג זה, תוך התאמה לסטנדרטים מקובלים בתעשייה.

3.7.6.6.3. פתרונות גיבוי ושחזור מותאמים, הכוללים מנגנוני ניטור וניהול ביצועים.

3.7.7. שימוש באחסון מחוץ לחצרות הספק

ככל והספק מציע שימוש בפתרונות **Storage as a Service** (**SaaS**) מבוססי ענן, עליו לעמוד בדרישות הבאות:

3.7.7.1. המיקום הגיאוגרפי של מרכזי האחסון יהיה בהתאם לדרישות פרק 4 אבטחת מידע.

3.7.7.2. אמצעי הגנה על הנתונים, כולל הצפנה בתעבורה ובמנוחה, כפי שמוגדר בפרק 4 אבטחת מידע.

3.7.7.3. זמני השהיה (**Latency**) והתחייבות לרמת ביצועים (**SLA**) עבור גישה, אחסון, ושחזור מידע.

3.7.7.4. תהליכי גיבוי ושחזור המיועדים לשירותים חיצוניים, עם זמני שחזור מוגדרים מראש (**RTO/RPO**).

3.7.7.5. על הספק להבטיח כי השימוש בפתרונות אחסון מחוץ לחצרותיו יתמוך בשילוב עם פתרונות אחסון אחרים (**On-Premise** או היברידי) תוך התאמה לדרישות פונקציונליות.

3.7.8. רכיבי אחסון למערכות דיווח ואנליטיקה (אופציונלי)

3.7.8.1. הספק רשאי ליישם רכיבי אחסון ייעודיים למערכות דיווח ואנליטיקה, בהתאמה למאפיינים הטכנולוגיים הייחודיים של מערכות אלו.

3.7.8.2. פתרונות אחסון למערכות דיווח ואנליטיקה יעמדו בדרישות הבאות:

3.7.8.2.1. תמיכה בביצועים גבוהים במיוחד לגישה לנתונים (**High Throughput**), כולל גישה מקבילית למידע (**Parallel Access**).

3.7.8.2.2. פתרונות אחסון מבוססי **Flash** או טכנולוגיות מתקדמות אחרות, המותאמים למאגרי מידע אנליטיים.

3.7.8.2.3. גמישות בקנה מידה, עם יכולת לטפל בגידול בנפחי המידע ובהרחבת המערכות לאורך זמן.

3.7.8.2.4. במידה והספק מציע פתרונות משולבים למערכות תפעוליות ואנליטיות, עליו לפרט כיצד יתבצע הניהול ההיברידי של המשאבים, תוך הבטחת ביצועים וזמינות לכל סוג מערכת.

3.8. שירותי תווכה (MIDDLEWARE)

3.8.1. עקרונות כלליים

3.8.1.1. על הספק להציע פתרון תווכה המאפשר אינטגרציה מלאה בין רכיבי המערכת, תוך תמיכה בתהליכים סינכרוניים וא-סינכרוניים. הפתרון יבטיח עמידה בסטנדרטים בינלאומיים מוכרים לאינטגרציה, כגון תקני **ISO/IEC 19510** לניהול תהליכים עסקיים (**BPMN**) או **OASIS AMQP** לתקשורת הודעות מבוזרות.

3.8.1.2. שירותי התווכה יכללו כלים מובנים לניהול תהליכים, תזמון העברת נתונים, וניהול זרימת מידע בין מערכות פנימיות וחיצוניות. על הכלים לכלול:

3.8.1.3. יכולת לתמוך בניהול תהליכים מבוזרים באופן גמיש ומדרגי.

3.8.1.4. ממשקי ניטור ובקרה בזמן אמת למעקב אחר התקדמות התהליכים.

3.8.1.5. יכולת לטפל בשגיאות ולהפעיל מנגנוני **Retry** אוטומטיים.

3.8.1.6. הפתרון המוצע יותאם לתמיכה בעומסים משתנים ויכלול מנגנונים לניהול עומסים (**Load Balancing**). על הספק להבטיח שמערכת התווכה תעמוד בזמינות של 99.5% לפחות ותתמוך ביכולות מדרגיות (**Scalability**) לשילוב עתידי של רכיבי מערכת חדשים או הרחבת פעילויות קיימות.

3.8.1.7. הספק רשאי, לפי שיקול דעתו, לעשות שימוש בטכנולוגיות **Serverless** או פתרונות **SaaS** לצורך מימוש האינטגרציות, בכפוף לדרישות המפורטות בפרק 4 אבטחת מידע. פתרון זה יכלול מנגנוני ניטור והצפנה מתקדמים המבטיחים עמידה בדרישות רגולטוריות, כמו **GDPR** או **PCI DSS**, בהתאם לאופי המידע המטופל.

3.8.1.8. הפתרון המוצע יכלול, לרבות אך לא רק, את התכונות הבאות:

3.8.1.8.1. ניהול **API** מבוזר: מנגנון המאפשר יצירה, חשיפה וניהול של ממשקי **API**, עם מעקב אחר ביצועים וזמינות.

3.8.1.8.2. תמיכה בפרוטוקולים מאובטחים: כולל **HTTPS**, **SFTP**, **MQTT**, או **AMQP** להעברת נתונים מאובטחת.

3.8.1.8.3. יכולות אוטומציה ואורקסטרציה: תמיכה בניהול תהליכים באמצעות ממשקי משתמש גרפיים (**GUI**) או תהליכי **Workflow** מותאמים אישית.

3.8.2. ניהול קבצים (**File Transfer Management - FTM**)

3.8.2.1. על הספק להציע פתרון לניהול העברת קבצים מאובטח ומבוקר בין רכיבי המערכת הפנימיים ובין המערכת למערכות צד ג'. הפתרון יכלול יכולת לניהול מעקב מלא אחר העברות, תיעוד אירועים ושמירת לוגים לצרכי תחקור.

3.8.2.2. העברת הקבצים תתבצע באמצעות פרוטוקולים מאובטחים ומוכרים בתעשייה, כגון:

3.8.2.2.1. **SFTP (Secure File Transfer Protocol)**.

3.8.2.2.2. **FTPS (File Transfer Protocol Secure).**

3.8.2.2.3. **HTTP (Hypertext Transfer Protocol Secure)** .

הפרוטוקולים ייושמו תוך עמידה בדרישות הצפנה כמו **TLS 1.2** ומעלה.

3.8.2.3. על פתרון ניהול הקבצים לכלול כלים לניטור ובקרה בזמן אמת של העברות, עם יכולת:

3.8.2.3.1. לזהות שגיאות ולהפעיל מנגנוני **Retry** לניסיונות חוזרים אוטומטיים במקרה של כשל.

3.8.2.3.2. לשלוח התראות יזומות במקרה של כשל או עיכוב משמעותי בתהליך ההעברה.

3.8.2.4. המערכת תתמוך בתזמון אוטומטי של העברות קבצים, המבוסס על כללים מוגדרים מראש, כגון:

3.8.2.4.1. זמנים יומיים קבועים להעברת נתונים.

3.8.2.4.2. התניות ספציפיות המבוססות על הגעת קבצים ממערכת צד ג'.

3.8.2.5. פתרון ניהול הקבצים יתמוך במבני נתונים מגוונים, כולל:

3.8.2.5.1. **JSON**

3.8.2.5.2. **XML**

3.8.2.5.3. **CSV**

3.8.2.5.4. טקסט רגיל (**Plain Text**)

.3.8.2.5.5 **PDF**

.3.8.2.5.6 **PNG/JPEG**

פתרון זה יבטיח תאימות לממשקים פנימיים וחיצוניים תוך עמידה בסטנדרטים של אינטגרציה מוכרים.

.3.8.2.6 הספק רשאי להציע פתרון המאפשר עיבוד נתוני אצווה (**Batch Processing**) כתוספת לשיפור יעילות התהליכים. יישום פתרון זה, אם יבחר, יותאם לצרכים תפעוליים מוגדרים ולדרישות ביצועים.

.3.8.2.7 הפתרון המוצע יכלול, לרבות אך לא רק, את התכונות הבאות:

.3.8.2.7.1 מעקב זרימת עבודה (**File Flow Monitoring**): דשבורד המאפשר מעקב אחר סטטוס כל קובץ בתהליך ההעברה.

.3.8.2.7.2 ניהול תיעוד היסטורי: יכולת גישה להיסטוריית ההעברות עבור ניתוח ביצועים ותחקור.

.3.8.2.7.3 שילוב אופציונלי עם שירותי ענן: תמיכה בהעברות לשירותי אחסון ענן נפוצים (לדוגמה: **AWS S3, Azure Blob**).

.3.8.3 תיווך הודעות ותהליכים א-סינכרוניים

בהתאמה לדרישות למתן שירותים כפי שמפורט בפרק 2 השירותים, הספק יעשה שימוש בטכנולוגיות מודרניות לעיבוד מסרים והודעות א-סינכרוניים, לפי סטנדרטים מקובלים בתעשייה.

.3.8.3.1 על הספק להטמיע פתרון להעברת הודעות מבוזרות (**Message Bus**) לצורך תמיכה בתהליכים א-סינכרוניים. הפתרון יעמוד בתקנים מוכרים בתעשייה, כגון **AMQP (Advanced Message Queuing Protocol)** או **STOMP (Streaming Text Oriented Messaging Protocol)**, המבטיחים תקשורת אמינה בין רכיבי המערכת.

.3.8.3.2 המערכת תתמוך בהעברת הודעות בזמן אמת, תוך ניהול תורים בנפח גבוה ויכולת עמידה בעומסים משתנים. הפתרון יכלול מנגנוני ניהול תורים (**Queue Management**) המאפשרים:

.3.8.3.2.1 טיפול בהודעות רבות בו-זמנית (**Parallel Processing**).

.3.8.3.2.2 ניהול עדיפויות (**Priority Queues**) לטיפול בהודעות קריטיות תחילה.

.3.8.3.3 הפתרון יכלול מנגנוני חזרה אוטומטית (**Retry Mechanisms**) למקרים של כשל בתהליך. מנגנונים אלה יאפשרו:

3.8.3.3.1. הגדרה דינמית של זמני החזרה.

3.8.3.3.2. תיעוד וניהול שגיאות, עם אפשרות להתריע למנהל המערכת במקרה של כשל מתמשך.

3.8.3.4. הפתרון המוצע ע"י הספק יכלול, בין היתר אך לא רק, את התכונות להלן:

3.8.3.4.1. תמיכה ב-**Secure Messaging**: העברת הודעות מוצפנות בהתאם לתקנים מוכרים, כגון **TLS 1.2** ומעלה.

3.8.3.4.2. מעקב אחרי הודעות (**Message Traceability**): יכולת לנטר את המסלול המלא של כל הודעה, כולל זיהוי חד-ערכי (**Unique Identifier**), תיעוד זמן ההגעה, זמן העיבוד, ותוצאה.

3.8.3.4.3. אינטגרציה עם מערכות צד ג': תמיכה בפרוטוקולים כמו **HTTP**, **REST**, או **Webhooks** לצורך שילוב הודעות עם מערכות חיצוניות.

3.8.3.5. פתרון תיווך ההודעות יבטיח עמידה ברמת זמינות של 99.5% לפחות ויכלול יכולת התאוששות אוטומטית (**Self-Healing**) במקרה של כשל ברכיבי המערכת.

3.8.4. מערכות לניהול תהליכים ואורקסטרציה

3.8.4.1. על הספק ליישם פתרון לניהול תהליכים מורכבים, הכולל אוטומציה של זרימות עבודה, בהתאם לדרישות למתן שירותים כפי שמפורט בפרק 2 השירותים. תכנון הפתרון יתבצע תוך הפעלת שיקול דעת מקצועי, בהתבסס על סטנדרטים מקובלים בתעשייה כמו **BPMN (Business Process Model and Notation)** לניהול תהליכים עסקיים.

3.8.4.2. הספק רשאי, לפי שיקול דעתו, לעשות שימוש בטכנולוגיות **SaaS** לניהול תהליכים, בכפוף לדרישות אבטחת המידע המפורטות בפרק 4 אבטחת מידע.

3.8.4.3. בתכנון הפתרון, על הספק להבחין באופן מקצועי בין מקרים המתאימים ליישום גישת **Choreography** (ניהול תהליכים מבוזר), לבין מקרים בהם נדרש יישום גישת **Orchestration** (ניהול תהליכים מרכזי), או שילוב ביניהם להשגת פתרון אופטימלי לדרישות.

3.8.4.4. המערכת שתוצע תתמוך בניהול תהליכים באמצעות כלים ויזואליים לניהול ואוטומציה של זרימות עבודה, עם יכולות:

3.8.4.4.1. יצירת זרימות עבודה מותאמות אישית בהתאם לדרישות הפונקציונליות.

3.8.4.4.2. ניטור תהליכים בזמן אמת באמצעות דשבורד מרכזי.

3.8.4.4.3. ניתוח ביצועים ותחקור תהליכים באמצעות דו"חות מתקדמים (**Analytics**).

3.8.4.5. הפתרון המוצע ע"י הספק יכלול, בין היתר אך לא רק, את התכונות להלן:

3.8.4.5.1. ניהול תלות בין תהליכים (**Dependency Management**): מנגנון לניהול יחסים בין תהליכים מורכבים, כולל טיפול בתהליכים מקבילים ותלויים.

3.8.4.5.2. אינטגרציה עם מערכות חיצוניות: תמיכה בממשקי **API** מבוססי **REST** או **SOAP** לניהול תהליכים חוצי ארגון.

3.8.4.5.3. תמיכה בפריסה בענן ובאתר הלקוח: יכולת להתאים את ניהול התהליכים למבנה המערכת (**On-Premise** או **Cloud**).

3.8.4.6. המערכת תבטיח זמינות של 99.5% לפחות ותתמוך במדרגיות אופקית ואנכית, המאפשרת הרחבה או שדרוג של תהליכים קיימים ללא פגיעה בביצועים.

3.8.5. אינטגרציה עם מערכות חיצוניות

3.8.5.1. פתרון התווכה יאפשר חיבור למערכות חיצוניות באמצעות פרוטוקולים וסטנדרטים מוכרים, כולל:

3.8.5.1.1. **HTTP/HTTPS** - לתקשורת סינכרונית

3.8.5.1.2. **RESTful API**- לניהול ממשקי שירות אפליקטיביים

3.8.5.1.3. **SFTP** או **FTPS** -להעברת קבצים בצורה מאובטחת

3.8.5.1.4. **AMQP** או **Kafka**- לצורך העברת מסרים א-סינכרוניים בתקשורת מבוזרת

3.8.5.2. מבנה הנתונים הנתמך על ידי המערכת יכלול פורמטים מקובלים לתעשייה:

3.8.5.2.1. **JSON** לפשטות ושימוש נרחב בממשקי **API**

3.8.5.2.2. **XML** לשמירה על תאימות לאחור במערכות קיימות

3.8.5.2.3. **AVRO** או **Protobuf** להעברת מסרים בנפחים גבוהים וביעילות גבוהה

3.8.5.3. על הספק לוודא כי פתרון האינטגרציה יתמוך במנגנוני עקיבות (**traceability**), תוך מעקב אחר המסרים המועברים:

3.8.5.3.1. רישום ותיעוד של מקור, יעד, ותוצאות כל הודעה.

3.8.5.3.2. מנגנונים לניטור שגיאות ושליחת התראות יזומות.

3.8.5.3.3. זיהוי חד-ערכי (**Unique Identifier**) לכל מסר לצורך תחקור ותיעוד.

3.8.5.4. הפתרון יעמוד בדרישות למתן השירותים המפורטות בפרק 2 השירותים, תוך שיתוף פעולה עם הרשות לפיתוח תקנים מקומיים במקרה שאין תקנים בינלאומיים מתאימים לתחום הביטוח והחיסכון ארוך טווח. תקני התקשורת, המידע ואבטחת המידע עשויים להסתמך בין היתר על תקן ברלין וכל זאת כפי שייקבע בהוראות הממונה לעניין זה.

3.8.5.5. הספק יוכל להציע שימוש בטכנולוגיות **Serverless** או **SaaS** לצורך מימוש האינטגרציה יתבצע בכפוף לדרישות אבטחת המידע בפרק 4.

3.8.5.6. הפתרון המוצע יכלול, בין היתר אך לא רק:

3.8.5.6.1. יכולת לניהול עומסים (**Load Balancing**) לצורך תמיכה בתקשורת עם מערכות צד ג'.

3.8.5.6.2. מנגנוני גיבוי והתאוששות מהירה לשמירה על יציבות התקשורת בעת כשל.

3.8.5.6.3. תאימות עתידית להרחבת הפתרון בהתאם לצרכים עסקיים או טכנולוגיים עתידיים.

3.8.6. תשתיות למעבר נתונים מאובטח

3.8.6.1. <u>יישום פרוטוקולים מאובטחים</u>

על הספק לוודא שכל תהליך העברת נתונים יתבצע באמצעות פרוטוקולים מאובטחים ומוכרים. מימוש הטכנולוגיות יכלול:

3.8.6.1.1. שימוש ב-**SFTP** להעברת קבצים בצורה מאובטחת.

3.8.6.1.2. יישום **HTTPS** בתקשורת מבוססת **HTTP**, תוך תמיכה בגרסאות **TLS 1.2** ומעלה.

3.8.6.1.3. שימוש ב-**MQTT** עם **TLS** לתקשורת מבוזרת וב-**AMQP** עם **TLS** לניהול הודעות א-סינכרוניות.

.3.8.6.1.4 פרטים מלאים על דרישות ההצפנה והאבטחה מפורטים בפרק 4 אבטחת מידע.

.3.8.6.2 <u>תעודות דיגיטליות</u>

.3.8.6.2.1 התעודות הדיגיטליות ישמשו לאימות זהויות ולהבטחת שלמות הנתונים.

.3.8.6.2.2 על הספק ליישם מנגנון מבוסס **PKI (Public Key Infrastructure)** לניהול תעודות דיגיטליות לרבות חידוש, תיקוף וביטול עבור רכיבי המערכת והתקשורת ביניהם לרבות תקשורת עם רכיבים של גורמים אחרים. התעודות יאפשרו חיבור מאובטח ישיר לגופים המוסדיים או למערכת לפי העניין והכל בכפוף לסטנדרט ולהוראות הממונה בהקשר זה.

.3.8.6.2.3 מימוש הטכנולוגיה יכלול תמיכה בניהול תעודות באמצעות שירות **Certificate Authority (CA)**, כולל תמיכה ב-**Certificate Revocation List (CRL)** לניהול תעודות שבוטלו.

.3.8.6.2.4 תכנון וניהול מנגנון התעודות יתבצע בהתאמה להנחיות המפורטות בפרק "אבטחת מידע".

.3.8.6.3 <u>טוקנים לאימות ואבטחת ממשקים</u>

על הספק ליישם מנגנוני זיהוי ואימות באמצעות טוקנים, עם התמיכה הבאה:

.3.8.6.3.1 **JSON Web Tokens (JWT)** לניהול הרשאות ותהליכים סינכרוניים וא-סינכרוניים.

.3.8.6.3.2 **OAuth 2.0 Tokens** לאימות גישה מול מערכות צד ג'.

.3.8.6.3.3 שימוש במנגנוני **Bearer Tokens** להעברת הרשאות בתקשורת מאובטחת **(HTTPS)** בלבד.

.3.8.6.3.4 על הספק לוודא שייצור, ניהול, וביטול הטוקנים ייעשו בהתאם לדרישות המפורטות בפרק "אבטחת מידע".

.3.8.6.4 <u>הצפנת נתונים בתקשורת</u>

על הספק ליישם הצפנה לכל נתון בתעבורה בין רכיבי המערכת:

.3.8.6.4.1 שימוש בהצפנה א-סימטרית עבור תעודות וטוקנים **(Asymmetric Encryption)**.

3.8.6.4.2. הצפנת הנתונים בתעבורה באמצעות מנגנון **TLS 1.2** ומעלה.

3.8.6.4.3. ניהול מפתחות הצפנה מבוסס טכנולוגיות מתקדמות, כגון פתרונות **HSM (Hardware Security Module)**.

תכנון פתרון ההצפנה ייעשה תוך הפניה להנחיות המפורטות בפרק 4 אבטחת מידע.

3.8.7. מנגנוני **Traceability** למסרים והודעות

3.8.7.1. על הספק ליישם מנגנון עקיבות (**Traceability**) שיאפשר מעקב מלא אחר כל מסר או הודעה העוברים בין רכיבי המערכת ובין המערכת למערכות צד ג'. כל מסר או הודעה יתועדו עם מזהה חד-ערכי (**Unique Identifier**) שיאפשר תחקור המסלול המלא של ההודעה, כולל מקור, יעד, וזמני שליחה, קבלה ועיבוד.

3.8.7.2. המנגנון יכלול תיעוד מלא של המסרים, תוך שמירה על נתונים רלוונטיים כגון תוצאה (**Success/Failure**) לכל הודעה. תהליך זה יכלול רישום אוטומטי של פרטי השגיאה במקרה של כשל והפעלה של מנגנון אוטומטי לניסיונות חוזרים (**Retry**) בהתאם לכללים מוגדרים.

3.8.7.3. הספק יספק פתרון לניטור בזמן אמת של זרימת המסרים, עם מנגנוני התראה אוטומטיים במקרה של חריגות או כשלים, לדוגמה: הודעות שלא נמסרו ליעדן בזמן הנדרש או הודעות שחוו כשלים חוזרים.

3.8.7.4. פתרון ה-**Traceability** יכלול גישה לנתונים באמצעות ממשק ניהול גרפי (**Dashboard**), שיאפשר הצגה ברורה של סטטוס ההודעות, זרימת העבודה, וזיהוי בעיות. הממשק יאפשר גם ניתוח נתוני הביצועים ודוחות מותאמים לצרכים תפעוליים.

3.8.7.5. על פתרון העקיבות להיות מותאם לדרישות אבטחת המידע המפורטות בפרק 4 אבטחת מידע, לרבות הצפנת המידע המתועד ושמירת הלוגים בתנאים מאובטחים. פרקי זמן לשמירת לוגים ותנאי הגישה יוגדרו בהתאם להנחיות בפרק זה.

3.8.7.6. הפתרון יאפשר אינטגרציה עם מערכות ניטור ותחקור מרכזיות לצורך אחזור וניתוח נתונים. תיעוד המסרים יתמוך בדרישות הרגולציה המקומית, לרבות יכולת לספק נתונים לצרכים עסקיים או חקירתיים במועד הנדרש.

3.8.7.7. במידה ונעשה שימוש במערכות מבוזרות או צד שלישי לניהול הודעות, כגון **Kafka** או **RabbitMQ**, על הספק להבטיח שהמערכת תומכת בניהול עקיבות לפי עקרונות אלו, תוך שמירה על ביצועים גבוהים ותמיכה בנפחי עבודה משתנים.

3.9. שירותי שרתים (BACKEND FOR FRONTEND, BFF)

3.9.1. עקרונות כלליים

3.9.1.1. על הספק ליישם שכבת **BFF** שתפעל כמתווך בין ה-**Frontend** לשירותי ה-**API** של המערכת, תוך התאמה מלאה לדרישות הפונקציונליות.

3.9.1.2. יש לוודא שה-**BFF** מותאם להפרדת תהליכים לפי סוגי משתמשים (כגון: בעלי רישיון, חברות ביטוח, רשות שוק ההון) ולהפחתת עומסים על השירותים האפליקטיביים המרכזיים.

3.9.2. ניהול משתמשים וגישה

3.9.2.1. ה-**BFF** יתמוך במנגנון אימות זהות מאובטח (**Authentication**) ובניהול הרשאות מבוסס תפקידים (**Role-Based Access Control - RBAC**) בהתאם לפרק 4 אבטחת מידע.

3.9.2.2. על המערכת לכלול שירות לרישום משתמשים ותהליך אישור משתמשים לסביבת ניסוי (**Sandbox**).

3.9.3. שירותי נתונים מותאמים

3.9.3.1. על ה-**BFF** לנהל דחיפת נתונים יזומה למשתמשים באמצעות **Push Notifications** מבוססי **Webhooks** או **MQTT**.

3.9.3.2. ה-**BFF** יאפשר חיפוש וגישת נתונים מותאמים לפי פרופיל המשתמש, כולל מידע על כמות פניות, פעולות שבוצעו, ודוחות מותאמים אישית.

3.9.4. תמיכה בשחרורי גרסאות

3.9.4.1. ה-**BFF** יתמוך במנגנון ניהול גרסאות של ה-**API**, עם יכולת ניהול מקביל של גרסאות פעילות בייצור וגרסאות עתידיות (**Versioning**).

3.9.4.2. שירותי ה-**BFF** יכללו ניהול יומן פעילות לגרסאות ה-**API**, כולל תמיכה בשקיפות מול המשתמשים לגבי שיפורים ושינויים עתידיים.

3.9.5. אינטגרציה עם מערכות צד ג'

3.9.5.1. יש לוודא שה-**BFF** מתממשק בצורה מאובטחת עם מערכות צד ג', כגון פורטלים חיצוניים או שירותי צד שלישי.

3.9.5.2. על המערכת לתמוך במנגנוני ניטור עקיבות (**Traceability**) ואימות של מידע המגיע ממערכות צד ג'.

3.10. שכבת תצוגה וחווית משתמש

3.10.1. שכבת התצוגה אחראית על יצירת ממשקי משתמש אינטואיטיביים, נגישים וחדשניים, המאפשרים גישה חלקה לשירותי המערכת ולתכנים השונים כפי שנדרשים ומפורטים בפרק 2 השירותים. תכנון השכבה ייתן מענה לצרכים מגוונים של משתמשי קצה, כולל ממשקים רספונסיביים המותאמים למכשירים ניידים, מחשבים שולחניים וטאבלטים.

3.10.2. הממשקים יתמכו לכל הפחות, ברזולוציות מסך הבאות:

3.10.2.1. מחשבים שולחניים: רזולוציות של **1920x1080** פיקסלים ומעלה, עם תמיכה אחורנית ברזולוציות של **1366x768**.

3.10.2.2. טאבלטים: רזולוציות של **800X1280** ומעלה, לרבות פורמטים רוחביים ואנכיים.

3.10.2.3. מכשירים ניידים: רזולוציות של **360x640** ומעלה, עם תמיכה בפורמטים רוחביים ואנכיים.

3.10.2.4. הממשקים יתמכו בדפדפנים הנפוצים ביותר, כולל:

3.10.2.5. **Google Chrome** גרסאות עדכניות ועד 2 גרסאות אחורה.

3.10.2.6. **Mozilla Firefox** גרסאות עדכניות ועד 2 גרסאות אחורה.

3.10.2.7. **Microsoft Edge** גרסאות מבוססות (**Chromium**).

3.10.2.8. **Safari** גרסאות עדכניות במערכות **macOS** ו – **iOS**.

3.10.2.9. דפדפן מובנה במערכת **Android** (גרסאות נתמכות רשמית).

3.10.3. האתר יתוכנן להיות נגיש על פי דרישות הנגישות הקבועות בחקיקה במדינת ישראל, ובפרט עמידה בתקני **WCAG 2.1** ברמת **AA**.

3.10.4. על הספק להבטיח הפרדה מוחלטת בין רכיבי הגרפיקה לבין הפונקציונליות של האתר. עיצוב גרפי ושינויים במראה האתר יתבצעו באמצעות שימוש בקבצי גרפיקה **SVG** ו-**PNG** , ולא ידרשו שינויים בקוד הפונקציונלי.

3.10.5. השפה הגרפית של האתר תעשה שימוש בתבניות ובגרפיקה וקטורית סטנדרטית, תוך תמיכה בסטנדרטים כמו:

3.10.5.1. **SVG 1.1/2.0** לתצוגה וקטורית מותאמת רזולוציה.

3.10.5.2. קבצי **PNG** לשימושים נוספים במידת הצורך.

3.10.6. האתר יתוכנן על פי עקרונות פיתוח מערכות אינטרנט עדכניות, לרבות:

3.10.6.1. שימוש בתגיות **HTML5** תקניות ובסטנדרטים של **W3C**.

3.10.6.2. תמיכה מלאה ב-**CSS3** לעיצוב דינמי ואחיד.

3.10.6.3. תאימות מלאה ל-**ES6 (ECMAScript 6)** ומעלה לצורך פיתוח קוד **JavaScript** מודרני.

3.10.6.4. שימוש במסגרות פיתוח **Frontend** עדכניות כגון **React**, **Vue.js**, או **Angular**, לפי בחירת הספק.

3.10.6.5. עמידה בעקרונות **PWA (Progressive Web Applications)** לצורך יצירת חוויה דמויית אפליקציה במכשירים ניידים.

3.10.7. על האתר לתמוך בתשתיות ניהול תוכן ותצוגה מותאמת אישית תוך יישום מנגנוני התאמה לפי פרופיל המשתמש.

3.10.8. הממשקים יתמכו באבטחת מידע מתקדמת ובשמירה על מידע רגיש בהתאם להנחיות המפורטות בפרק 4 אבטחת מידע.

3.11. תחקור נתונים, דוחות ואנליטיקה

3.11.1. עקרונות כלליים

3.11.1.1. שכבת הנתונים והאנליטיקה במערכת תספק פתרון לניהול, עיבוד וניתוח נתונים בקנה מידה גדול, תוך דגש על יצירת תובנות עסקיות, תמיכה בהחלטות תפעוליות, אופטימיזציה של עלויות, וניהול אבטחת מידע.

3.11.1.2. על הספק להבטיח שהמידע הנאסף והמעובד לא יכלול מידע פרטי ואישי של לקוחות. נתונים רגישים יעברו תהליך התממה (**Anonymization**) בהתאם להנחיות הממונה על הגנת הפרטיות ואבטחת המידע.

3.11.1.3. הספק רשאי להשתמש בפתרונות צד ג' **SaaS** כגון **Snowflake**, **Databricks**, או פתרונות דומים, בכפוף לדרישות בפרק 4 אבטחת מידע.

3.11.2. תובנות עסקיות וניהול תפעולי

3.11.2.1. המערכת תספק תשתית ליצירת דוחות ניתוח ומעקב אחר ביצועי המערכת, כולל:

3.11.2.1.1. ניתוח מגמות ושיפורים לשיפור חוויית המשתמש ולמעקב אחר השימוש בשירותים.

3.11.2.1.2. כלים לניהול ותפעול תשתיות, כולל ניטור ביצועים, זיהוי צווארי בקבוק והפקת המלצות לשיפור ביצועים.

3.11.2.1.3. פתרונות לניהול עלויות תשתית (**FinOps**), כולל ניתוח צריכת משאבים, חיזוי עלויות, ואופטימיזציה תקציבית.

3.11.2.1.4. יובהר כי לא יתבצע עיבוד משנה (**Sub processing**) למידע אישי בלי אישור (רגולטורי) מפורש.

3.11.3. ניהול מונטיזציה של מידע

3.11.3.1. המערכת תכלול כלים לניהול מונטיזציה של המידע (**Data Monetization**), אשר יאפשרו:

3.11.3.1.1. זיהוי ערך עסקי מתוך המידע הזמין והגדרת מודלים להכנסות מבוססות נתונים.

3.11.3.1.2. אינטגרציה עם כלי **BI** מתקדמים לצורך חישוב הערך הפיננסי של המידע.

3.11.3.1.3. ניהול הרשאות מבוסס תפקידים לצורך שיתוף מידע בין שותפים עסקיים בצורה מבוקרת ומאובטחת.

3.11.4. תצוגות ודוחות מותאמים

3.11.4.1. המערכת תתמוך ביצירת דוחות ותצוגות מותאמות אישית למשתמשים שונים, כולל בעלי רישיון, לקוחות קצה, גופים מוסדיים, הרגולטור ומערכות צד ג'.

3.11.4.2. מפרט הדוחות ודרישות התצוגה הנדרשת כפי שמפורטים בפרק 5 המימוש.

3.11.4.3. הדוחות יתמכו בפורמטים סטנדרטיים לייצוא נתונים, כגון **AVRO, Parquet, CSV, JSON**, ו-**Excel**.

3.11.5. אינטגרציה עם מערכות צד ג'

3.11.5.1. המערכת תאפשר לכלי צד ג' להירשם כמנויים לקבלת עדכוני מידע בתצורת **pub/sub**.

3.11.5.2. הספק יספק מנגנונים לתמיכה במנויים אלו, תוך שמירה על אבטחת מידע, פרטיות, ותאימות לרגולציה.

3.11.6. ניהול נתונים מבוזר ותמיכה ב-**Big Data**

3.11.6.1. המערכת תכלול כלים לניהול נתונים מבוזר ואחוד (**Data Federation**), המאפשרים שילוב נתונים ממקורות מגוונים לצורך תחקור מתקדם.

3.11.6.2. פתרונות הנתונים יתמכו במדרגיות מלאה ובניתוחי נתונים בקנה מידה גדול (**Big Data**), תוך שמירה על ביצועים גבוהים וזמן תגובה קצר.

3.11.7. אבטחת מידע וניהול הרשאות

3.11.7.1. על הכלים לכלול מנגנוני הרשאות מתקדמים לניהול גישה לנתונים, תוך יישום עקרונות **Data Governance**.

3.11.7.2. הגישה לנתונים תהיה מנוהלת על פי רמות הרשאה מבוססות תפקידים ודרישות פרטניות, בהתאם להנחיות בפרק 4 אבטחת מידע.

3.11.8. ארכיטקטורת נתונים וכלים מוצעים

3.11.8.1. על הספק להציע ארכיטקטורת מערכת מלאה לניהול דוחות ואנליטיקה, הכוללת טכנולוגיות וכלים מתקדמים ליישום היכולות הנדרשות.

3.11.8.2. אם הספק אינו מספק פתרונות בינה מלאכותית ישירות, עליו להציג מנגנונים להנגשת המידע בצורה אינטראקטיבית למערכות **AI** משיקות.

3.11.8.3. הארכיטקטורה תתמוך במתודולוגיות עיבוד נתונים בזמן אמת ובסביבות **Big Data** מתקדמות.

3.12. רכיבי קצה - משתמשים ולקוחות

3.12.1. עקרונות כלליים

3.12.1.1. על הספק להציג מפרט טכני מלא ומפורט של הדרישות ממערכות המשתמשים לצורך התחברות ותפעול הממשקים והשדרים מול מערכת הסליקה.

3.12.1.2. הספק יהיה אחראי להבטיח שהתשתיות, רכיבי הקצה, ומערכות המשתמשים יתממשקו בצורה מלאה, תקינה ויעילה למערכת הסליקה, תוך שמירה על חוויית משתמש מיטבית.

3.12.1.3. דרישות לאימות משתמשים ורכיבי קצה יפורטו בפרק 4 אבטחת מידע במכרז זה, ויהיו בכפוף להראות הממונה ובאחריות הספק לוודא עמידה בהן.

3.12.2. לקוחות ובעלי רישיון

3.12.2.1. דרישות לאימות לקוחות ובעלי רישיון יפורטו בפרק 4 אבטחת מידע.

3.12.2.2. על הספק לפרט את הדרישות הטכניות של חיבור באמצעות שימוש בדפדפן אינטרנט, לרבות:

3.12.2.2.1. גרסאות מערכת הפעלה נתמכות (**Windows, macOS**, או אחרות).

3.12.2.2.2. דרישות חיבור לרשת (לדוגמה: מהירות מינימלית ותצורת רשת נדרשת).

3.12.2.2.3. דפדפנים נתמכים והגרסאות המינימליות הנדרשות.

3.12.2.2.4. רכיבים נוספים שעשויים להיות נחוצים, כמו תוספי דפדפן או תוכנות צד ג'.

3.12.3. דרישות תשתית נוספות

3.12.3.1. על הספק להציג דרישות טכניות עבור מערכות, שיתחברו למערכת באמצעות **API**.

3.12.3.2. המפרט יכלול:

3.12.3.2.1. דרישות חיבור לרשת, כולל תמיכה בתקשורת מאובטחת באמצעות פרוטוקולים כגון **HTTPS/TLS**.

3.12.3.2.2. גרסאות נתמכות של מערכות הפעלה ושרתים עבור משתמשים.

3.12.3.2.3. פורמטים נתמכים להעברת מידע (**JSON, XML, AVRO**, או אחרים).

3.12.3.2.4. פרטים טכניים נוספים הנדרשים לצורך אינטגרציה עם שירותי ה-**API** של המערכת.

3.12.4. התאמה טכנולוגית

3.12.4.1. על הספק להבטיח שהמפרט הטכני יעמוד בסטנדרטים מקובלים בתעשייה, תוך התאמה לצרכים של משתמשי קצה מגוונים (לקוחות, בעלי רישיון וגופים מוסדיים).

3.12.4.2. הספק יפרט כיצד יטופלו שינויים טכנולוגיים עתידיים, כגון עדכוני גרסה של מערכות הפעלה, דפדפנים, או פרוטוקולים.

3.12.5. תאימות ושירות

3.12.5.1. הספק יהיה אחראי לספק תמיכה טכנית לגופים המתחברים למערכת, כולל סיוע בהתממשקות, זיהוי בעיות, ומתן פתרונות עבור רכיבי קצה שאינם עומדים בדרישות.

3.12.5.2. הספק יוודא שכל רכיב קצה עומד בהנחיות אבטחת המידע המפורטות בפרק 4 אבטחת מידע.

3.13. רכיבים וכלים נוספים

3.13.1. סך הפתרונות הנדרשים ממערכת הסליקה יכללו רכיבים וכלים נוספים אשר יספקו תמיכה בתהליכים מרכזיים, ייעול תפעול, שיפור אבטחת מידע וניהול מידע לאורך מחזור חיי המערכת. על הספק להציע פתרונות אשר יתמכו בדרישות המפורטות בפרק 2 השירותים, תוך שימוש בכלי **SaaS**, ככל שנדרש, ובהתאם להנחיות המפורטות בפרק 4 אבטחת מידע.

3.13.2. על הספק להטמיע מנגנון לחתימות דיגיטליות מאובטחות, אשר יהיה מותאם לחוקי מדינת ישראל ולתקני אבטחת מידע בינלאומיים. המנגנון יאפשר חתימה על מסמכים ותהליכים קריטיים, תוך שמירה על עקיבות ובקרת גישה.

3.13.3. המערכת תכלול פתרון לארכוב מידע המותאם לצרכים משפטיים ורגולטוריים. יש לכלול מנגנונים לשמירה על נתונים לטווח ארוך, עם אופטימיזציה לעלות ותמיכה במדיניות מחזור חיי נתונים (**Data Lifecycle Management**).

3.13.4. על הספק להציע מנגנון לשליחת הודעות והתראות למשתמשים בערוצים מגוונים כגון **Email, SMS** ו-**Push Notifications**. המנגנון יאפשר ניהול תבניות הודעות מותאמות אישית לפי פרופיל המשתמש ודרישות המערכת.

3.13.5. המערכת תכלול כלים לניהול ותזמון משימות (**Schedulers**), כולל אוטומציה של תהליכים חוזרים או תהליכים מבוססי זמן. על הספק לספק פתרון המאפשר מעקב אחר ביצוע התהליכים, זיהוי תקלות וניהולן בצורה מבוקרת.

3.13.6. על הספק להטמיע מנגנונים לניהול ותחקור יומני פעילות (**Audit Logs**) לצורך מעקב אחר שינויים, תחקור תקלות וציות לדרישות רגולטוריות.

3.13.7. על הספק לספק מערכת לניהול ותיעוד ידע אשר תשמש את משתמשי הקצה וצוותי התמיכה. המערכת תכלול תכני הדרכה מובנים, דוקומנטציה מסודרת ומאגר שאלות נפוצות (**FAQ**) שינוהל בצורה דינמית ויהיה זמין למשתמשים באתר או באפליקציה.

3.13.8. המערכת תאפשר שילוב פתרונות תקשורת מבוססי צ׳אט ובינה מלאכותית, כולל צ׳אטבוטים לתמיכה אינטראקטיבית במשתמשים. יישום רכיב זה יתבצע לפי שיקול דעת הספק ובהתאם לצרכים תפעוליים או לשיפור חוויית המשתמש.

3.13.9. על הספק להציג פתרונות מבוססי טכנולוגיות סטנדרטיות, תוך הדגשת יכולות אינטגרציה עם מערכות קיימות ואפשרויות הרחבה עתידיות.

3.14. שליטה, בקרה, זמינות, גיבוי והתאוששות מאסון

3.14.1. סעיף זה עוסק בהיבטים הטכנולוגיים הדרושים להבטחת שליטה, ניטור ובקרה (שו"ב), זמינות גבוהה, גיבוי והתאוששות מאסון (**DR**). על הספק להציג פתרונות טכנולוגיים מלאים הכוללים ארכיטקטורה, כלים וטכנולוגיות המיועדים למימוש יכולות אלו, תוך עמידה בדרישות המפורטות בחלק המשכיות עסקית שבפרק 4 אבטחת מידע. כל פתרון יעמוד בתקנים בינלאומיים מוכרים ויכלול שילוב טכנולוגיות מתקדמות, לרבות:

3.14.1.1. **ISO/IEC 27040**- הגנה על אחסון נתונים, כולל ניהול אבטחה, גיבוי והתאוששות.

3.14.1.2. **ISO/IEC 22301**- ניהול המשכיות עסקית, כולל יעדי זמינות ותהליכי התאוששות מאסון.

3.14.1.3. **Uptime Institute Tier Standards**- רמות זמינות לתשתיות **IT Tier 3** ו **Tier 4**-עבור מערכות קריטיות.

3.14.1.4. **NIST SP 800-34**- מדריך לניהול תוכניות התאוששות מאסון במערכות מידע.

3.14.1.5. **ITIL (Information Technology Infrastructure Library)** ניהול זמינות ושירותי **IT**.

3.14.1.6. **ISO/IEC 20000** - ניהול שירותי **IT** כולל בקרה על תשתיות ותהליכים.

3.14.1.7. **SNMP (Simple Network Management Protocol)** סטנדרט לניהול תשתיות רשת.

3.14.2. ניטור ובקרה

3.14.3. על הספק להטמיע מערכת שו"ב מתקדמת לניטור בזמן אמת של תשתיות, אפליקציות ותהליכים עסקיים. המערכת תכלול רכיבי ניטור פרואקטיביים המאפשרים זיהוי מוקדם של תקלות ואנומליות. המערכת תכלול שימוש בפתרונות כגון **Prometheus** ו-**Grafana** לניטור ביצועי תשתיות. כמו כן, יש לשלב כלי **BAM** (**Business Activity Monitoring**) לניטור מדדים עסקיים קריטיים בזמן אמת. על הספק להבטיח התראות אוטומטיות, ניתוח מגמות, ואינטגרציה עם פתרונות **SIEM** לצורך ניטור מאובטח ובקרה מרכזית.

3.14.4. זמינות גבוהה ויתירות

3.14.5. על הספק להבטיח זמינות גבוהה (**High Availability**) של המערכת ברמת זמינות של לפחות 99.5%. הפתרונות יכללו יתירות מלאה בתשתיות קריטיות, לרבות רשתות, שרתים, בסיסי נתונים ואחסון, תוך שימוש בתצורות **Active-Active** או **Active-Passive**. יש ליישם מנגנוני **Load Balancing** לניהול עומסים ומנגנוני **Failover** אוטומטיים להבטחת המשכיות השירות. הפתרונות יעמדו בדרישות **Uptime Institute Tier Standards** ברמות **Tier 3** או **Tier 4**.

3.14.6. גיבויים

3.14.7. על הספק להציג פתרונות גיבוי מתקדמים שיבטיחו שמירה ואבטחת נתוני המערכת. הגיבויים יתבצעו בהתאם להנחיות המוגדרת בחלק המשכיות עסקית בפרק 4 אבטחת מידע, תוך שימוש בשיטות כגון **Snapshot** ו- **Offsite Backup**. הגיבויים יתבצעו בתדירות המתאימה לסוגי המידע ויכללו שמירה יומית לנתונים קריטיים ושמירה שבועית או חודשית למידע ארכיוני. יש להבטיח הצפנת גיבויים ובקרת גישה, בהתאם לסטנדרטים **ISO/IEC 27040** ו-**NIST SP 800-34**.

3.14.8. שחזור נתונים

3.14.9. פתרונות השחזור יבטיחו זמני **RTO** (**Recovery Time Objective**) של עד 4 שעות וזמני **RPO** (**Recovery Point Objective**) של אפס אובדן נתונים (**RPO=0**). יש לתמוך בשחזור פריטי מידע בודדים, כולל שחזור מלא או חלקי של נתונים ורכיבי מערכת.

3.14.10. טכנולוגיות למימוש תוכניות **DRP**

3.14.11. על הספק להציג טכנולוגיות מתקדמות למימוש תוכניות (**Disaster Recovery Plan**) **DRP**, בהתאם להנחיות המשכיות עסקית שבפרק 4 אבטחת מידע. התוכנית תכלול מנגנוני דילוג אוטומטיים בין אתרים חלופיים, הגדרות שלבי שחזור הכוללות זיהוי התקלה, מעבר לאתר חלופי ושיקום המערכת. על הספק לוודא כי תוכנית ה-**DRP** מעודכנת ונבחנת לפחות אחת לשנה או לאחר שינויים מהותיים במערכת.

3.14.12. בדיקות התאוששות תקופתיות

3.14.13. הספק יבצע בדיקות התאוששות תקופתיות לפחות אחת לשנה. הבדיקות יכללו תרגול תרחישי כשל, הפעלת אתר **DR** למשך 24 שעות לפחות, ובדיקת המשכיות עסקית ללא השבתת המערכת המרכזית.

3.14.14. שקיפות ובקרה

3.14.15. על הספק להבטיח ממשקי ניטור ודוחות מפורטים, המאפשרים מעקב אחר סטטוס הגיבויים, תהליכי השחזור ותפקוד מערכות היתירות. המערכת תספק התראות בזמן אמת על כשלים בגיבוי ובשחזור.

3.14.16. אינטגרציה עם מערכות קיימות

3.14.17. הפתרונות המוצעים על ידי הספק יותאמו לתשתיות קיימות ויתמכו בהרחבות עתידיות. הספק רשאי להשתמש בכלי **SaaS** בתחום השו"ב, הגיבוי וההתאוששות, בכפוף לדרישות בפרק 4 אבטחת מידע.

3.15. סביבות עבודה

3.15.1. עקרונות כלליים

3.15.1.1. פרק זה מגדיר את הדרישות המרכזיות לתכנון, הקמה וניהול של סביבות עבודה שונות, המותאמות לצרכים התפעוליים, הפיתוחיים והאבטחתיים של המערכת.

3.15.1.2. על הספק להבטיח בידוד מלא בין הסביבות, שימוש בכלים טכנולוגיים מתקדמים לניהולן ויישום מנגנונים מבוקרים למעבר בין סביבות.

3.15.2. סביבות נדרשות

3.15.2.1. סביבת פיתוח (**Development**) תיועד לפיתוח ותחזוקה של קוד המערכת, תוך גישה חופשית למפתחים ושילוב כלי פיתוח.

3.15.2.2. סביבת בדיקות (**Testing**) תכלול תרחישי בדיקות אוטומטיות וידניות, לצורך בדיקת איכות הקוד ורכיבי המערכת.

3.15.2.3. סביבת אינטגרציה (**Integration**) תאפשר אימות אינטגרציה בין רכיבי המערכת לפני העלאת גרסאות לסביבת טרום ייצור.

3.15.2.4. סביבת הדרכה (**Training**) תשמש לתרחישי הדרכה וסימולציות עבור משתמשי קצה וצוותי תמיכה.

3.15.2.5. סביבת טרום ייצור (**Pre-Production**) תדמה את סביבת הייצור ותכלול את כל רכיבי המערכת לצורך בדיקות סופיות.

3.15.2.6. סביבת ייצור (**Production**) תשמש לפעילות בזמן אמת ותעמוד בדרישות זמינות, ביצועים ואבטחת מידע מחמירות.

3.15.2.7. סביבת ארגז חול (**Sandbox**) מיועדת למפתחים וספקי צד ג' לצורך חיבור, התנסות ופיתוח תוך שימוש בממשקי המערכת.

3.15.3. ניהול והפרדת סביבות

3.15.3.1. על כל סביבה להיות מבודדת פיזית או לוגית, למניעת השפעות הדדיות בין תהליכים ובין משתמשים.

3.15.3.2. יש לנהל כל סביבה באמצעות מנגנוני בקרת גישה מבוססת תפקידים (**RBAC**), המגבילים את הגישה לפי תפקידי המשתמשים ואופי השימוש בסביבה בכפוף לדרישות בפרק 4 אבטחת מידע.

3.15.4. כלים לניהול סביבות עבודה

3.15.4.1. על הספק להשתמש בכלי ניהול סביבות עבודה אוטומטיים, כגון **Terraform** או **Ansible**, לצורך הגדרה וניהול תשתיות סביבות.

3.15.4.2. יש להטמיע כלי **CI/CD** לניהול אינטגרציה רציפה (**Continuous Integration**) והעלאת שינויים לסביבות בצורה מבוקרת, תוך שימוש בפתרונות כמו **Jenkins** או **GitLab CI/CD**. כמפורט בסעיף 3.16 להלן.

3.15.5. תמיכה באבטחת מידע בסביבות

3.15.5.1. כל סביבה תעמוד בדרישות אבטחת מידע זהות לסביבת הייצור, לרבות הצפנת נתונים וניטור תעבורה בהתאם לדרישות המפורטות בפרק 4 אבטחת מידע.

3.15.5.2. יש להבטיח שמידע רגיש אינו מועבר או משוכפל בין סביבות ללא בקרת גישה מאובטחת, ובפרט למנוע זליגת מידע רגיש מסביבת הייצור לסביבות פיתוח, בדיקות או ארגז חול.

3.15.6. גמישות לאוטומציה ובדיקות

3.15.6.1. על הספק להטמיע כלי בדיקות אוטומטיות כגון **Selenium** או **Cypress** לצורך זיהוי מוקדם של תקלות ותמיכה ברציפות הפיתוח.

3.15.6.2. סביבות הבדיקות יתמכו בבדיקות עומסים וביצועים, כולל בדיקות עומסים לרכיבי תשתית ולנתונים. כפי כמפורט בסעיף 3.16 להלן.

3.15.7. ארגז חול לעידוד חדשנות

3.15.7.1. סביבת ארגז חול תאפשר חיבור מבוקר ומאובטח של צדדי ג' תוך שימוש בממשקי **API** של המערכת.

3.15.7.2. על הספק להבטיח גמישות עבור ספקי צד ג' לצורך ניסויים ופיתוח פתרונות חדשניים ללא סיכון לסביבת הייצור.

3.15.7.3. הסביבה תכלול גישה לנתוני דמה (**Mock Data**) או נתונים מונפשים (**Synthetic Data**) בהתאם להנחיות פרטיות ורגולציה כמפורט בפרק 4 אבטחת מידע.

3.15.8. שקיפות וניטור סביבות

3.15.8.1. על הספק להטמיע כלי ניטור ובקרה עבור כל סביבה, לצורך מעקב אחר פעילות, זיהוי תקלות ותפעול יעיל.

3.15.8.2. על הספק להבטיח קיומו של ממשק מרכזי לניהול סביבות העבודה, שיאפשר תצוגה של סטטוס כל הסביבות בזמן אמת.

3.15.9. הצגת ההצעה הטכנולוגית

3.15.9.1. על הספק להציג הצעה מפורטת הכוללת את ארכיטקטורת סביבות העבודה המתוכננת.

3.15.9.2. ההצעה תכלול פירוט הכלים הטכנולוגיים לניהול ובקרת סביבות.

3.15.9.3. ההצעה תכלול תהליכי עבודה מבוקרים למעבר בין סביבות (**Promotion Workflow**).

3.15.9.4. ההצעה תכלול מנגנונים להבטחת אבטחת מידע ושקיפות.

3.15.9.5. על הספק לכלול תוכנית מפורטת לשילוב ותפעול סביבה ייעודית לעידוד חדשנות באמצעות ארגז חול.

3.16. כלי פיתוח ובדיקות

3.16.1. תמיכה במחזור פיתוח מלא (**SDLC**)

3.16.1.1. על הספק להקים סביבת פיתוח התומכת בכל שלבי מחזור חיי התוכנה (**SDLC**), החל מתכנון, פיתוח, בדיקות, הפצה ועד לתחזוקה שוטפת.

3.16.1.2. הספק יבסס את סביבת הפיתוח על מתודולוגיות מוכרות כגון **Agile** ו-**DevOps**, ויתאים את התהליכים, לפי שיקול דעתו, למסגרות הידע **Agile Manifesto** ו-**DevOps Handbook**.

3.16.1.3. הסביבה תתמוך באינטגרציה רציפה (**CI**) והפצת גרסאות רציפה (**CD**) לניהול תהליכי פיתוח ושחרור גרסאות בצורה מבוקרת.

3.16.1.4. על הספק להשתמש בכלים כגון **Jenkins, GitLab CI/CD, CircleCI** או **Azure DevOps**, תוך הבטחת ניהול **Pipeline** מלא הכולל **Build**, בדיקות ושחרור גרסאות.

3.16.2. כלי ניהול דרישות, תכנון, עיצוב ואפיון

3.16.2.1. הספק יספק כלים לניהול דרישות, תכנון ועיצוב כגון **Jira, Asana, Azure Boards** או כלים דומים.

3.16.2.2. יש להבטיח שכלי התכנון יתמכו בשיתוף פעולה בצוותים מבוזרים, כולל תמיכה בזמן אמת.

3.16.2.3. כלים כמו **Miro, Figma** או **Draw.io** ישמשו לתכנון ואפיון תהליכים, עם ממשקים אינטגרטיביים לכלים נוספים בסביבה.

3.16.3. תמיכה בעבודה מבוזרת ושיתוף פעולה

3.16.3.1. סביבת הפיתוח תתאים לעבודה מבוזרת של צוותים תוך שימוש במערכות ניהול קוד מקור כגון **GitHub, GitLab** או **Bitbucket**.

3.16.3.2. על הספק להבטיח תמיכה בניהול ענפים (**Branching**) ומיזוג שינויים (**Merging**), תוך שמירה על עקיבות ותיעוד תהליכי שינוי.

3.16.3.3. יש לשלב פתרונות לניהול **Pull Requests**, מעקב אחר שינויים בקוד ותיעוד מלא של גרסאות.

3.16.4. כלי פיתוח מתקדמים

3.16.4.1. על הספק להציע עורך קוד אינטראקטיבי כגון **Visual Studio Code, IntelliJ IDEA**, או **Eclipse**, המספק תמיכה באינטגרציות לכלים נוספים.

3.16.4.2. יש לשלב כלי ניתוח קוד סטטי, כגון **SonarQube**, לזיהוי מוקדם של בעיות קוד ואבטחת מידע.

3.16.4.3. על הספק לספק פתרונות לניהול תלויות בקוד באמצעות כלים כגון **Maven** או **Gradle**, המאפשרים עדכון אוטומטי של ספריות וניהול חבילות.

3.16.4.4. סביבת הפיתוח תכלול ניהול ארטיפקטים ותוספי תוכנה עם פתרונות כמו **Artifactory** או **Nexus**, כולל ניהול גרסאות וסרטיפיקציה של חבילות קוד.

3.16.5. כלי בדיקות

3.16.5.1. הסביבה תכלול תמיכה בבדיקות אוטומטיות לכל רמות הבדיקות, לרבות בדיקות יחידה (**Unit Tests**), אינטגרציה (**Integration Tests**) ובדיקות מערכת (**System Tests**).

3.16.5.2. יש לשלב כלי בדיקות מתקדמים כגון **Selenium, Cypress** או **Playwright** לבדיקת ממשקי משתמש, וכלים כמו **JUnit** או **PyTest** לבדיקות יחידה.

3.16.5.3. על הספק להטמיע פתרונות לבדיקות עומסים וביצועים, כגון **JMeter** או **Gatling**, ולשלב כלי סימולציה לתרחישי קצה כמו **WireMock**.

3.16.5.4. הספק יקים שתי סביבות ניסוי נפרדות: סביבת ניסוי עבור בדיקות שיבוצעו טרם עלייה לאוויר של גרסה חדשה או עדכון של מערכת הסליקה וסביבת בדיקות שוטפת לבחינת מוכנות, כשירות ותקינות מערכות המשתמשים ועבודתן אל מול מערכת הסליקה.

3.16.5.5. מטרת סביבת הניסוי עבור בדיקות שיבוצעו טרם עלייה לאוויר הינה לבדוק את מוכנות משתתפי המערכת לפעול על פי הגרסה החדשה או העדכון, בהתאם לכללי המערכת שפורסמו על ידי מערכת הסליקה, בטרם העלאת הגרסה או העדכון. סביבת ניסוי זו תהיה זמינה במועדים שיאושרו על ידי הרשות, ותתמוך לפחות בבדיקות הבאות:

3.16.5.5.1. בדיקת ממשקי המבנה האחיד החדשים לרבות כלל התהליכים הקשורים בהעברתם. הבדיקה תכלול מגוון ממצה של תסריטים עסקים ותאפשר מעקב אחר היזונים חוזרים. כמו כן, יבדקו כל סוגי הפעולות שמושפעות משינוי הגרסה (רגרסיה).

3.16.5.5.2. פעולות המורכבות ממספר תהליכים ושמתרחשות במקביל בין מספר סוגי משתתפים, כגון העברת כספים בין גופים מוסדיים.

3.16.5.5.3. פעולות המשלבות העברת מידע וכסף, כגון הפקדת כספים על ידי מעביד והעברת מידע לגבי ביצוע הפקדה.

3.16.5.6. מטרת סביבת בדיקות שוטפות לאפשר למשתמשים שמעוניינים בכך לבדוק את התאמתן להוראות כללי המערכת ודרישות מערכת הסליקה, כגון, משתתפים חדשים או משתמשים שביצעו עדכון או שינוי במערכותיהן המיכוניות. סביבת בדיקות שוטפות תתייחס לפחות לאלה:

3.16.5.7. בדיקת ממשקי המבנה האחיד הקיימים לרבות כלל התהליכים הקשורים בהעברתם. הבדיקה תכלול מגוון ממצה של תסריטים עסקים ותאפשר מעקב אחר היזונים חוזרים.

3.16.5.8. בדיקה שוטפת אוטומטית לבחינת איכות הקבצים המועברים באמצעות מערכת הסליקה.

3.16.5.9. סביבות הניסוי יפעלו בהתאם לתנאים הבאים:

3.16.5.9.1. סביבות הניסוי ישמשו לבדיקת תקינות הממשקים והתהליכים בהתאם לכלל הבדיקות שמבוצעות על ידי מערכת הסליקה, לרבות הבדיקות המתייחסות לאיכות

המידע המועבר, ויועברו היזונים חוזרים לגבי כל סוגי השגיאות והתקלות שיימצאו בקבצים.

3.16.5.9.2. מערכת הסליקה תספק תמיכה טכנית ותמיכה ברמת התוכן לאנשי המיכון, הפיתוח והאפיון של המשתמשים לגבי שני סוגי סביבות הניסוי לעיל, בנוגע לשגיאות, התקלות והקשיים העולים מתוך הבדיקות שיבוצעו על ידי המשתתפים בסביבת הניסוי (מערך התמיכה למפתחים ומתכנתים).

3.16.5.9.3. מערכת הסליקה תפיק אישורים לגבי מוכנות המשתמשים, לצורך הצגתם למשתמשים או לממונה, והכל בהתאם להוראות הממונה.

3.16.5.9.4. הספק יקבע נוהל לעניין ניהול סביבת ניסוי שיתייחס לנושאים שבסעיף זה ואשר יובא לאישור הממונה. הנוהל יכלול גם קביעה של מועדים לביצוע בדיקות שוטפות (להלן – **נוהל סביבת ניסוי**).

3.16.6. תמיכה במתודולוגיית **Clean Code** ו-**Clean Architecture**

3.16.6.1. סביבת הפיתוח תתמוך בכתיבת קוד על פי עקרונות **Clean Code** ותכנון מבנה ברור לפי **Clean Architecture** (**Common practice published by Robert C. Martin and was widely adopted**).

3.16.6.2. יש לשלב כלים לניהול איכות קוד, כגון **ESLint** או **Prettier**, המסייעים בכתיבה הגהה ותחזוקה של הקוד.

3.16.7. אבטחת איכות ואבטחת מידע

3.16.7.1. על הספק להטמיע כלי סריקת קוד אוטומטיים כגון **Checkmarx, Snyk** או **WhiteSource**, לצורך זיהוי מוקדם של בעיות אבטחת מידע ותאימות. המימוש יהיה בהתאם לדרישות בפרק 4 אבטחת מידע.

3.16.7.2. סביבת הפיתוח תכלול כלים לניהול איכות המוצר, ניטור באגים, ובדיקת כיסוי קוד באמצעות בדיקות מוטציות (**Mutation Testing**).

3.16.8. ניהול תשתיות באמצעות קוד (**IaC**)

3.16.8.1. הספק יספק תמיכה בתשתיות מבוססות קוד (**Infrastructure as Code**), תוך שימוש בכלים כמו **Terraform, Ansible** או **Pulumi**.

3.16.8.2. על הסביבה לתמוך בכתיבת סקריפטים לאוטומציה של הקמת סביבות עבודה וניהולן.

3.16.9. שקיפות וניהול משימות

3.16.9.1. סביבת הפיתוח תכלול כלי ניהול משימות כגון **Jira, Trello** או **Azure DevOps**, שיאפשרו מעקב אחר ביצוע משימות, הגדרת יעדים ומעקב אחר **KPI**.

3.16.9.2. הכלים יאפשרו תצוגה ברורה של סטטוס הפרויקטים, זיהוי צווארי בקבוק והמלצות לשיפור ביצועים.

3.16.10. תמיכה במודולריות ומדרגיות

על ארכיטקטורת התוכנה להיות מודולרית, תוך תמיכה בשילוב רכיבי מערכת ושדרוגם בהתאם לדרישות עתידיות.

3.16.11. ניהול גרסאות ותצורה

3.16.11.1. הספק ישלב כלי ניהול גרסאות כגון **Git**, לצד פתרונות לניהול תצורה ושינויים בצורה מבוקרת.

3.16.11.2. ניהול פיצ׳רים יתבצע באמצעות מנגנוני **Feature Flags**, עם פתרונות כגון **LaunchDarkly** או **Split**, לניהול הדרגתי של שינויים לפי שיקול דעתו של הספק.

3.16.12. ניטור ובקרת איכות בפיתוח

3.16.12.1. על הספק להציע כלים לניטור ביצועי קוד ולבקרת תקלות, כגון **New Relic** או **Datadog**.

3.16.12.2. הספק יטמיע מנגנונים המאפשרים הפקת דוחות בזמן אמת על סטטוס התהליך והמלצות לשיפור.

3.16.13. שימוש בטכנולוגיות **AI**

3.16.13.1. ככל שנעשה שימוש בטכנולוגיות **AI** לשיפור והתייעלות בתהליכי פיתוח ובדיקות, על הספק להבטיח שהשימוש אינו חושף זכויות יוצרים או פוגע בפרטיות נתוני המשתמשים ולקוחות.

3.16.13.2. הספק יישם מנגנוני פרטיות ואבטחת מידעכגון ניהול מאובטח של נתוני קלט ופלט, ויפעל בהתאם לתקני פרטיות בינלאומיים והכל בכפוף לדרישות בפרק 4 אבטחת מידע, הגנת הפרטיות, והמשכיות עסקית.

3.17. שגרות עבודה ותקנים

3.17.1. עקרונות כלליים

3.17.1.1. פרק זה מגדיר את שגרות העבודה, הנהלים והמדיניות שעל הספק ליישם לצורך ניהול ותפעול המערכת. הפרק מתמקד בהבטחת מחזורי עבודה סדורים, יעילות תפעולית, ושמירה על אמינות המערכת, תוך עמידה בתקנים והנחיות רגולטוריות.

3.17.1.2. שגרות העבודה ייושמו בהתאם לתקנים בינלאומיים מוכרים, לרבות:

3.17.1.2.1. **ISO/IEC 20000** לניהול שירותי **IT**.

3.17.1.2.2. **ITIL** לניהול שגרות שירות, ניהול שינויים, וטיפול בתקלות.

3.17.1.2.3. **CMMI** לשיפור וניהול תהליכים ארגוניים.

3.17.1.2.4. **ISO/IEC 27001** לניהול מערכות אבטחת מידע, כפי שמוגדר בפרק 4 אבטחת מידע.

3.17.1.3. על הספק להבטיח תיעוד מלא של כל הנהלים, השגרות והתהליכים, תוך הבטחת נגישות לכל בעלי העניין ואפשרות לעדכון שוטף.

3.17.2. ניהול מחזור חיי תוכנה (**SDLC**)

3.17.2.1. הספק יגדיר שגרות לניהול מחזור חיי התוכנה (**SDLC**) בהתאם למתודולוגיות **Agile** ו-**DevOps**, תוך הקפדה על שימוש באוטומציה בכל שלב במחזור החיים.

3.17.2.2. הספק יגדיר את התהליכים המרכזיים לניהול **SDLC**, כולל:

3.17.2.2.1. שלב התכנון: ניהול דרישות, אפיון ועיצוב.

3.17.2.2.2. שלב הפיתוח והבדיקות: ניהול איכות הקוד, שילוב בדיקות ידניות ואוטומטיות, ובדיקות רגרסיה.

3.17.2.2.3. שלב שחרור גרסאות: ניהול שינויים ושחרור גרסאות מבוקר.

3.17.2.2.4. שלב התחזוקה: ניהול עדכונים שוטפים, טיפול בתקלות ושדרוגים.

3.17.3. מדיניות שימוש בקוד פתוח

3.17.3.1. על הספק להגדיר את מדיניות העבודה עם קוד פתוח, תוך עמידה בתקנים והנחיות רגולטוריות רלוונטיות.

3.17.3.2. הספק יפרט את הדרישות לניהול עדכונים בקוד פתוח, זיהוי סיכונים, וניהול תאימות לרגולציות.

3.17.3.3. על הספק ליישם תהליכים לזיהוי וניהול חשיפות בקוד פתוח, ולהבטיח שימוש בטוח תוך מניעת פגיעה בזכויות יוצרים או פרטיות.

3.17.4. מדיניות שימוש בתשתיות ענן

3.17.4.1. ככל ורלוונטי, הספק יגדיר את המדיניות לשימוש בתשתיות ענן ציבורי, פרטי או היברידי, תוך עמידה בדרישות רגולטוריות ואבטחת מידע.

3.17.4.2. המדיניות תכלול הנחיות לניהול משאבים, אופטימיזציה תקציבית (**FinOps**), ושימוש במנגנוני בקרה והפרדה בין סביבות ענן שונות.

3.17.4.3. יש להבטיח שימוש בשיטות מוכרות לתכנון וניהול ענן, כגון **Well-Architected Framework** של **AWS**, או פתרונות מקבילים.

3.17.5. ניהול ספקים משנה

3.17.5.1. הספק יגדיר נהלים לניהול ספקי משנה ושותפים, לרבות תהליכים למעקב אחר עמידה בהתחייבויות חוזיות, בקרת איכות השירותים המוצעים, וניהול סיכונים.

3.17.5.2. על הספק לכלול מנגנונים לניהול חוזים והסכמים, תוך הגדרת מדדי ביצוע (**KPIs**) ומנגנוני פיקוח שוטף.

3.17.6. תמיכה וזמני תגובה

3.17.6.1. הספק יגדיר נהלים ברורים לטיפול בפניות ותקלות, תוך הקפדה על זמני תגובה ותיקון (**SLAs**) בהתאם לחומרת הפנייה.

3.17.6.2. הספק יטמיע ויישם מערכת לניהול פניות משתמשים, הכוללת מעקב אחר סטטוס הפניות, מתן התראות ועדכון שוטף של מבקשי השירות.

3.17.6.3. נהלי התמיכה יכללו תהליכים לשיפור רציפות השירות, באמצעות ניתוח תקלות ותהליכי למידה שוטפים.

3.17.7. ניטור ובקרה (שו"ב)

3.17.7.1. הספק יטמיע נהלי ניטור ובקרה (**NOC/SOC**) לניהול תשתיות, אפליקציות ותהליכים עסקיים, תוך שימוש בסטנדרטים לניהול אירועים ותקלות לפי **ITIL**.

3.17.7.2. הנהלים יתייחסו לתרחישי מעקב בזמן אמת אחר ביצועי המערכת והתשתיות, כולל ניהול התראות וטיפול מידי באירועים.

3.17.8. עדכון ותחזוקת נהלים

3.17.8.1. על הספק לתעד את כל הנהלים ושגרות העבודה בצורה מסודרת ומבנית, תוך הבטחת נגישותם לכלל בעלי העניין.

3.17.8.2. נהלים ושגרות ייבחנו ויעודכנו באופן שוטף, לפחות אחת לשנה או בהתאם לשינויים מערכתיים, רגולטוריים או טכנולוגיים.

3.17.8.3. הספק יבטיח כי שינויים ותוספות בנהלים מתבצעים בתהליך מבוקר ומאושר.

3.17.9. בקרת תקציב **FinOps**

3.17.9.1. על הספק להטמיע כלים ומתודולוגיות טכנולוגיות לניהול ובקרת תקציב, במטרה לאפשר אופטימיזציה של עלויות תשתית, תפעול ושירותי המערכת. הפתרונות יותאמו לעקרונות **FinOps** המודרניים וישלבו יכולות אנליטיות מתקדמות ותובנות מבוססות נתונים.

3.17.9.2. הכלים שיסופקו יאפשרו:

3.17.9.2.1. ניטור הוצאות בזמן אמת, תוך פיקוח על עלויות תשתית ענן ותשתיות מקומיות.

3.17.9.2.2. ניתוח מגמות הוצאה, כולל זיהוי רכיבים או שירותים בעלי עלויות חריגות והשפעותיהם על התקציב הכולל.

3.17.9.2.3. הגדרת תקציבים ומעקב אחר עמידה ביעדים תקציביים שנקבעו על ידי הנהלת המערכת.

3.17.9.3. הכלים יכללו יכולות חיזוי המאפשרות:

3.17.9.3.1. בניית תחזיות עלויות לטווח קצר ולטווח ארוך, בהתבסס על נתוני שימוש היסטוריים ותהליכים עתידיים.

3.17.9.3.2. סימולציות של תרחישים פיננסיים שונים לצורך הערכת ההשפעות התקציביות של שינויים בתשתיות או בשירותים.

3.17.9.4. הספק הזוכה יפיק דוחות תקופתיים מותאמים אישית לבקרה הכוללים:

3.17.9.4.1. פירוט מלא של הוצאות לפי סוגי משאבים, שירותים או מחלקות בארגון.

3.17.9.4.2. המלצות אוטומטיות לאופטימיזציה, כולל השבתת משאבים בלתי מנוצלים או התאמת רמות שירות לפי צרכים בפועל.

3.17.9.5. הכלים יאפשרו שליטה ובקרה באמצעות:

3.17.9.5.1. הגדרת תקרות תקציב (**Budget Caps**) והתראות על חריגות תקציביות בזמן אמת.

3.17.9.5.2. ממשקי ניהול מתקדמים המאפשרים יישום החלטות אופטימיזציה ישירות מהמערכת.

3.17.9.5.3. המערכת תתמוך באינטגרציה עם מערכות **ERP** וכלים פיננסיים קיימים בארגון, כדי לאפשר סנכרון מידע פיננסי ולשפר את יכולות הדיווח והבקרה.

3.17.9.6. הכלים יתמכו במתודולוגיות ניהול עלויות כגון **Cost Allocation** ו-**Showback/Chargeback**, לצורך ייחוס עלויות לפי יחידות ארגוניות או מחלקות.

3.17.9.7. על הספק הזוכה להבטיח שהפתרונות עומדים בסטנדרטים מקובלים בתחום **FinOps**, תוך שימוש בטכנולוגיות מוכרות כגון **CloudHealth, AWS Cost Explorer, Azure Cost Management**, או פתרונות מקבילים המותאמים לדרישות אבטחת המידע במערכת.

3.18. ניהול סיכונים במערכות מידע

3.18.1. עקרונות כלליים לניהול סיכונים

3.18.1.1. הספק יטמיע תהליך שיטתי ומובנה לניהול סיכונים במערכות מידע, הכולל זיהוי, הערכה, טיפול ומעקב מתמשך אחר סיכונים לאורך מחזור חיי המערכת.

3.18.1.2. ניהול הסיכונים יתבצע בהתאם למסגרות בינלאומיות מוכרות, לרבות:

3.18.1.2.1. **ISO/IEC 27005** לניהול סיכוני אבטחת מידע, המספק מתודולוגיה לזיהוי, הערכה וטיפול בסיכונים.

3.18.1.2.2. **ISO 31000** לניהול סיכונים ארגוני, המתמקד בגישה אחודה לניהול סיכונים בכל רמות הארגון.

.3.18.1.2.3 **NIST Risk Management Framework (RMF)** המספק כלים להגדרת מדיניות ולביצוע ניטור סיכונים.

.3.18.1.2.4 **COBIT** כמסגרת לניהול ובקרת מערכות מידע, המשלבת מדדי ביצוע ודרכי בקרה.

.3.18.1.2.5 **CMMI** לשיפור תהליכים והערכת רמות בשלות לניהול סיכונים ופרויקטים.

.3.18.2 תהליך ניהול סיכונים

.3.18.2.1 זיהוי סיכונים

.3.18.2.1.1 הספק יגדיר מנגנון לזיהוי סיכונים פוטנציאליים הכולל מיפוי מקורות איומים, נכסים קריטיים ותהליכים חשופים לפגיעה.

.3.18.2.1.2 על הספק לשלב תהליכי סיעור מוחות, סקירת תרחישים ובחינה של אירועים קודמים כמקור ללמידה וזיהוי סיכונים.

.3.18.2.2 הערכת סיכונים

.3.18.2.2.1 הספק יבצע הערכת סיכונים באמצעות ניתוח איכותי וכמותי, תוך שימוש במטריצות סיכונים הכוללות הסתברות והשלכות.

.3.18.2.2.2 תהליך ההערכה יכלול זיהוי השפעות עסקיות, תפעוליות ורגולטוריות של הסיכונים.

.3.18.2.2.3 על הספק להציג דוחות מסכמים המפרטים את תוצאות ההערכה, כולל דירוג סיכונים לפי חומרה וחשיבות.

.3.18.3 טיפול בסיכונים

.3.18.3.1 הספק יגדיר מנגנוני טיפול הכוללים:

.3.18.3.1.1 מניעת סיכונים: יישום טכנולוגיות ותהליכים לצמצום חשיפה.

.3.18.3.1.2 צמצום סיכונים: מנגנונים להפחתת ההשפעות השליליות של אירועים.

.3.18.3.1.3 העברת סיכונים: שימוש בביטוחים, שירותים חיצוניים או פתרונות אחרים.

.3.18.3.1.4 קבלת סיכונים: החלטה מודעת לניהול סיכונים בעלי הסתברות או השפעה נמוכה.

3.18.4. ניטור ובקרת סיכונים

3.18.4.1. על הספק להפעיל מנגנוני ניטור מתקדמים לזיהוי שינויים בפרופיל הסיכונים בזמן אמת.

3.18.4.2. יש להבטיח ניטור שוטף של תשתיות, אפליקציות, תהליכים עסקיים וממשקי צד ג'.

3.18.4.3. הניטור יתבצע באמצעות מערכות ייעודיות לניהול ובקרה, כולל הפקת התראות אוטומטיות וטיפול מהיר באירועים.

3.18.4.4. כל שינוי בפרופיל הסיכונים או זיהוי של סיכון חדש יוביל לעדכון תוכניות הטיפול באופן מיידי.

3.18.5. הצגת דוחות תקופתיים

3.18.5.1. הספק יתחייב להציג לממונה בפורטל הייעודי עבור הרשות דוחות מפורטים על ניהול הסיכונים הטכנולוגיים באופן תקופתי לרשות בהתאם לדרישות בסעיף 5.7 להלן ולהנחיות הרשות כפי שיהיו מעת לעת.

3.18.5.2. דוחות אלו יכללו:

3.18.5.2.1. סקירה מעודכנת של פרופיל הסיכונים, כולל דירוגם לפי חומרה.

3.18.5.2.2. תיעוד אירועי סיכון שהתרחשו, ניתוח הגורמים לאירועים ותוכניות פעולה מתקנות.

3.18.5.2.3. מעקב אחר יישום פעולות מתקנות ושיפורים בתהליכי ניהול הסיכונים.

3.18.5.2.4. מדדי ביצוע מרכזיים (**KPIs**) להערכת אפקטיביות תהליך ניהול הסיכונים.

3.18.6. תיעוד ובקרת תהליכים

3.18.6.1. הספק יתעד את כל שלבי ניהול הסיכונים בצורה מפורטת, כולל זיהוי, הערכה, טיפול ובקרה.

3.18.6.2. על הספק להפעיל מנגנונים לבקרת איכות ולסקירה תקופתית של התיעוד, לפחות אחת לשנה.

3.18.6.3. תיעוד זה ייבחן על ידי גורם חיצוני או פנימי המאושר על ידי המזמין, לצורך אימות אפקטיביות התהליך.

3.18.7. הכשרת צוותים ובעלי עניין

3.18.7.1. הספק יבטיח הכשרות שוטפות לצוותי התפעול והניהול, המתמקדות בניהול סיכונים, זיהוי איומים והפעלת מנגנוני תגובה.

3.18.7.2. ההכשרות יתבצעו בהתאם לשינויים טכנולוגיים ורגולטוריים, ויכללו סימולציות להתמודדות עם תרחישי קצה.

3.18.8. התאמה לדרישות רגולטוריות

3.18.8.1. תהליכי ניהול הסיכונים יעמדו בדרישות הרגולטוריות שנקבעו על ידי הרשות או כל גוף פיקוח רלוונטי אחר.

3.18.8.2. על הספק להבטיח עדכון המדיניות והתהליכים בהתאם לשינויים רגולטוריים, כולל בחינה שוטפת של עמידה בדרישות אלו.

3.19. אנשים ותהליכים

3.19.1. תקשורת ושיתוף ידע

3.19.1.1. הספק יפרט את התהליכים והנהלים לשיתוף ידע בין הצוותים הטכנולוגיים, תוך הבטחת זרימת מידע חלקה ואפקטיבית.

3.19.1.2. יש לפרט את האמצעים והנהלים לשיפור תקשורת בין צוותים ובין יחידות טכנולוגיות שונות בארגון.

3.19.1.3. הספק יציג אמצעים להטמעת תרבות ארגונית המקדמת שיתוף פעולה, העצמת עובדים ואחריות אישית.

3.19.1.4. יש להציג שיטות ואמצעים להטמעת תחושת אחריות אישית אצל עובדי הטכנולוגיה, כגון:

3.19.1.4.1. מנגנוני דיווח שוטפים.

3.19.1.4.2. תהליכי מעקב אחר ביצועים אישיים.

3.19.2. אבטחת מידע וכוח אדם

3.19.2.1. בהתאם לדרישות המפורטות בפרק 4 אבטחת מידע, על הספק להציג את הנהלים לניהול כוח אדם בהיבטי אבטחת מידע.

3.19.2.2. יש לפרט אמצעים לניהול ובקרה על כוח אדם בתהליכים רגישים, כולל:

3.19.2.2.1. סינון ובדיקות רקע של מועמדים לתפקידים קריטיים.

3.19.2.2.2. מנגנוני ניטור ובקרה של פעולות עובדים בתהליכים קריטיים.

3.19.2.2.3. מנגנונים לזיהוי והתמודדות עם מעילות או חשדות לפעילות זדונית.

3.19.2.3. יש להציג את הנהלים הנוגעים לשימוש בציוד קצה, כולל:

3.19.2.3.1. ניהול גישה לציוד קצה ותשתיות רגישות.

3.19.2.3.2. אמצעים לזיהוי עובדים והזדהותם מול רשת הארגון.

3.19.2.4. נהלי גישה מרחוק יכללו בקרות גישה מבוססות תפקידים והגבלות מפורטות על פעילויות שאינן נדרשות לתפקיד.

3.19.2.5. יש להגדיר נהלים לחופשות מרכזות ורוטציות תפקידים, במטרה להפחית סיכונים הקשורים לשחיקה ולריכוזיות ידע.

3.19.3. התאמה לדרישות רגולטוריות

3.19.3.1. הספק יתחייב לעמוד בכל דרישות הרשות בהיבטי ניהול כוח אדם.

3.19.3.2. על הספק להבטיח עדכון הנהלים ותהליכי העבודה בהתאמה לשינויים רגולטוריים ולצרכי הארגון.

3.20. מעבר מדורג מכספות לממשקי API

3.20.1. עקרונות כלליים

3.20.1.1. פרק זה מגדיר את הכלים הטכנולוגיים והאילוצים הדרושים לתקופת המעבר מטכנולוגיית כספות לטכנולוגיה של **API**.

3.20.1.2. מטרת הפרק היא לאפשר לספק לנהל את המעבר בצורה מדורגת ויעילה, תוך שמירה על זמינות מלאה של השירותים והתאמה לדרישות המערכת והרגולציה.

תכנית העבודה ולוחות הזמנים למעבר מפורטים בפרק 5 המימוש.

3.20.2. ניהול השינוי הטכנולוגי

3.20.2.1. על הספק הזוכה לפרט את הגישה לניהול שינוי טכנולוגי במהלך התקופה בה ייעשה שימוש בשתי הטכנולוגיות להעברת מידע במקביל (להלן: "תקופת הביניים"), תוך התמקדות בנקודות הבאות:

3.20.2.1.1. מנגנונים להבטחת זמינות שירותים בסביבת הכספות ובסביבת ממשקי **API** בו-זמנית.

3.20.2.1.2. תהליך עדכון ובדיקת תוכנות ושירותים המשפיעים על תפקוד המערכת בשתי הסביבות.

3.20.2.1.3. בקרות טכנולוגיות למניעת שיבושים במהלך המעבר.

3.20.3. כלים וטכנולוגיות ייעודיים לתקופת הביניים

3.20.3.1. הספק יפרט את הכלים והתהליכים הנדרשים לתקופת הביניים, הכוללים:

3.20.3.1.1. כלי מיגרציה להעברת נתונים בצורה מאובטחת ואמינה בין הכספות לטכנולוגית **API**.

3.20.3.1.2. כלי בדיקות ייעודיים לבדיקת תקינות הנתונים והתאמתם לאחר המיגרציה.

3.20.3.1.3. פתרונות לניטור ובקרה משולבים (**Aggregated Monitoring**), המאפשרים תצוגה מאוחדת של מצב כל רכיבי המערכת, כולל כספות, **API**, תשתיות נתונים ורשתות.

3.20.3.1.4. כלים לניהול גרסאות במקביל לשינויים טכנולוגיים ותפעוליים.

3.20.3.1.5. פתרונות תיעוד אוטומטיים המבטיחים שמירה על עקיבות תפעולית ומידע על פעולות שבוצעו במהלך תקופת המעבר.

3.20.4. תקופת הרצה ואינטגרציה

3.20.4.1. הספק יפרט את המשמעויות הטכנולוגיות של הרצה במקביל, ככל שתידרש, כולל:

3.20.4.1.1. שמירה על תפקוד מלא של שירותי הכספות וממשקי **API** במהלך תקופת ההרצה.

3.20.4.1.2. שימוש בכלי בדיקות עומסים וביצועים להבטחת יציבות המערכת בכל אחת מהסביבות.

3.20.4.1.3. ניהול נתונים כפול, כולל סנכרון נתונים בין הסביבות, במידת הצורך.

3.20.4.1.4. מנגנוני ניטור בזמן אמת לתקלות בשתי הסביבות ותהליכי תגובה מהירים.

3.20.5. בדיקות קבלה מול גופים מעורבים

3.20.5.1. על הספק להגדיר תהליך ברור לבדיקות קבלה מול גופים מוסדיים ומערכות צד ג', הכולל:

3.20.5.1.1. מנגנוני בדיקה לממשקי **API** קיימים וחדשים.

3.20.5.1.2. התאמת שירותים טכנולוגיים לצרכים העסקיים של השותפים, תוך שימוש בכלי בדיקות ייעודיים.

3.20.5.1.3. דיווח בזמן אמת על בעיות תאימות טכנולוגית ומתן פתרונות מיידיים.

3.20.5.1.4. הדרכה ושיתוף פעולה עם הגופים המעורבים בתקופת המעבר, במידת הצורך.

3.20.6. ניהול סיכונים בתהליך המיגרציה

3.20.6.1. הספק יתחייב לבנות ולהפעיל תוכנית ניהול סיכונים ייעודית לתקופת המיגרציה, שתכלול:

3.20.6.1.1. מנגנוני זיהוי מוקדם של כשלי מיגרציה ותהליכי תגובה מובנים.

3.20.6.1.2. שיטות לניהול ומעקב אחר סיכונים לאורך כל שלבי המעבר.

3.20.6.1.3. בקרות המיועדות לצמצום סיכונים הקשורים להעברת נתונים, זמינות המערכת ושירותי הממשקים.

3.20.7. תוכנית חזרה לאחור

3.20.7.1. הספק יכין תוכנית חזרה לתצורת הכספות, שתופעל במקרים חריגים שבהם המעבר לממשקי **API** לא יאפשר עמידה בדרישות השירות.

3.20.7.2. התוכנית תכלול:

3.20.7.2.1. מנגנונים לחזרה מיידית לתצורה הקודמת ללא פגיעה במידע או בשירותים.

3.20.7.2.2. תהליך מובנה לבחינת תקינות הכספות לאחר חזרה לאחור.

3.20.7.2.3. צעדים לאבחון וטיפול בתקלות שאינן מאפשרות את המשך המיגרציה, לצד שיפור בתוכנית העתידית.

פרק 4 – אבטחת מידע, הגנת הפרטיות והמשכיות עסקית

4.1. כללי

4.1.1. הפעלת מערכת הסליקה ופיתוחה, כפופות להוראות חוק הגנת הפרטיות התשמ"א-1981 ותקנותיו ובכלל זה תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, להוראות חוק הייעוץ הפנסיוני ולתקנות אבטחת מידע. ההוראות הקבועות בפרק זה לעניין אבטחת המידע המועבר או השמור במערכת הסליקה יחולו למעט במקרה של סתירה עם הוראות הדין.

4.1.2. באחריות הספק להשתמש בכל אמצעי אבטחת המידע הנדרשים על מנת להבטיח את סודיות המידע המועבר באמצעות מערכת הסליקה או השמור בה, למנוע זליגת מידע מהמערכת לגורם בלתי מורשה, למנוע כל שימוש לבד ממטרותיו על פי כל דין ועל פי תנאי המכרז ולמנוע מניעת שירותים והשבתה ממושכת.

4.1.3. הספק מתחייב להגדיר לכל הפחות את המסמכים הבאים וכמפורט להלן בהמשך פרק זה. ויובהר כי לממונה תהיה זכות ולדרוש לערוך בהם שינוי:

- מדיניות אבטחת מידע וניהול סיכוני סייבר;
- נוהל/נהלי אבטחת מידע;
- מסמך מיפוי וסיווג נכסי מידע אשר יכלול לכל הפחות התייחסות למערכות הפעלה, אפליקציות וקטעי קוד פתוח בהם משתמש הספק;
- תכנית עבודה שנתית להגנת הפרטיות, סייבר ואבטחת מידע לרבות העלאת מודעות עובדים;
- נוהל מוכנות לאירועי סייבר;
- מסמך המתאר את ארכיטקטורת אבטחת המידע המוצעת במערכת הסליקה;
- מסמך המתאר את אמצעי האבטחה הפיזית המוצעים במערכת הסליקה;
- נוהל או מסמכים נוספים בתחום אבטחת המידע והגנת הפרטיות בהתאם לדרישת הממונה.

4.1.4. הספק מתחייב לערוך את הסקרים הבאים, כמפורט להלן בהמשך פרק זה:

- סקר הגנה על הפרטיות;
- סקר סיכוני סייבר באמצעות גורם חיצוני בלתי תלוי;
- מבדקי חדירה באמצעות גורם חיצוני בלתי תלוי אשר יכללו, בין היתר, מבדקי חדירות אפליקטיביות ותשתיתיות.

4.2. עקרונות אבטחת מידע והגנת הסייבר

4.2.1. על הספק ליישם עקרונות אבטחת מידע וסייבר על פי תורת הגנת הסייבר המודרנית. עקרונות אלו מבוססים על שיטות עבודה מתקדמות המיועדות להתמודד עם איומים במערכות קריטיות. העקרונות המרכזיים כוללים:

- <u>אחריות הנהלה</u> - הנהלת הספק תשאנה באחריות כוללת להטמעת תהליכי אבטחת מידע וסייבר, תוך הגדרת תפקידים ברורים, הקצאת משאבים ומנגנוני בקרה[2].
- <u>הגנה מבוססת סיכון</u> - ההשקעה באבטחת המידע תתבצע בהתאם לרמת הקריטיות של כל נכס ולפוטנציאל הנזק הנובע מאובדן סודיות, שלמות או זמינות.
- <u>הגנה רב-ממדית</u> - ייושם דגש על שילוב של שלושה מרכיבים: אנשים (הכשרת צוותים), תהליכים (נהלים ומדיניות) וטכנולוגיה (שימוש בכלים מתקדמים).
- <u>הגנה פרואקטיבית</u> - יוטמעו בקרות שמטרתן למנוע איומים פוטנציאליים, לזהות חדירות בזמן אמת (סריקת חולשות עיתית) ולספק תגובה מהירה לשיקום המערכת.
- <u>שמירה על דינמיות</u> - מערכת האבטחה תהיה גמישה ותתעדכן בהתאם לשינויים בסביבה הטכנולוגית ולאיומים חדשים שמתגלים.
- <u>שימוש במידע מודיעיני</u> - הטמעת תהליכים מבוססי ידע וניסיון מתעשיית הסייבר, לרבות ניתוח איומים עכשוויים ושימוש במידע מודיעיני ממערכות ניטור מתקדמות.

4.2.2. באחריות הספק לוודא כי מערכות החומרה והתוכנה המשמשות לצורך הפעלת מערכת הסליקה מהימנות, מקנות רמה גבוהה של זמינות ואמינות, ומעניקות הגנה נאותה מפני גישה לא מורשית (לרבות חדירה וגישה שלא בהתאם להרשאות הגישה של גורם פנימי), מניעת גישה, שיבוש, הפרעה, הונאה או גרימת נזק למחשב או לחומר מחשב כהגדרתם בחוק המחשבים, בהתחשב ברגישות המידע.

4.2.3. באחריות הספק לוודא כי כל תוכנת תשתית (קרי – תוכנת מדף, שלא פותחה ייעודית עבור הספק) שתשולב במערכת, אינה גורמת לנזק ממשי או לנזק באבטחת מידע ותסופק כשהיא בגרסתה המקורית, על גבי מדיה מקורית שהונפקה ע"י היצרן, או באמצעות טעינה ישירה מאתר היצרן (בכפוף לבדיקת **HASH** תקין). השימוש בתוכנה יתאפשר רק במהלך התקופה בה התוכנה נתמכת על-ידי היצרן.

4.2.4. באחריות הספק להבטיח את קיומם של אמצעים לאבטחת המידע המועבר במערכת הסליקה ולניהול סיכונים הקיימים או העלולים להתקיים במערכת, למניעתם, ככל האפשר, או להגבלתם. לשם כך, הספק ומערכת הסליקה יעמדו

[2] להרחבה, ראו הנחיית הרשות להגנת הפרטיות בנושא תפקיד הדירקטוריון בקיום חובות החברה לפי תקנות הגנת הפרטיות (אבטחת מידע).

במבחני הסמכה לפי תקן ISO 27001 של מכון התקנים או לפי תקן מקביל של מי שאושר לעניין זה לפי סעיף 12 לחוק התקנים.

4.2.5. הספק מתחייב לעמוד בכל התקנים הקבועים בפרק זה ולעדכן אותם בהתאם למקובל בשוק כפי שיהיה מעת לעת.

4.3. מדיניות אבטחת מידע וניהול סיכוני סייבר

4.3.1. הספק יגדיר את מדיניות אבטחת המידע וניהול סיכוני הסייבר במערכת הסליקה במסמך אשר יתייחס לכל הדרישות המובאות בחוק הגנת הפרטיות ותקנות אבטחת מידע, בחוק הייעוץ הפנסיוני ותקנותיו ובהוראות חוזר ניהול סיכוני סייבר.

4.3.2. מסמך מדיניות אבטחת המידע וניהול סיכוני הסייבר, יומצא על ידי הספק ויועבר לעיון הממונה בשלב ההקמה.

4.3.3. הספק יטמיע מדיניות ותהליכים מותאמים לזיהוי, ניתוח ומענה לסיכוני סייבר משתנים בסביבה הדינמית שבה פועלת המערכת. תהליכים אלו יבטיחו את יכולת המערכת להתמודד עם איומים חדשים ומתפתחים, תוך הפחתת הסיכון למתקפות והשפעותיהן.

4.3.4. הספק יבצע תהליך בחינה ועדכון של מסמך מדיניות אבטחת המידע וניהול סיכוני הסייבר בהתאם לשינויים במדיניות, לשינויים בהערכת הסיכונים ולשינויים טכנולוגיים או שינויים מהותיים במערכת הסליקה ולכל הפחות אחת ל- 12 חודשים ובהתאם לדרישת הממונה.

4.4. ניהול סיכונים דינמיים

4.4.1. <u>זיהוי סיכונים מתפתחים</u>

4.4.1.1. מעקב אחר איומים גלובליים:

הספק יבצע ניטור רציף של מקורות מידע גלובליים על איומים, כגון מתקפות ממוקדות על מערכות פיננסיות או פרצות חדשות בתשתיות טכנולוגיות.

4.4.1.2. מנגנוני זיהוי מוקדם:

הספק יעשה שימוש במערכות מבוססות בינה מלאכותית (AI) ולמידת מכונה (ML) לזיהוי מוקדם של תבניות פעילות חריגה במערכות המערכת. למען הסר ספק, מערכות כאמור יהיו פנימיות ולא יחצינו מידע לגורמים חיצוניים.

4.4.1.3. שיתוף מידע עם גורמי רגולציה וסייבר:

הספק יבחן השתתפות במאגרי מידע ושיתוף פעולה עם רגולטורים וגופים מקצועיים לזיהוי מהיר של איומים המכוונים למגזר הפיננסי.

4.4.2. עדכון שוטף של מדיניות האבטחה

4.4.2.1. סקירה תקופתית של מדיניות אבטחת המידע:

הספק יבצע סקירה תקופתית של מדיניות האבטחה כדי לוודא את התאמתה לאיומים החדשים ולשינויים בסביבה העסקית והטכנולוגית.

4.4.2.2. הטמעת שינויים נדרשים:

הספק יישם שינויים במדיניות האבטחה, בהתאם לאיומים שהתגלו.

4.4.3. תהליכי ניהול תגובה

4.4.3.1. תוכנית תגובה לאיומים חדשים:

הספק יגדיר נהלים ברורים להתמודדות עם איומים חדשים או מתפתחים, כולל חלוקת אחריות בין צוותים, לוחות זמנים לתגובה ואמצעי חירום.

4.4.4. סימולציות ותהליכי למידה:

4.4.4.1. הספק יערוך סימולציות תקופתיות של תרחישי תקיפה עדכניים כדי לבחון את יכולת המענה של המערכת.

4.4.4.2. הספק יבצע ניתוח מקרים קודמים (**Post-Mortem**) להפקת לקחים ושיפור יכולות המענה.

4.4.5. שימוש בטכנולוגיות מתקדמות

4.4.5.1. הספק יטמיע מערכות ניטור מתקדמות המסוגלות לזהות מתקפות סייבר חדשות בזמן אמת ולהתריע בפני גורמי האבטחה.

4.4.6. יישום הגנה פרואקטיבית- הספק

4.4.6.1. הספק יעשה שימוש בכלים פרואקטיביים כגון חומות אש חכמות, סינון קוד זדוני ומנגנוני זיהוי התנהגות חשודה (**UEBA - User and Entity Behavior Analytics**).

4.4.7. ניהול ועדכון תשתיות ותהליכים

4.4.7.1. בחינה מחזורית של תשתיות טכנולוגיות- הספק יבצע בדיקות תקופתיות למערכות הסליקה לאיתור חולשות והטמעת תיקונים נדרשים.

4.4.7.2. ניהול מחזור חיים של רכיבי תוכנה וחומרה- הספק יעדכן באופן שוטף את רכיבי התוכנה והחומרה לשחרור גרסאות חדשות, יסגור פרצות אבטחה וירחיב את יכולות ההגנה.

4.4.8. הכשרת צוותים וניהול ידע- הספק יבצע הדרכות ועדכונים מקצועיים לצוות העובדי של מערכת הסליקה בנוגע לאיומים חדשים וטכנולוגיות הגנה מתקדמות.

4.4.9. ניהול מרכז ידע ארגוני:

4.4.9.1. הספק ייצר מאגר מידע פנים-ארגוני המכיל דוגמהות לאיומים חדשים, פתרונות יישומיים, ונהלים מעודכנים להתמודדות עם סיכונים משתנים.

4.4.9.2. הספק יוודא באמצעות תהליכים אלו שמערכת הסליקה תישאר עמידה וגמישה בפני איומים משתנים, תוך שיפור מתמיד של מנגנוני ההגנה ותאימות לסטנדרטים המחמירים ביותר.

4.4.9.3. הספק יטמיע תהליך ידני או ממוכן לסיווג המידע בארגון (**Data Classification**) כגון: מידע אישי, מידע אישי בעל רגישות מיוחדת, מידע עסקי רגיש, מידע פומבי.

4.5. הערכת סיכוני סייבר ופרטיות

על הספק ליישם תהליך מחזורי להערכת סיכוני סייבר, המאפשר זיהוי, ניתוח וטיפול מתמשך באיומים קיימים ומתפתחים. תהליך זה יבטיח עדכניות וגמישות בהתמודדות עם שינויים טכנולוגיים ועסקיים, תוך הפחתת החשיפה לסיכונים. התהליך יכלול את השלבים הבאים:

4.5.1. שלב זיהוי הסיכונים

4.5.1.1. מיפוי ותיעוד נכסים ותהליכים קריטיים- זיהוי כל הנכסים הקריטיים והתהליכים העסקיים של המערכת, כולל מערכות מידע, ובכלל זה מאגרי המידע, תשתיות פיזיות וקשרים עם ספקי משנה.

4.5.1.2. הטמעת מערכות **CTI Solution** לניטור מודיעין איומי סייבר אל מול מיפוי ותיעוד הנכסים.

4.5.1.3. מיפוי ממשקים פנימיים וחיצוניים- זיהוי נקודות גישה ותקשורת בין מערכות המערכת לבין גורמים פנימיים וחיצוניים, כגון ספקים, שירותי ענן ורשויות רגולציה.

4.5.1.4. הערכת תלות בנכסים חיצוניים- זיהוי נכסים שמנוהלים על ידי ספקי צד שלישי, ניתוח התלות בהם והערכת השפעתם על המערכת במקרה של כשל או פגיעה[3].

4.5.2. שלב ניתוח הסיכונים

[3] על התקשרות עם ספק לעמוד בתנאים הקבועים בתקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017. להרחבה, ראו מדריך פעולה להתקשרות עם ספקי מיקור חוץ - תקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע).

4.5.2.1. הערכת פוטנציאל הנזק- ניתוח ההשפעות האפשריות של כל סיכון על זמינות המערכת, סודיות ושלמות הנתונים, והשלכות כלכליות ותפעוליות.

4.5.2.2. מדידת הסבירות למימוש סיכון- הערכת ההסתברות להתממשות הסיכון, תוך התחשבות במידע מודיעיני, תקריות עבר וסביבות טכנולוגיות.

4.5.2.3. חישוב רמת סיכון כוללת- שילוב בין פוטנציאל הנזק לסבירות למימוש, במטרה להגדיר את רמת הקריטיות של כל סיכון.

4.5.3. <u>שלב עדכון הבקרות</u>

4.5.3.1. יישום בקרות מותאמות- עדכון ושדרוג הבקרות הקיימות בהתאם לממצאי הערכת הסיכונים, כולל אמצעים טכנולוגיים, תהליכיים ואנושיים.

4.5.3.2. סגירת פערי אבטחה- טיפול בממצאים קריטיים ותיעדוף יישום בקרות המפחיתות את רמת החשיפה לסיכונים.

4.5.3.3. מעקב אחר ביצועי הבקרות- ניטור רציף של האפקטיביות של הבקרות שהוטמעו ועדכונן במידת הצורך.

4.5.4. <u>שלב הבקרה והמעקב</u>

4.5.4.1. בדיקות תקופתיות- ביצוע סקרי סיכונים מחזוריים לפחות פעם בשנה, או בתגובה לאירוע סייבר משמעותי או שינוי טכנולוגי.

4.5.4.2. מעקב ודיווח להנהלה- הפקת דוחות מסכמים להנהלה על ממצאי הערכות הסיכון והפעולות שננקטו בעקבותיהם.

4.5.4.3. שימוש במערכות לניהול סיכונים (**ERM**)- שילוב מערכות לניהול סיכונים ארגוניים לניטור ומעקב מתמיד אחר רמת החשיפה לסיכונים.

4.5.5. <u>שלב התכנון העתידי</u>

4.5.5.1. בניית תכנית עבודה לסגירת פערים- גיבוש תכנית מפורטת הכוללת לוחות זמנים, משאבים נדרשים ואחראים לביצוע פעולות מתקנות.

4.5.5.2. שיפור מתמיד- שילוב לקחים מהערכת הסיכונים המחזורית בתכנון האסטרטגי של המערכת, במטרה לשפר את עמידות המערכת לאורך זמן.

4.6. תכנון המשכיות עסקית והתאוששות מאסון

4.6.1. הספק יגדיר מסגרת עבודה לניהול המשכיות עסקית אשר תכלול: (א) ניתוח סיכונים אליהם הוא חשוף בקרות תרחיש ייחוס, לרבות ניתוח תוצאות, השלכות

ומשמעויות עסקיות, (ב) הגדרת תהליכים ושירותים חיוניים בפעילות העסקית, (ג) קביעת יעדי שירות למצב חירום ויעדי התאוששות, לרבות רמות התאוששות וזמני התאוששות צפויים, בהתאם ליעדי השירות והזמינות שהוגדרו בפרק 6 **SLA** (ד) בניית תכנית להמשכיות עסקית תוך התייחסות לתפקידים ותחומי אחריות של גורמים שונים בניהול מצב חירום וקיום התכנית בפועל וכן התייחסות לאופן ההתאוששות מאסון של הספק, (ה) הטמעת התכנית להמשכיות עסקית.

4.6.2. <u>תוכניות גיבוי ושחזור</u> - על הספק להטמיע תוכניות גיבוי ושחזור נתונים ברמה הגבוהה ביותר, המבטיחות זמינות מלאה של נתוני מערכת הסליקה גם במצבי חירום. התוכניות יכללו קביעת פרמטרים ברורים של **RTO (Recovery Time Objective)** ו-**RPO (Recovery Point Objective)**, המגדירים את זמן ההתאוששות המרבי המותר ואת רמת הנתונים המקסימלית שאינה ניתנת לשחזור במקרה של כשל וכל זאת בהתאם להוראות הממונה כפי שיעודכנו מעת לעת. תוכניות אלו ייבחנו באופן תקופתי באמצעות בדיקות יעילות ייעודיות, המדמות תרחישי משבר ומאפשרות וידוא של יכולת ההתאוששות בזמן ובדיוק הנדרשים. כמו כן, על הספק לעדכן את תוכניות הגיבוי והשחזור על בסיס לקחים מהבדיקות התקופתיות, שינויים טכנולוגיים או איומים שהתגלו, במטרה להבטיח את התאמתן המלאה לסביבה הדינמית שבה פועלת מערכת הסליקה.

4.6.3. <u>התאוששות בזמני חירום</u> - על הספק להבטיח תכנון ושמירה על תפקוד מערכות קריטיות של מערכת הסליקה בזמני חירום, בין אם מדובר באירועי סייבר, תקלות טכנולוגיות או משברים סביבתיים. תכנון זה יכלול הקצאת משאבים ייעודיים שיאפשרו המשכיות תפקודית ללא פגיעה בשלמות הנתונים או בזמינותם. על הספק לוודא שכל הרכיבים הקריטיים, כגון מערכות מידע, תשתיות ענן ותהליכי עיבוד נתונים, ימשיכו לפעול בצורה תקינה, תוך העדפה לפתרונות חלופיים המיועדים לגיבוי מערכות במקרה של כשל כולל. יש לתעד את כל תהליכי ההתאוששות, לרבות המנגנונים המשמשים להחזרת המערכות לפעולה מלאה, ולהבטיח כי הצוותים המעורבים מיומנים בביצועם.

4.6.4. <u>ניתוח השפעה עסקית (**BIA**)</u> - כחלק בלתי נפרד מתכנון המשכיות עסקית, על הספק לבצע ניתוח השפעה עסקית (**BIA**) מעמיק, שמטרתו להעריך את ההשלכות הפוטנציאליות של אירועי כשל או משבר על פעילות המערכת. הניתוח יזהה את התהליכים והמערכות הקריטיות ביותר, יכמת את הנזקים האפשריים כתוצאה מהפסקת פעילותם, ויתעדף את סדרי העדיפויות בהגנה עליהם. **BIA** ישמש כלי מרכזי לתכנון משאבים ותהליכים שיבטיחו מענה מיטבי בתרחישי חירום, תוך התמקדות במניעת נזקים עסקיים משמעותיים. ניתוח זה יבוצע לפחות אחת לשנה או במקרים של שינויים משמעותיים בסביבת הפעילות (המוקדם מבניהם), והתוצאות יוטמעו בתוכניות המשכיות עסקית והתאוששות מאסון, כדי להבטיח עמידות ותפקוד רציף של המערכת.

4.7. הגנת הפרטיות (עיצוב לפרטיות)

4.7.1. הספק יבטיח כי המערכת הטכנולוגית שתשמש את מערכת הסליקה תמזער, ככל הניתן ובשים לב לחלופות טכנולוגיות מקובלות, את הסיכון לפגיעה בפרטיות הלקוחות, בהתאם לחוק הגנת הפרטיות, תקנות אבטחת מידע והוראות סעיף 31טז בחוק הייעוץ הפנסיוני.

4.7.2. הספק יערוך תסקיר השפעה על הפרטיות שיכלול סקר סיכוני אבטחת מידע בדגש על המידע האישי המועבר במערכת הסליקה בהתאם לתקנות הגנת הפרטיות (אבטחת מידע) והוראות הרשות להגנת הפרטיות כפי שיתנו מעת לעת.

4.7.3. הספק ישתף פעולה עם כללי שלבי אישור תסקיר הגנה על הפרטיות, לרבות הליכי ההתייעצות להם יידרש הממונה עם הרשות להגנת הפרטיות במשרד המשפטים.

4.7.4. תסקיר השפעה על הפרטיות יערך במתכונת כפי שפורסמה על ידי רשות הגנת הפרטיות לביצוע תסקיר כאמור בלינק שלהלן.. התסקיר יכלול, לכל הפחות, את השלבים הבאים:

שלב 1: קבלת החלטה על ביצוע תסקיר השפעה על הפרטיות.
שלב 2: תיאור כללי של פעילויות עיבוד המידע.
שלב 3: התייעצויות עם בעלי העניין (ככל שרלוונטי).
שלב 4: הערכת החוקיות, הצורך והמידתיות של פעולת עיבוד המידע.
שלב 5: זיהוי והערכת הסיכונים לפגיעה בפרטיות.
שלב 6: זיהוי אמצעים לצמצום הסיכונים שאותרו.
שלב 7: תיקוף ואישור התסקיר.

4.7.5. הספק יפעל בהתאם להוראות לעניין סודיות ואבטחת מידע כאמור בסימן ד' לפרק ה'1 לחוק הייעוץ הפנסיוני ולהוראות לשמירת מידע כאמור בפרק ג' לתקנות אבטחת מידע. מבלי לגרוע מהאמור, הספק יפעיל מנגנון ארגוני וטכנולוגי שמטרתו להבטיח כי הספק פועל לפי עקרון "צמצום המידע", ובכלל זאת מעביר את המידע המינימלי הנדרש לביצוע הפעולה, ואינו מחזיק מידע עודף מעבר למידע ולסוגי המידע המינימליים הנדרשים למתן השירותים לפי מכרז זה ולביצוע הפעולות המפורטות בסעיף 31ט לחוק הייעוץ הפנסיוני ופעולות הבקרה על המידע לפי סעיף 31טז לחוק.

4.7.6. הספק יפעיל מנגנון ארגוני וטכנולוגי שמטרתו להבטיח כי המידע המוחזק על ידו נכון, שלם, ברור ומעודכן. מצא הספק, על סמך המנגנון כאמור, כי מוחזק מידע שאינו נכון, שלם, ברור או מעודכן, ינקוט בכל האמצעים הנדרשים לצורך תיקון המידע או מחיקתו.

4.7.7. הספק ירשום את מאגרי המידע בהתאם לחוק הגנת הפרטיות ותקנותיו.

4.7.8. כחלק מהבקרות שיש לבצע בסעיף "אבטחת שרשרת אספקה ומיקור חוץ" במכרז זה, הספק נדרש לבחון את עמידת ספקי מיקור חוץ בדרישות הגנת הפרטיות והכל בכפוף להוראות הרלוונטיות לספקי משנה בפרק 5 המימוש.

4.8. מבדקי חוסן (חדירה)

4.8.1. הספק יערוך מבדקי חוסן על ידי גורם חיצוני בלתי תלוי המתמחה בביצוע מבדקי חוסן. הספק יוכל לערוך את המבדקים על ידי אותו גורם חיצוני לכל היותר לגבי שתי בדיקות ברצף.

4.8.2. המבדקים יכללו בין השאר, מבחני חדירה ברמה תשתיתית ואפליקטיבית; מבדקים המדמים ניסיון תקיפה מרשתות חיצוניות (כגון רשת האינטרנט, חיבור לספקים או שותפים עסקיים) ורשתות פנימיות; בדיקות הנדסה חברתית; בחינת היכולת להחדרת תוכנות עוינת וגילויה ע"י מערכות הבקרה; התחזות ופישינג, הן על ידי משתמש והן על ידי מי שאינו מזוהה כמשתמש, בשיטות **Black Box** ו-**White Box** לפחות.

4.8.3. המבדקים יבוצעו על פי מתודולוגיות בדיקה מקובלות **Best Practice** (למשל **OWASP, NIST SP 800-115**).

4.8.4. הממונה רשאי להעביר טרם ביצוע הסקר דגשים לביצוע הסקר בהתאם למקובל בשוק ולהתפתחויות. באחריות הספק לפנות למפקח הפרויקט טרם ביצוע הסקר לקבלת הדגשים.

4.8.5. כל גרסה חדשה תכלול בדיקת קוד מאובטח כתנאי להפעלתה תוך יישום עקרונות פיתוח מאובטח. בכל פיתוח חיצוני או פנימי יתועדו קטעי הקוד הפתוח לצורך תחזוקה[4]

4.8.6. מבדקי חדירה מלאים הכוללים את כל תשתיות ומערכות מערכת הסליקה יערכו בכל 12 חודשים וכן לפני הטמעת שינויים טכנולוגיים משמעותיים ו/או הפעלת שרות חדש מהותי כגון הפעלת ממשק במסגרת חוזר מבנה אחיד להעברת מידע ונתונים בשוק החיסכון הפנסיוני, לרבות השלמת שלבי ההקמה של המערכת ותכונות נוספות במערכות. .

4.8.7. תוצאות המבדק ותוכנית להפחתת הסיכונים שעלו יועברו לממונה על הפרטיות ולממונה על אבטחת המידע, מנכ"ל הספק (ומנהל הפרויקט), לתיקון הליקויים שנתגלו במסגרת המבדק, ככל שנתגלו. הצגה זו תכלול, לכל הפחות, פירוט סיכונים שיוריים, תכנית הפחתת סיכונים ופירוט הסיכונים המשמעותיים שהספק החליט שלא להפחית לרמה מזערית ככל שניתן.

4.8.8. ליקויים קריטיים שנתגלו במבדקי החוסן, ותכנית העבודה לטיפול בליקויים ידווחו לממונה ויתוקנו באופן מידי ולא יאוחר מ- מ-7 ימי עסקים המועד שבו נתקבלו אצל הספק. במקרה בו הליקוי הקריטי לא נתן לטיפול מידי ולכל היותר עד 7 ימי עסקים מיום שנודע על הממצא במסגרת הסקר. הספק יבחן בקרות מפצות להקטנת הסיכון שיוצר הליקוי הקריטי ועד לתיקונו הספק ידווח למפקח הפרויקט על ממצא כאמור, והממונה יהיה רשאי לקצר את לוחות הזמנים לטיפול בממצא.

[4] למידע נוסף בנוגע לקוד הפתוח וחובת התיעוד - ניתן לעיין במסמך שפרסמה הרשות לעניין זה: עקרונות לניהול סיכוני אבטחת מידע בעת שימוש בקוד פתוח במערכות המאגר.

4.9. ניטור, תגובה וניהול אירועי סייבר

4.9.1. מרכז ניטור (SOC): על הספק להקים ולהפעיל מרכז ניטור אבטחת סייבר **SOC (Security Operations Center)**, שמטרתו לנטר את פעילות המערכת בזמן אמת ולנתח לוגים ותעבורת נתונים באופן שוטף. המרכז יכלול את המרכיבים הבאים:

4.9.1.1. ניטור בזמן אמת של כלל רכיבי המערכת, כולל שרתים, תחנות עבודה, רשתות וסביבות ענן, לזיהוי פעילות חשודה או חריגה (אנומליות).

4.9.1.2. שימוש בטכנולוגיות מתקדמות כגון **SIEM (Security Information and Event Management)** ו- **UEBA (User and Entity Behavior Analytics)** לאיסוף וניתוח אירועים.

4.9.1.3. הקפדה על שמירת לוגים לתקופה שנקבעה מראש בהתאם לדרישות רגולטוריות, תוך אבטחתם מפני שינוי או גישה לא מורשית.

4.9.1.4. הפעלת צוותים ייעודיים לניתוח אירועים חריגים והעברת המידע לצוותי תגובה תוך זמן קצר.

4.9.2. תוכנית ניהול אירועים - על הספק להטמיע תוכנית לניהול אירועי סייבר, שתספק תהליך ברור ומובנה לטיפול באירועים, החל מזיהוי ראשוני ועד לשיקום המערכת. התוכנית תכלול:

4.9.2.1. תהליך זיהוי ותגובה:

4.9.2.1.1. הגדרת מדדים **(KPIs)** לאיתור איומים ומעקב אחר התקדמות הטיפול באירועים.

4.9.2.1.2. קביעת תרחישים ידועים מראש **(Use Cases)** לטיפול באירועים מסוגים שונים, כולל מתקפות מניעת שירות **(DDoS)**, פריצות לחשבונות משתמשים והדלפות נתונים.

4.9.2.2. דיווח פנימי וחיצוני:

4.9.2.2.1. מנגנוני דיווח פנימיים להנהלה הבכירה ולממונה על אבטחת המידע.

4.9.2.2.2. דיווח רגולטורי בזמן אמת על אירועים חמורים, בהתאם לחוקים ולדרישות.

4.9.2.3. סימולציות ותחקירים:

4.9.2.3.1. ביצוע תרגולים וסימולציות תקופתיות להכשרת צוותים ולשיפור מוכנות לתרחישים מגוונים.

4.9.2.3.2. תחקור אירועים בסיום התהליך והפקת לקחים ליישום במדיניות האבטחה.

4.10. הגנה פרואקטיבית

כדי להקדים ולמנוע אירועי סייבר, על הספק לפעול בגישה פרואקטיבית שתכלול:

4.10.1. זיהוי מקדים של איומים:

4.10.1.1. שימוש בכלי **Threat Intelligence** לזיהוי מוקדם של איומים פוטנציאליים, המבוססים על מידע גלובלי ואירועים מקומיים.

4.10.1.2. ניטור תעבורת הרשת לזיהוי פעילות חריגה עוד לפני התממשות האיום.

4.10.1.3. חקירת מגמות על בסיס שבועי.

4.10.2. מניעה והקטנת סיכונים:

4.10.2.1. הטמעת בקרות מניעתיות, כגון מערכת לניהול הרשאות, ניהול גישה מבוסס תפקידים(**RBAC**) והצפנה חזקה (תיושם הצפנה לפי תקן **NIST FIPS 140-2/3**). לרבות שילוב פרוטוקולי הצפנה חסינים מפני מחשוב קוונטי (**Post-quantum cryptography - PQC**).

4.10.2.2. הגבלת נקודות גישה קריטיות באמצעות סגמנטציה ברשת והפרדת סביבות.

4.10.3. שיקום מהיר של המערכת:

4.10.3.1. קביעת נהלי גיבוי ושחזור שיבטיחו התאוששות מהירה לאחר מתקפה.

4.10.3.2. תיעדוף הטיפול ברכיבים קריטיים תוך שמירה על רציפות תפעולית.

4.11. ניהול משתמשים והרשאות

4.11.1. הספק יעשה שימוש בממשקי ניהול של מערכת הסליקה אשר יאפשרו הפרדת סמכויות (מדרג הרשאות) לפי השתייכות לסוגי משתמשים (פרופילים), לקוחות, קבוצות, הרשאות נקודתיות וכדומה.

4.11.2. הספק יגדיר נהלים המתייחסים לתהליך לניהול המשתמשים וההרשאות במערכות הסליקה, החל מיצירת חשבון משתמש, מתן הרשאות , נעילת החשבון בתום העסקה ובקרה אחר הביטול. כל התהליך מלווה באישורים המתאימים.

4.11.3. ממשק ניהול ההרשאות יהא במודול נפרד אשר אינו נגיש למשתמשי המערכת, למעט: הממונה על אבטחת המידע; מנהלי המערכת; ומבקרי ההרשאות, לרבות אחראי על בקרה לאחר ביצוע שינוי בידי מנהלי המערכת. בעלי התפקידים המוזכרים בסעיף זה יקבעו על ידי הספק, למעט הממונה על אבטחת המידע שיקבע בהתאם למפורט בפרק זה.

4.11.4. עובדי הספק יקבלו הרשאות אדמיניסטרציה לשרת מערכת הסליקה ככל שנדרש לשם הפעלת המערכת ותחזוקתה בלבד, אך לא יקבלו הרשאות לצפייה במידע המועבר במערכת או נשמר בה או לעדכון מידע זה.

4.11.5. המערכת תאפשר מתן הרשאות קריאה בלבד למידע שהועבר במערכת ונשמר בה למשך תקופת הביקורת, כהגדרתה בתקנות אבטחת המידע, לעובדי הספק השייכים לתחום הבקרה ואשר אינם ממלאים תפקיד אחר במערכת. ההרשאה תינתן לשם בירור מחלוקות או בקרה על פעולת המערכת.

4.11.6. הספק יגדיר לפחות שני עובדים בכירים שאישורם יידרש לשם גישה לחלקים רגישים של מערכת הסליקה ולביצוע פעולות חיוניות במערכת, כפי שהוגדרו במסמך מדיניות אבטחת המידע.

4.11.7. הרשאות גישה לעובדי מערכת הסליקה יינתנו בהתאם לסוג העובד, תפקידו, הפעולות שרשאי על פי כל דין לבצע במערכת, ובכפוף לאימות זהות העובד. ההרשאות יינתנו על בסיס עיקרון הפרדת תפקידים ועל בסיס עיקרון "צמצום גישה" (**Least Privilege**) כך שלא יתאפשר לעובד בודד לבצע מעגל עבודה שלם.

4.11.8. זיהוי ואימות העובדים במערכת הסליקה (**Authentication**) יתבצע ע"י שיוך סיסמה ומשתמש אישי לכל עובד, בכפיפות למדיניות הסיסמאות. עבור מערכות רגישות יידרש שימוש באימות רב שלבי (**Multi Factor Authentication**) על מנת לבצע התחברות למערכת. על אף האמור לעיל, במקרים בהם יש צורך בקיום חשבונות שאינם אישיים, כגון כאלה המיועדים לשימוש על ידי תהליך ממוכן, יוגדרו אמצעים מיוחדים לשמירה על סודיות אמצעי ההזדהות של החשבון, להגבלת השימוש בו ככל הניתן ויוגדר גורם האחראי על החשבון. בנוסף, תוגדר מדיניות ניהול סיסמאות סדירה במשתמשים אפליקטיביים.

4.11.9. הממונה על אבטחת המידע ינהל רישום מעודכן בכל עת של סוגי תפקידים וסוגי משתמשים, הרשאות הגישה המתאימות לכל סוג תפקיד ולכל סוג משתמש ושמות בעלי תפקידים או שמות משתמשים אלה. כמו כן, יערוך בקרה לפחות פעם ברבעון לגבי חשבונות של עובדים שעזבו, חשבונות שלא נעשה בהם שימוש במשך תקופת הרבעון, שינוי תפקיד המשתמש והרשאותיו. אחת לשנה, לכל הפחות, תתבצע סקירת הרשאות כל העובדים בה יאושר כי הרשאות העובדים תואמות את הגדרת תפקידם.

4.11.10. הרשאות הגישה של הלקוח או הגורם השלישי הפועל בשמו של הלקוח יבוטלו במקרה של שינוי במעמד הלקוח, מיד עם הבאת המידע על ביצוע השינוי לידי הספק, כמפורט להלן:

4.11.10.1. ביטול תוקף אמצעי הזיהוי המשמש לזיהוי הלקוח במערכת הסליקה.

4.11.10.2. שינוי במעמד החוקי של הלקוח או הגורם השלישי הפועל בשמו של הלקוח המחייב שינוי הרשאות הגישה שלו למערכת הסליקה.

4.11.10.3. בקשת משתמש להפסיק את פעילותו במערכת הסליקה, בכפוף להוראות כל דין.

4.11.10.4. בקשה של לקוח לבטל הרשאה של הגורם השלישי הפועל בשמו.

4.11.10.5. <u>הוראת הממונה לפטור ממתן שירות למשתמש מסוים בהתאם להוראות סעיף 31 יא(ב) לחוק הייעוץ.</u>

4.11.11. לצורך מזעור הסיכון לפגיעה בפרטיותם של הלקוחות, במקרה של הפרה של צד ג' את הוראות אבטחת המידע של מערכת הסליקה, לרבות הוראות תקנות אבטחת המידע כפי שיפורסמו לצדדי ג' שיתחברו למערכת, הספק ישעה את הרשאות הגישה של צד ג' או עובדו בכפוף להוראות כל דין. הספק יודיע לממונה בכתב בהקדם האפשרי על השעיית הרשאות הגישה כאמור, לפי העניין, עד השלמת בירור הנושא מול הלקוח ובתיאום עם הממונה.

4.12. ניהול המידע

4.12.1. העברת מידע אל נמען באמצעות מערכת הסליקה תיעשה באופן שיבטיח כי הגישה למידע והצפייה בו תתבצע על ידי מי שרשאי לכך או בהרשאתו בלבד.

4.12.2. ניהול המידע המועבר במערכת הסליקה יבוצע בהתאם להוראות תקנות אבטחת מידע, לרבות מגבלות על הגישה למידע, מועד מחיקת המידע או פרק הזמן לשמירתו, ואופן שמירת המידע בבסיס הנתונים ובטבלאות המערכת, בהתאם לסוגי המידע השונים הכוללים לפחות את אלה:

א. פרטי זיהוי של הלקוח;

ב. מידע לגבי פרטי המוצר הפנסיוני של לקוח;

ג. נתוני העברות כספים שהועברו במערכת;

ד. נתונים על העברות כספים שבוצעו והועברו מחוץ למערכת;

ה. נתונים אודות המידע כהגדרתם בתקנות 24-25 לתקנות אבטחת המידע של המערכת;

ו. נתונים לצורך גביית דמי החיבור ודמי השימוש במערכת הסליקה.

4.12.3. המידע השמור במערכת הסליקה או המועבר בה, ישמר במערכת לפרק הזמן הקצר ביותר המאפשר למערכת לבצע את הפעולות המנויות במכרז, בהתאם להוראות פרק זה ובכפוף לתקנות אבטחת מידע.

4.12.4. פרטי הזיהוי של לקוח שהמידע אודותיו מועבר במערכת הסליקה ישמרו במאגרים מוצפנים נפרדים בשיטת הצפנה מקובלת כמפורט בסעיף 4.12.9 להלן, ובצורה נפרדת. כל פעולה המבוצעת לגבי מידע המועבר במערכת או השמור בה תיעשה באופן שאינו מאפשר למי שאינו מורשה גישה למידע מסוים לזהות את הלקוח שמידע אודותיו עובר או שמור במערכת, בזמן העברתו או במועד שמירתו.

4.12.5. המידע המועבר במערכת הסליקה יימחק בתום תקופת הביקורת כהגדרתה בתקנות אבטחת מידע במערכת סליקה פנסיונית מרכזית, בהתאם לנהלי המערכת אשר אושרו על ידי הממונה, למעט נתונים אודות המידע ונתונים על כספים שהועברו דרך המערכת אשר יישמרו למשך התקופה המנויה בתקנות אבטחת המידע במערכת סליקה פנסיונית מרכזית.

4.12.6. הספק ישמור את הנתונים אודות המידע ונתוני העברת כספים במערכת סליקה פנסיונית מרכזית, באופן שניתן יהיה להציגו כרשומה מוסדית כהגדרתה בפקודת הראיות. הספק יעביר לאישור הממונה את מבנה הרשומה המוסדית כחלק מהאפיון של כל שלב.

4.12.7. הספק יתעד כל ניסיון לפגיעה בשלמות המידע או לשימוש בו ללא הרשאה (להלן - **אירוע אבטחה**), באופן אוטומטי, לרבות מנגנוני התרעה על אירועי אבטחה והיקף הפגיעה באבטחת המידע השמור במערכת או המועבר בה ובפרטיות החוסכים נשוא המידע, כמפורט בתקנות אבטחת מידע. נתוני התיעוד של מנגנון הבקרה יישמרו למשך 24 חודשים לפחות. יובהר, כי אין באמור כדי לגרוע מחובת הדיווח המיידית לרשות להגנת הפרטיות, בקרות אירוע אבטחה חמור, בהתאם לתקנה 11(ד) לתקנות אבטחת מידע.

4.12.8. במקרה של אירוע אבטחה הפוגע בשלמות המידע השמור במערכת הסליקה או המועבר בה, יבצע הספק שחזור מידע בהתאם לנהלי הגיבוי וההתאוששות כמפורט בפרק זה, באישור מנהל הפרויקט והממונה על אבטחת המידע. המערכת תתעד כל פעולה של שחזור מידע כאמור ותשמור אותם למשך 24 חודשים לפחות.

4.12.9. <u>הצפנה וחתימה</u>

4.12.9.1. הספק יישם הצפנה לפי תקן **NIST FIPS 140-2/3**. לרבות שילוב פרוטוקולי הצפנה חסינים מפני מחשוב קוונטי **Post-quantum cryptography - PQC)** ההצפנה תתבצע על המידע הרגיש הנשמר במערכת הסליקה או מועבר בין הממשקים החיצוניים והפנימיים, לרבות העברה ברשת תקשורת אלחוטית, רשת ציבורית או באינטרנט. בנוסף, הספק יישם הצפנה לפי תקן **NIST SP 800-57** לניהול מחזור חיי מפתחות קריפטוגרפיים וכן לפי תקן **SP 800-131A** ובהתאם להנחיות מערך הסייבר הלאומי בישראל (לפרויקטים ממשלתיים או ציבוריים).

4.12.9.2. מערכת הסליקה תכלול מנגנון למניעת התכחשות בכל פעולה במערכת וחתימה אלקטרונית כהגדרתה בחוק חתימה אלקטרונית באופן המבטיח את אימות זהות מבצע הפעולה. מערכת הסליקה תגדיר נהלים ומנגנונים מתאימים ליצירה, עדכון, התקנה, אחסון, שמירה וניטור הגישה על מפתחות הצפנה הרלוונטיים לפעילותה.

4.12.9.3. תבוצע הצפנה במנוחה עבור מאגרי נתונים כך שלא יהיו נגישים ללא מפתח ההצפנה בעת פריצה למערכת. מפתח ההצפנה ישמר באופן מאובטח שימנע גישה או שימוש לא מורשה.

4.12.9.4. הצפנת נתונים רגישים תתבצע באמצעות אלגוריתמים מתקדמים כגון **AES-256**.

4.12.9.5. הספק יתחייב לבדוק אחת לשנה את רמת ההצפנה הנהוגה בפרויקט, ולהבטיח עמידה בתקני שוק מעודכנים, לרבות החלפת אלגוריתמים במידה ואלה יצאו משימוש/הומלצו לא לשימוש על NIST או גופים אחרים מקובלים.

4.12.9.6. במקרים שבהם ייעשה שימוש באלגוריתם או בפרוטוקול הצפנה שאינו מאושר עוד על ידי NIST או גורם רגולציה רלוונטי או במקרה של דרישה מפורשת של הלקוח, הספק יחליפו תוך 60 יום מקבלת התרעה על כך להצפנה העומדת ברמה הנדרשת.

4.13. אבטחת מידע בתשתיות טכנולוגיות

4.13.1. הספק יישם את עקרון ההגנה בשכבות **(Defense in depth)**, בין היתר יישם מנגנוני בקרה כגון:

4.13.1.1. חומת אש **Firewall**;

4.13.1.2. מערכות גילוי ותגובה מפני חדירה **Intrusion detection systems (IDS) / Intrusion Prevention System (IPS)**;

4.13.1.3. סינון תוכן וגלישה בטוחה **URL & DNS filter** ו **Mail security**;

4.13.1.4. חסימת תוכנות לא מאושרות **(Application Control)** על בסיס **White List**;

4.13.1.5. מנגנון לזיהוי פעילות משתמשים **UEBA - User & Entity Behavior Analytics**;

4.13.1.6. מנגנון מלכודת דבש "**Honeypot**";

4.13.1.7. **WAF – Web application firewall**;

4.13.1.8. **Web app and API protection (WAAP)**;

4.13.1.9. מניעת זליגת מידע (**DLP - Data Loss Prevention**) ממערכת הסליקה ובקרה אחר המידע היוצא מהמערכת;

4.13.1.10. מערכות הכנה על עמודת קצה **EPP**, כגון **Endpoint Detection and Response (EDR)**;

4.13.1.11. **Patch Management** - מערכת לניהול והפצת עדכוני אבטחה (פאצים);

4.13.1.12. הגנה על כל בסיסי נתונים **Database activity monitoring (DAM) \ DB firewall**;

4.13.1.13. הצפנות בתנועה ובמנוחה ברמת החומרה **(Volume Level Encryption)** והצפנות ברמת האפליקציה **(application layer encryption)**;

4.13.1.14. לוגים ישמרו בתצורת **Write once read many (WORM)** ;

4.13.1.15. לא יעשה שימוש במערכות שסיימו את תקופה התמיכה על ידי היצרן **Life Products)(EOL - End Of**;

4.13.1.16. מנגנוני איסוף לוגים וניטור אנומליות למרכז **SIEM\SOC**;

4.13.2. הספק יתקין אמצעי הגנה נאותים מפני חדירה לא מורשית למערכת הסליקה, הכנסת רכיבים לא מורשים או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב.

4.13.3. הספק יפריד את המערכת הטכנולוגית המשמשת את מערכת הסליקה לשם ניהול המידע השמור במערכת או המועבר בה, ממערכות טכנולוגיות אחרות המשמשות אותו.

4.13.4. מערכת הסליקה תוכל להתממשק ולפעול עם מוצרי הקשחה חיצוניים כגון: **Net-IQ, eTrust**, סימנטק, **Bigfix**, וכד'.

4.13.5. הספק יישם הקשחת מערכות בהתאם למתודולוגיות מקובלות ו **Best Practice** בתעשייה, כגון: **Center for Internet Security (CIS) Benchmarks.**

4.13.6. הספק יישם אמצעי הגנה על מערכות קצה, תוך התחשבות בסיכוני הפעלת קוד עוין וסיכוני חדירה למערכות.

4.13.7. הספק יישם הצפנת מידע רגיש במערכות קצה (כגון מידע הנמצא על מחשבים ניידים, טאבלטים, התקני אחסון ניידים וטלפונים ניידים).

4.13.8. הספק יטמיע אמצעי אבטחה, למניעת חדירה והתפשטות קוד עוין במערכותיו, שיכללו מספר שכבות אבטחה כגון: סינון תקשורת וקבצים נכנסים, סריקת מערכות קבצים, הגנה בזמן אמת על שרתים או תחנות קצה, מערכות אנומליה ומערכות ניטור ומניעה ייעודיות.

4.13.9. הספק יממש כלים ויטמיע אמצעי אבטחה מקובלים למניעת סיכוני מעילות והונאות.

4.13.10. בעת חיבור אמצעי מדיה למערכות מידע יעשה שימוש במנגנוני הגנה אפקטיביים המונעים חדירת קוד עוין, כגון שימוש במערכות "הלבנת קבצים".

4.13.11. כל ערוץ הכנסת קבצים, בין אם למערכות המידע של הספק או למערכת הסליקה ידרשו לעבור סריקה באמצעות מערכת הלבנה מערכת הלבנה **CDR (Content Disarm and Reconstruction)** ובתנאי שלא נתגלו בהם פוגעניים (קבצים "נקיים" ובטוחים לשימוש).

4.13.12. <u>הגנה על התקשורת</u>

4.13.12.1. הספק יישם מידור בין החלקים השונים ברשת באמצעות חלוקה לוגית או פיסית של הרשת והגבלת אפשרות הקישור בין הרשתות השונות. רמת המידור תיקבע בהתאם לרגישות הנתונים המנוהלים במערכות. המידור יתבצע באמצעות **Firewall**.

4.13.12.2. הספק יבצע הפרדה מוחלטת של רשתות אלחוטיות מרשת הייצור שלו. לחילופין וככל שלא מדובר ברשת אלחוטית לשירות אורחיו, הספק יישם מנגנונים מספקים לאבטחת רשתות אלחוטיות, לרבות הצפנה, הזדהות חזקה **MFA**, מניעת התקפות על הרשת ומניעה של התחברות גורמים או ציודים בלתי מורשים לרשת האלחוטית.

4.13.12.3. לא תתאפשר גישה ישירה לרשת האינטרנט ולמערכות חיצוניות אחרות מרשתות המשתמשים ורשתות המנהלה. ההפרדה תתבצע ע"י מערכות משיקות, כלי סינון לתכנים ואפליקציות, רשתות נפרדות ואמצעי הפרדה.

4.13.12.4. הספק ישתמש באמצעי הגנת סייבר המתאימים לסיכוני גישה מרחוק לרשת הגוף וינקוט בגישת "אפס אמון" **(Zero Thrust)** לפני הקמה ואישור קישוריות, כגון אמצעי סינון תקשורת ותוכן, אמצעי ניטור הגנת סייבר ותהליכי בקרה. האמצעים יותאמו לסיכונים ייחודיים לשירותי רשת שונים, כגון דואר אלקטרוני, **DNS**, שירותי העברת קבצים, שירותי **Web** ועוד.

4.13.12.5. הספק יגדיר אמצעי אבטחה מוגברים כגון: שימוש בהזדהות חזקה **MFA**, הצפנה מקצה לקצה וניטור בגישה מרחוק לרשת הגוף, על גבי תשתית תקשורת ציבורית או מנקודות קצה שאינן מאובטחות דיין.

4.13.13. <u>תיעוד (לוגים)</u>

4.13.13.1. מערכת הסליקה תתעד כל ניסיון גישה אל המערכת ובסיסי הנתונים, גם אם כשל, וכל גישה בפועל באופן אוטומטי, כך שניתן יהיה להתחקות אחר מסלול הגישה, סוג הגישה ורכיבי המערכת והמידע אליהם בוצעה הגישה, לרבות טבלאות המערכת.

4.13.13.2. מנגנון התיעוד יתמוך במשלוח התרעות מידיות על פעולות חריגות לממונה על הגנת הפרטיות ולממונה על אבטחת המידע, אשר יוגדרו על ידו. האחריות על הגדרת הפעולות החריגות כאמור, היא על הממונה לאבטחת מידע.

4.13.13.3. הממונה על אבטחת המידע יבחן את הליקויים שנתגלו כתוצאה מהתיעוד כאמור מדי יום.

4.13.13.4. מערכת הסליקה תמנע, ככל הניתן, את האפשרות להפסיק את פעילות מנגנון התיעוד כאמור בסעיף זה, או צמצום פעילותו, ולהתריע בפני מנהלי המערכת על הפסקת פעילות או צמצום פעילות מנגנון תיעוד זה.

4.13.13.5. מנגנון התיעוד (הלוג) יתייחס לכל הפחות למבצע הפעולה, המקום ממנו בוצעה הפעולה, תאריך ושעת ביצוע הפעולה במדויק, האם הגישה אושרה או נדחתה, רכיב המערכת שאליו נעשה ניסיון הגישה וככל שהגישה אושרה גם היקף הגישה.

4.13.13.6. נתוני הרישום של מנגנון התיעוד (לוגים) יישמרו למשך שנתיים לפחות ויהיו מוגנים מפני מחיקה או שינוי בלתי מורשה.

4.13.13.7. אין באמור כדי לגרוע מחובות התיעוד לגבי נתונים על אודות המידע בהתאם לתקנות אבטחת המידע לתקופה של 7 שנים החל בתום תקופת הביקורת.

4.14. בקרות אבטחת מידע בענן

ככל ויבחר הספק להשתמש בשירותי מחשוב ענן יבצע זאת בהתאם לאמור להלן בסעיף זה.

4.14.1. בטרם הפעלת שימוש במערכות מבוססות ענן, על הספק לבצע הערכת סיכונים ייעודית ולהציגה לממונה.

4.14.2. ככל ויאושר שימוש בענן מחוץ לגבולות מדינת ישראל, הספק לא יאחסן מידע רגיש או נתוני לקוחות בענן מחוץ לגבולות מדינת ישראל.

4.14.3. גישה לנתונים בענן תבוצע דרך כתובות מורשות בלבד.

4.14.4. הספק יכלול בהסכם ההתקשרות עם ספק מחשוב הענן, יכולת שליטה ובקרה שלו על ספק מחשוב הענן וכן אפשרות חד צדדית להפסקת השימוש בשירותי ספק מחשוב הענן תוך מחיקת המידע ממערכותיו והתחייבותו שלא ניתן לאחזר מידע זה במערכותיו.

4.14.5. על הספק ליישם מדיניות אבטחת מידע בענן מקיפה. המדיניות תתבסס על סטנדרטים מתקדמים, דרישות רגולטוריות, ותהליכי אבטחה מותאמים לסביבת ענן, כמפורט להלן:

4.14.5.1. יישום מנגנון הגנה לסביבת ענן **CNAPP (Cloud Native Application Protection Platform)**, פלטפורמת הגנה על יישומים בענן. זוהי גישה הוליסטית לאבטחת יישומים בענן, המשלבת מספר יכולות אבטחה, מספק יכולות כגון סריקת פגיעויות,

אנטי וירוס, זיהוי חדירות ומניעתן, ניהול זהויות וגישה, וניטור פעילות, כגון:

4.14.5.1.1. **(Cloud Workload Protection Platform) CWPP**: הגנת מערכות/נכסים בענן (כמו מכונות וירטואליות, קונטיינרים ופונקציות ללא שרת)

4.14.5.1.2. **(Cloud Security Posture Management) CSPM**: ניהול ובקרה על מצב האבטחה בענן, סריקה וניטור של הגדרות אבטחה בענן כדי לוודא שהן תואמות לסטנדרטים ול**best practices** .

4.14.5.1.3. **SASE (Secure Access Service Edge)**: גישת אבטחה המאחדת פונקציות רשת ואבטחה בענן**SASE** . משלבת בין יכולות של **SD-WAN** (רשת תקשורת רחבה מוגדרת תוכנה) לבין פונקציות אבטחה כגון חומת אש כשירות **(FWaaS),** גישה מאובטחת לאינטרנט **(SWG), CASB (Cloud Access Security Broker)** ו**SASE .(ZTNA) Zero Trust Network Access-** מאפשרת גישה מאובטחת וגמישה למשאבים בענן ומחוצה לו, מכל מקום ובכל זמן.

4.14.5.1.4. **DSPM (Data Security Posture Management)**: ניהול ובקרת מצב אבטחת מידע. מנגנון זה מתמקד באבטחת מידע בענן, ומאפשר לגלות, לסווג ולנטר את המידע הרגיש המאוחסן בענן **DSPM**. סורק את סביבות הענן השונות ומאתר מידע רגיש, כגון מספרי כרטיסי אשראי, מספרי תעודות זהות ומידע רפואי. בין היתר נסייע לנהל את הרשאות הגישה למידע ולמנוע דליפות מידע.

4.14.5.1.5. שימוש בהצפנה מתקדמת:

4.14.5.1.6. נתונים בתעבורה יאובטחו באמצעות פרוטוקולים מוצפנים (TLS/SSL).

4.14.5.1.7. נתונים המאוחסנים בענן יעברו תהליך הצפנה (תיושם הצפנה לפי תקן **NIST FIPS 140-2/3**. לרבות שילוב פרוטוקולי הצפנה חסינים מפני מחשוב קוונטי **Post-quantum cryptography - PQC)** באמצעות מפתחות שנשלטים על ידי המערכת בלבד.

4.14.5.2. בקרות גישה ואימות רב-שלבי **(MFA)**:

4.14.5.2.1. ייושמו שיטות אימות רב-שלבי (**MFA**) לכל הגורמים המורשים לגשת לשירותי הענן, כולל עובדים, ספקים ושירותים חיצוניים.

4.14.5.3. מעקב פעולות משתמשים:

4.14.5.3.1. הטמעת מערכות לניטור פעולות משתמשים בזמן אמת, לצורך זיהוי פעילות חריגה (אנומליות באמצעות מערכת **SOC\SIEM** מרכזית) ודיווח אוטומטי לממונה אבטחת המידע.

4.14.5.4. אכיפת מדיניות הפרדת דיירים (**Multi-Tenant**):

4.14.5.4.1. במסגרת ניהול הסיכונים ורגישות המידע יבחן שימוש בתצורת **Single Tenant**, כגון **Dedicated instance**.

4.14.5.4.2. במקרים של סביבות משותפות, על הספק להטמיע טכנולוגיות טוקניזציה, הצפנה ומיסוך נתונים להבטחת פרטיות מוחלטת (תיושם הצפנה לפי תקן **NIST FIPS 140-2/3**. לרבות שילוב פרוטוקלי הצפנה חסינים מפני מחשוב קוונטי - **Post-quantum cryptography (PQC)**.

4.14.6. <u>תאימות ורגולציה</u>

4.14.6.1. תאימות לתקני אבטחת מידע:

4.14.6.1.1. עמידה בתקנים כמו **ISO 27017** (אבטחת מידע בענן), **ISO 27018** (הגנת פרטיות בענן) ודרישות חוק הגנת הפרטיות ותקנות אבטחת מידע , **STAR Level 2**.

4.14.6.2. מגבלות גיאוגרפיות על אחסון נתונים:

4.14.6.2.1. נתוני מערכת הסליקה יאוחסנו בענן הממוקם בגבולות ישראל, למעט אם ניתנה לכך הרשאה רגולטורית מפורשת.

4.14.6.3. דרישות **SLA**:

4.14.6.3.1. ספק הענן יתחייב לרמות זמינות ושירות המוגדרות בהסכמי **SLA**, עם מנגנונים לתגובה מיידית במקרה של תקלות. והתואמים את יעדי ההתאוששות שלך מערכת הסליקה.

4.14.7. <u>מעקב וניהול מתמשך</u>:

4.14.7.1. ניטור ואכיפה שוטפת:

4.14.7.1.1. שימוש בטכנולוגיות- קונטיינרים (כגון **doker**) הם סביבות ריצה זמניות. כאשר קונטיינר נסגר, כל המידע שנוצר בתוכו, כולל לוגים, עלול להימחק. הספק יאסוף את הלוגים לפני סגירת הקונטיינר.

4.14.7.1.2. הספק ייצר לוגים ברמת האפליקציה של מערכת הסליקה.

4.14.7.1.3. התקנת מערכות לניטור פעילות הענן, כולל ניטור תשתיות, תעבורת רשת, גישה לשירותים ואיתור חריגות בזמן אמת. מערכות הניטור ישולבו למערכת **SIEM\SOC** מרכזית.

4.14.7.2. בדיקות תקופתיות:

4.14.7.2.1. הספק יבצע בדיקות סדירות להערכת הביצועים והתאימות של שירותי הענן לדרישות האבטחה, כולל מבדקי חדירה וביקורות אבטחה.

4.14.7.3. מנגנוני התראה אוטומטיים:

4.14.7.3.1. שימוש במנגנוני התראה אוטומטיים לזיהוי ניסיונות פריצה או כשלים טכניים במערכות הענן.

4.14.8. <u>תכנון לסיום התקשרות</u>

4.14.8.1. מדיניות למחיקת נתונים מאובטחת:

4.14.8.1.1. הספק יבטיח מחיקת נתונים מלאה משירותי הענן במקרה של סיום התקשרות עם ספק ענן, תוך התחייבות ברורה לכך שלא ניתן לשחזר את הנתונים בהתאם לתקנים מקובלים למשל **Nist 800-88**.

4.14.8.2. תהליכי העברה לספק חלופי:

4.14.8.2.1. הספק יתכנן את המערכות למניעת סיכוני "נעילת ספק" **(Vendor lock-in)**.

4.14.8.2.2. הגדרת נהלים להעברה מאובטחת של נתונים ותשתיות לספק ענן חלופי, מבלי לפגוע בזמינות או בשלמות המידע.

4.14.9. <u>שיפור רציף והכשרת צוותים</u>

4.14.9.1. עדכון מדיניות אבטחת הענן:

4.14.9.1.1. עדכון מדיניות האבטחה בענן בהתאם לשינויים טכנולוגיים, דרישות רגולטוריות או איומים שהתגלו.

4.14.9.2. הדרכות עובדים וספקים:

4.14.9.2.1. קיום הדרכות תקופתיות לצוותי מערכת הסליקה ולספקים החיצוניים, במטרה לשפר את היכולות לזהות ולמנוע איומים הקשורים לענן.

4.15. אבטחה פיזית של מתקני מערכת הסליקה

4.15.1. הספק יוודא כי רכיבי מערכת הסליקה, אשר מופו כאמור, יישמרו במקום מוגן, המתאים לאופי פעילות המערכת ולרגישות המידע המועבר בה או נשמר בה, ואשר מונע חדירה אליו בלא הרשאה.

4.15.2. הספק ינקוט אמצעים סבירים לבקרה על הגישה לאתרי מערכת הסליקה ולתיעוד גישות שבוצעו, לרבות מיגון האתרים והכנסה והוצאה של ציוד אל אתרים אלה ומהם.

4.15.3. הספק ישתמש באבטחה פיזית המבוססת על מעגלי הגנה. כך, אזורים בהם מאוחסן מידע רגיש או ציוד המאפשר גישה לרכיבים רגישים של מערכת הסליקה, לרבות רכיבים המאפשרים גישה למערכות סליקה כספית או מערכות ליבה, יהיו במעגל ההגנה האחרון (הפנימי ביותר). מעגל ההגנה הראשון יוצב בכניסה למתקני מערכת הסליקה, מעגל הגנה שני יוצב בכניסה לכל קומה, מעגל הגנה שלישי יוצב בכניסה לפרוזדורים או מבואות, מעגל הגנה רביעי יוצב בכניסה לאזורים רגישים יותר כגון חדר הארכיב, חדר המחשב, ארון מסמכים וכדומה. בנוסף למעגלי ההגנה כאמור, בחדר הארכיב תוצב כספת לשמירת מסמכים סודיים. כל הכניסות למתקני מערכת הסליקה, לכל קומה, למבואות ולפרוזדורים וכן לאזורים רגישים יצולמו באמצעות מצלמות ויכללו בקרת גישה באמצעות התקן פיזי אישי של העובד או באמצעות אמצעי זיהוי ביומטרי.

4.15.4. הרשאות כניסה לאזורים רגישים יינתנו בהתאם לתפקידי העובד ולא תינתן גישה לעובד לאזורים רגישים מעבר לנדרש לו על פי תפקידו.

4.16. אבטחת שרשרת אספקה ומיקור-חוץ

4.16.1. <u>בקרות ספקים וספקי משנה</u>

4.16.1.1. על הספק להטמיע מערך בקרות מקיף להבטחת תאימות אבטחת המידע של כלל ספקי השירות ותתי-הספקים המעורבים בפעילות מערכת הסליקה. מערך זה יכלול דרישות מחמירות לעמידה בתקנים רלוונטיים כגון **ISO 27001, SOC 2 Type 2** ותקנים דומים נוספים המתאימים לסביבה הקריטית של המערכת.

4.16.1.2. הספק יידרש לוודא שכל ספק חיצוני פועל בהתאם למדיניות אבטחת המידע של מערכת הסליקה ומיישם בקרות אבטחה הנדרשות להבטחת סודיות, שלמות וזמינות הנתונים המועברים או

המאוחסנים במערכותיהם. בדיקות התאימות יכללו סקרי אבטחה תקופתיים, סקירת חוזים והסכמי שירות (**SLA**) להבטחת מענה הולם לסיכונים ייחודיים. בנוסף, תיערך בדיקה מקדימה (**Due Diligence**) לפני התקשרות עם כל ספק חיצוני חדש, שתכלול בחינת ההיסטוריה שלו בתחום אבטחת המידע ותהליכי ניהול הסיכונים שהוא מפעיל.

4.16.1.3. במהלך התקשרות עם ספקים ותתי-ספקים, הספק יחויב לבצע בדיקות שוטפות לאימות הבקרות, כולל מבדקי חדירה, סקירת לוגים ואנליזה של אירועים חריגים. תוצאות הבדיקות יתועדו ויועברו להנהלת הספק לצורך ניטור מתמשך ושיפור מערך ההגנה.

4.16.1.4. הספק יבצע סקר ספקים (לספקים חיצוניים) אחת לשנה לפחות ויפעל לטיפול בליקויים שימצאו.

4.16.2. <u>עקרונות לאבטחת מיקור-חוץ</u>

4.16.2.1. על הספק להגדיר מדיניות מקיפה ומפורטת לניהול אבטחת המידע במיקור-חוץ, הכוללת את כל שלבי ההתקשרות עם צדדים שלישיים – החל מרכש, דרך פיתוח ותפעול, ועד לסיום ההתקשרות. המדיניות תכלול רכיבים קריטיים שיבטיחו עמידה מלאה בדרישות האבטחה של המערכת.

4.16.2.2. בשלב הרכש, על הספק לכלול דרישות אבטחת מידע מפורטות במסמכי המכרז ובהסכמי ההתקשרות עם צדדים שלישיים לרבות הסכמי סודיות. דרישות אלו יגדירו את רמת הבקרות הנדרשת, כולל מנגנוני הצפנה (תיושם הצפנה לפי תקן **NIST FIPS 140-2/3**). זאת לרבות שילוב פרוטוקולי הצפנה חסינים מפני מחשוב קוונטי (**Post-quantum cryptography - PQC**), בקרת גישה ושיטות להגנה על נתוני המערכת. הספק יבטיח שספקים חיצוניים מחויבים לדווח על אירועי סייבר בזמן אמת ולשתף פעולה באופן מלא בתהליך ניהול האירוע.

4.16.2.3. בשלב הפיתוח, יש ליישם בקרות אבטחה מותאמות לפיתוח מאובטח (**Secure Development Lifecycle**), תוך ביצוע בדיקות אבטחה תכופות לקוד ולתשתיות המפותחות על ידי צד שלישי. הספק יידרש לעקוב אחרי תיקון חולשות שהתגלו, תוך שמירה על תיעוד מלא של הפעולות שבוצעו.

4.16.2.4. בשלב התפעול, יש להטמיע מנגנונים לניטור פעילות ספקי מיקור-החוץ בזמן אמת. מנגנונים אלו יכללו שימוש במערכות ניטור וגילוי חריגות, כגון **SIEM (Security Information and Event**

Management), וביצוע מבדקים תקופתיים למידת התאימות של ספקי המיקור למדיניות האבטחה.

4.16.2.5. בעת סיום ההתקשרות, על הספק להגדיר נהלים ברורים להעברת נתונים לרשות או לספק חלופי, תוך הבטחת מחיקה מוחלטת של נתוני המערכת ממערכות הספק הנוכחי. יש להבטיח שהליך זה יתבצע בהתאם לתקני האבטחה המחמירים ביותר, עם בקרה צמודה מצד צוותי אבטחת המידע של המערכת.

4.16.2.6. מדיניות זו תיבדק ותעודכן באופן תקופתי על מנת להתאים לשינויים טכנולוגיים, רגולטוריים ואיומים חדשים, ולוודא שמערך מיקור-החוץ של המערכת עומד ברמות ההגנה הגבוהות ביותר.

4.17. תצורת אבטחת המידע

4.17.1. מערכות ואמצעי אבטחת הגישה למערכת הסליקה יעודכנו באופן שוטף לאורך חייה בהתאם להתפתחות הסיכונים ולטכנולוגיות מקובלות בתחום וכן בהתאם להתפתחות תקני אבטחת מידע בינלאומיים מקובלים ובהתאם להוראות הממונה כפי שיהיו מעת לעת.

4.17.2. מערכת הסליקה לא תאפשר שימוש בהתקנים נתיקים/ניידים לשם העברת מידע שהועבר או נשמר במערכת הסליקה, למעט לצורך גיבוי הנתונים.

4.17.3. מערכת הסליקה תקושר לרשת האינטרנט ולמערכות חיצוניות אחרות לשם הפעלת היישומים הנדרשים לתפעול המערכת בלבד.

4.17.4. יובהר, כי בטרם יישום שלב ב' ו-ג' לתכנית העבודה, יעביר הספק תרשים תצורת אבטחת המידע מפורט ויאושר על ידי הממונה.

4.18. הדרכות ותודעת אבטחה של עובדי הספק

4.18.1. <u>אבטחת מידע בניהול כוח אדם</u>

הספק יערוך נוהל לגיוס עובדים, תהליכי עבודה וסיום עבודה בהיבט של אבטחת המידע.
לצורך סעיף 4.18 זה, עובד –לרבות אדם המועסק באופן ישיר על-ידי הספק הזוכה או באמצעות מיקור חוץ של הספק הזוכה ויש לו גישה למערכת הסליקה או למידע המצוי בה.
נוהל זה יכול שיהיה חלק מנוהל אבטחת המידע, ויכלול התייחסות לנושאים הבאים לפחות, והכל בכפוף לתקנות אבטחת מידע, ובאישור הממונה:

4.18.1.1. הליך גיוס עובדים, לרבות עריכת בדיקות מהימנות מועמד לעבודה בשים לב לתפקיד שאותו הוא מיועד למלא, והחתמת עובד על

התחייבות לשמירה על סודיות ולאחריות העובד בכל הנוגע להיבטי סיכוני סייבר ופרטיות. מועמד לתפקיד המוגדר כרגיש הכולל הרשאות גישה למידע רגיש המועבר או נשמר במערכת הסליקה או גישה למידע כספי או שיש לו הרשאות העלולות להוות סיכון למערכת יידרש לעמוד גם בבדיקת פוליגרף, כחלק מבדיקת הכשירות (בדיקות מהימנות של עובדים תעשינה בהתאם למתכונת שתאושר מראש על ידי הספק לתכלית ראויה ובמידה שאינה עולה על הנדרש. המידע שייאסף במסגרת הבדיקות ייחשב כמידע סודי).

4.18.1.2. אחריות העובד לשמירה על אבטחת מידע ופעולות שיש לנקוט לשם כך.

4.18.1.3. תכנית הכשרה והדרכה לפעולות הנדרשות לשמירה על אבטחת המידע והעלאת המודעות לנושא ולסיכונים, בטרם מתן הרשאות גישה, לרבות יידוע העובדים על מערכות אבטחת המידע והבקרות הקיימות והדרכות תקופתיות לעובדים.

4.18.1.4. הספק יערוך בדיקות מהימנות לעובדים קיימים לפי סבב קבוע ולפחות אחת בכל חמש שנים לעובד.

4.18.1.5. הספק יערוך נוהל לתהליך סיום עבודה, הנוהל יתייחס לעובדים (לרבות עובדים במיקור חוץ ועובדי קבלן) העוברים תפקיד או מסיימים את העסקתם, לחסימת הרשאות גישה למידע שאינו נדרש עוד, החזרת ציוד ונכסי מידע של המערכת.

4.18.1.6. הממונה על הפרטיות ואבטחת המידע יקיים הדרכה לעובדי הספק ולמורשי הגישה למידע המועבר במערכת הסליקה או הנשמר בה בנוגע לתקנות אבטחת מידע, מדיניות אבטחת המידע, נוהל אבטחת המידע והוראות פרק זה, בהיקף הנדרש למילוי תפקידם. הדרכה כאמור תתקיים אחת לשנה ולעובד חדש, סמוך למועד העסקתו ככל שניתן.

4.18.1.7. זיהוי עובדי מערכת הסליקה יעשה תוך שימוש באמצעי זיהוי חזק הכולל אמצעי חומרה המאפשר זיהוי חד-ערכי. לעניין סעיף זה, זיהוי חזק הינו זיהוי המבוסס על שני גורמים לפחות מבין אלה:

- תכונה פיזיולוגית ייחודית של המשתמש (**Something you are**).
- פריט הנמצא ברשות המשתמש (**Something you have**).
- פריט מידע הידוע למשתמש (**Something you know**).

4.18.1.8. הספק יקבע מדיניות ניהול הסיסמאות של מערכת הסליקה אשר תאושר על ידי הממונה, ותכלול את כלי המדיניות הבאים לפחות:

- סיסמאות מורכבות ולא טריוויאליות, בהתאם לסטנדרטים

מקובלים;

- אורך סיסמה מינימלי של 9 תווים לפחות;
- שמירת היסטוריית סיסמאות של 24 הסיסמאות האחרונות לפחות;
- הפעלת שומר מסך עם דרישת סיסמה לאחר 15 דקות של אי-פעילות לכל היותר;
- החלפת סיסמה למשתמש מדי 3 חודשים לפחות;
- חסימת משתמש לאחר 5 ניסיונות כושלים לזיהוי לכל היותר.

שינויים ו/או חריגות מהמדיניות שהותוותה לעיל יהיו כפופים לאישור הממונה.

4.19. פיתוח ואפליקציה

4.19.1. <u>תיעוד שלבי הפיתוח והקוד:</u>

תיעוד בתוך קוד הוא קריטי להבנה, תחזוקה ושיתוף פעולה בפרויקטי פיתוח תוכנה. הספק יבצע תיעוד פונקציות ומתודות באמצעות תיאור תמציתי:

- תיאור תמציתי לכל פונקציה או מתודה, יש לכתוב תיאור קצר וברור של מטרת הפונקציה (מה הפונקציה עושה, מה היא מקבלת כקלט, מה היא מחזירה כפלט)
- יש לתעד את סוג הנתונים של כל פרמטר, משמעותו וכל הגבלה עליו (למשל, טווח ערכים);
- יש לתעד את סוג הנתונים של ערך ההחזרה ומשמעותו;
- אם יש בפונקציה לוגיקה מורכבת או לא אינטואיטיבית, יש להוסיף הערות המסבירות את ההיגיון מאחורי הקוד.

4.19.2. <u>מתודולוגיות פיתוח מאובטח</u>

הספק מתחייב להפעיל מתודולוגיות פיתוח מאובטח העומדות בתקני אבטחת מידע בינלאומיים מקובלים, כגון **OWASP Secure Coding Practices** ו- **ISO 27034**, מתודולוגיות אלו יבטיחו תהליך פיתוח אחיד ושיטתי, הכולל זיהוי מוקדם של סיכוני אבטחה וניהולם בצורה מושכלת. המתודולוגיה צריכה לכלול תהליכי בקרת איכות אבטחה, ניהול סיכונים מובנה ותיעוד מלא של כל שלבי הפיתוח לרבות תיעוד מלא ומובנה של רכיבי קוד פתוח המשמשים את המערכת (ראה גם סעיף 4.9.15 לעניין ניהול **SBOM** עבור רכיבי קוד פתוח).

4.19.3. <u>נוהלי פיתוח מאובטח</u>

על הספק להטמיע נוהלי פיתוח מאובטח בתהליך העבודה, לרבות:

- יישום עקרונות תכנון מאובטח **(Secure by Design)** ;
- ביצוע בדיקות אבטחה לאורך כל שלבי הפיתוח, כולל בדיקות חדירה, ניתוח קוד סטטי ודינמי ;
- שימוש בכלים ייעודיים לניטור חולשות פוטנציאליות, זיהוי בעיות אבטחה בזמן אמת ותיקונן.

4.19.4. <u>עקרונות עיצוב להגנה על הפרטיות</u>

הספק ישלב בתהליך הפיתוח עקרונות עיצוב להגנה על הפרטיות **(Privacy by Design)** :

- צמצום איסוף ושמירת נתונים למינימום הנדרש.
- יישום טכנולוגיות להצפנה (תיושם הצפנה לפי תקן **NIST FIPS 140-2/3**). לרבות שילוב פרוטוקולי הצפנה חסינים מפני מחשוב קוונטי **Post-quantum cryptography - PQC)** ואנונימיזציה של מידע אישי כדי למנוע שימוש בלתי מורשה.
- הבטחת תאימות מלאה לחוקים ולרגולציות בנושאי פרטיות, תוך פיקוח שוטף ועדכונים בהתאם לשינויים בסביבה הרגולטורית.

4.19.5. <u>שימוש בקוד פתוח</u>

בעת שימוש בקוד פתוח, על הספק לבצע את הפעולות הבאות:

- הספק ינהל תיעוד מפורט למקור הקוד (**software bill of materials - SBOM**) והעמידה בדרישות הרגולטוריות תיעוד זה יבוצע כחלק ממסגרת מחזור חיי פיתוח מאובטח (**SSDLC**) כאמור בסעיף 4.19.3 לעיל).
- הספק יתעד את אופן השימוש בקוד הפתוח והיכן שולב ביישום.
- יבצע בדיקות אבטחת מידע מעמיקות לקוד הפתוח, כולל בדיקת פגיעויות ידועות ויישום בקרות תיקון במידת הצורך.
- יבטיח כי רישיון הקוד עומד בדרישות השימוש, ללא מגבלות העלולות לסכן את המערכת.

4.19.6. <u>פיתוח ממשקים **(OpenAPI)**</u>

בעת פיתוח ממשקי **API**, על הספק להבטיח עמידה בסטנדרטים מתקדמים ובשיטות אבטחת מידע חדשניות. דרישות אלו כוללות:

- שימוש בפרוטוקולי הזדהות והרשאות מתקדמים כגון **OAuth2,** תוך יישום בקרות חזקות לניהול זהויות וגישה.
- הצפנת נתונים בשתי רמות :
- א. רמת **Transport** – הבטחת תקשורת מאובטחת באמצעות **TLS 1.2** ומעלה, עם המלצה על **TLS 1.3.**

ב. רמת – **Messages** הצפנה מקצה לקצה של התוכן המועבר בין ממשקים.

- עמידה בתקן **IDAS (Identification, Authentication and Trust Services)**, המבטיח תהליך זהות, אימות ושירותי מסחר אלקטרונים מקוונים מאובטחים.
- מנגנונים למניעת הונאה וזיוף באמצעות בדיקות **Integrity** בכל שלב.

4.19.7. <u>תהליך מחזורי לפיתוח מאובטח **(SSDLC - Secure System Development Life Cycle)**</u>

הספק יאמץ תהליך מחזורי לפיתוח מאובטח הכולל שלבים ברורים ושיטתיים:

4.19.7.1. שלב דרישות ואפיון:

- הגדרת דרישות אבטחה כחלק אינטגרלי מהדרישות העסקיות והטכנולוגיות.
- זיהוי מוקדם של סיכונים פוטנציאליים בנוגע למידע בעל רגישות מיוחדת ומידע עסקי רגיש אחר ולשימוש בממשקים.

4.19.7.2. שלב עיצוב ופיתוח:

- הטמעת עקרונות עיצוב מאובטח כמו סגמנטציה של תהליכים רגישים, מניעת זליגת נתונים והפרדת סביבות עבודה.
- בדיקות נרחבות ליישום העקרונות בתשתיות הפיתוח.

4.19.7.3. שלב בדיקות וביקורת איכות:

- ניהול תהליך **QA** הכולל בדיקות חדירה, ניתוח קוד סטטי ודינמי.
- שימוש במערכות אוטומטיות לגילוי חולשות **(SAST/DAST)**.

4.19.7.4. שלב הפריסה והתחזוקה:

- יישום תהליכי **Deployment** מאובטחים, כולל אימות חתימות קבצים והצפנת עדכונים.
- ניהול עדכוני תוכנה שוטפים ושמירה על תאימות לגרסאות הקיימות.

4.19.8. <u>בקרות ניהול אבטחה בתהליך הפיתוח</u>

4.19.8.1. על הספק ליישם בקרות מתקדמות לניהול אבטחת מידע בתהליך הפיתוח, הכוללות לכל הפחות:

- מעקב אחר שינויים בתוכנה באמצעות כלים לניהול גרסאות **(Version Control)** והבטחת עקיבות מלאה.
- ניתוח סיכונים מתמשך תוך שימוש בכלים מתקדמים כגון **Threat Modeling**, במטרה לזהות נקודות תורפה כבר בשלב

הפיתוח.

- בקרת הרשאות למפתחים ואבטחת סביבת העבודה.

4.19.9. <u>הדרכות ותודעת אבטחת מידע לצוותי הפיתוח הבקרה</u>

הספק יחויב להטמיע תוכנית הדרכה והכשרה מובנית לצוותי הפיתוח הבקרה והתחזוקה, שתתעדכן באופן שוטף בהתאם להתפתחויות בעולם אבטחת המידע. תוך דגש על הבנה מעמיקה של שיטות פיתוח מאובטח והתמודדות עם אתגרי אבטחת מידע. התוכנית תכלול לכל הפחות התייחסות ל:

4.19.9.1. הדרכות בסיסיות ומתקדמות:

- הקניית ידע מעשי בנושאי פיתוח מאובטח, זיהוי חולשות אבטחה וכתיבה נקייה מקוד זדוני.
- הסברה על עקרונות אבטחת מידע, כגון **OWASP Top 10** .

4.19.9.2. תרגולים וסימולציות:

- סימולציות המדמות תרחישי תקיפה בזמן אמת, תוך זיהוי וטיפול מידי בסיכונים פוטנציאליים.
- תרגול במערכות **Sandbox** לצמצום טעויות אנוש בסביבת הייצור.

4.19.9.3. הסמכות ייעודיות:

- עידוד הסמכה מקצועית לצוותי הפיתוח, כגון **CSSLP** .

4.19.10. <u>שימוש בבדיקות סטטיות ודינמיות בתהליך הפיתוח</u>

הספק יבצע בדיקות אבטחת מידע כחלק אינטגרלי ממחזור חיי הפיתוח:, אשר יכללו לכל הפחות את הבדיקות שלהלן:

4.19.10.1. בדיקות סטטיות **(SAST)**:

- סריקה של קוד המקור לאיתור חולשות אבטחה לפני שלב ההרצה.
- זיהוי טעויות שכיחות כמו הזנות לא בטוחות **(Input Validation)** או זליגת נתונים **(Data Leakage)** .

4.19.10.2. בדיקות דינמיות **(DAST)** :

- הרצת סימולציות בזמן אמת על אפליקציות מתפקדות, במטרה לחשוף פרצות לא צפויות.
- בדיקות ניהול סשנים **Authentication**, ואימות תקינות תקשורת מוצפנת.

4.19.10.3. בדיקות פוסט-פיתוח:

- בדיקות חדירה **(Penetration Tests)** להערכת עמידות המערכת מפני מתקפות ייעודיות.
- ניתוח דוחות הבדיקות ותיעוד לקחים לתהליך הפיתוח העתידי.

4.19.11. ניהול תהליכי תיקון ותיעוד פגיעויות

על הספק להבטיח תהליכים מסודרים לטיפול ותיעוד של פגיעויות שהתגלו:

4.19.11.1. ניהול פגיעויות:

- יצירת תוכנית תיקון ברורה עם סדרי עדיפויות מבוססי סיכון **(Risk-Based Prioritization)**.
- תיעדוף חולשות קריטיות שמידת השפעתן על המערכת גבוהה במיוחד.

4.19.11.2. תיעוד מלא:

- יצירת דוחות מפורטים הכוללים תיאור הפגיעות, הצעדים שננקטו לטיפול בה, וזמני התגובה.
- שמירה על דוחות אלו לצרכי בקרה פנימית ודיווח לרגולטור.

4.19.12. עמידה בתקנים ורגולציות בינלאומיות

4.19.12.1. על תהליך הפיתוח לעמוד בדרישות רגולטוריות ותאימות לתקנים מקובלים בינלאומיים, כגון התקנים שלהלן וכפי שיתעדכנו מעת לעת:

- **ISO 27001/27034/2022** לניהול אבטחת מידע בתהליכי פיתוח;
- **PCI DSS**לניהול אבטחת מערכות פיננסיות.;
- תקני וסטנדרטיים לאבטחת ממשקים (כגון **OpenAPI** ו **eIDAS**);
- **NIST SP 800-218 Secure Software Development Framework (SSDF)**;
- **OWASP Developer Guide**.

4.19.13. הגנה על ממשקים חיצוניים **(API Security)**

ממשקי **API** משמשים כחוליה קריטית במערכות הפיתוח. על הספק לנקוט צעדים להגנה על הממשקים, הכוללים לכל הפחות את הצעדים הבאים:

4.19.13.1. ניהול זהויות והרשאות :

- יישום מנגנוני הזדהות והרשאות מתקדמים כגון **OAuth2**, תוך הקפדה על עקרונות הגבלת גישה למינימום ההכרחי **(Least Privilege)**.

- שימוש ב **JWT (JSON Web Tokens)**-לאימות זהות המשתמשים ולהבטחת תקשורת מאובטחת.

4.19.13.2. בקרות גישה לממשקים:

- קביעת מגבלות על תדירות השימוש ב **API (Rate Limiting)**-לצמצום מתקפות **DdoS**.
- יישום **Whitelisting** לרשימת כתובות **IP** מורשות.

4.19.13.3. הגנה מפני מתקפות מבוססות **API**:

- מנגנונים למניעת מתקפות **Injection** ו **XSS (Cross-Site Scripting)**-.
- ניתוח תעבורת נתונים לזיהוי פעילות חריגה.

4.19.14. <u>הגנה על שרשרת האספקה של הקוד</u>

על הספק ליישם בקרות לניהול אבטחת הקוד בכל שלבי שרשרת האספקה:

4.19.14.1. ניהול גרסאות מאובטח:

- שימוש במערכות ניהול גרסאות (כגון **Git**) המאפשרות מעקב אחר שינויים בקוד ושחזור לגרסאות קודמות במקרה של תקלות.
- אימות חתימות דיגיטליות של קבצים כדי למנוע שימוש בקוד שהוזרם בצורה זדונית.

4.19.14.2. בדיקות תשתיות ושירותים חיצוניים:

- ניתוח תלויות **(Dependencies)** בקוד הפתוח המשולב בפרויקט, כולל בדיקות תאימות ועדכניות.
- שימוש בכלים כגון **SCA (Software Composition Analysis)** לזיהוי רכיבי קוד פגיעים.

4.19.14.3. בקרת סביבות עבודה:

- הפרדה בין סביבות הפיתוח, הבדיקות והייצור למניעת דליפת מידע או שימוש לא מורשה בקוד.
- יישום בקרות גישה הדוקות למפתחים ולמנהלי מערכת.

4.19.15. <u>ניהול עדכונים ושדרוגים</u>

ניהול עדכוני תוכנה הוא מרכיב מרכזי בשמירה על אבטחת המערכת לאורך זמן. הספק מתחייב:

4.19.15.1. ניהול מחזור עדכונים:

- פיתוח תוכנית עדכונים מתוזמנת הכוללת טיפול בפרצות אבטחה

(Patches), שדרוגי גרסה ותיקונים לשיפור ביצועים.

- אימות תקינות העדכונים באמצעות בדיקות **QA** לפני פריסתם בסביבת הייצור.

4.19.15.2. עדכונים דחופים :

- הגדרת נוהל לטיפול בעדכוני אבטחה דחופים **(Hotfixes)** למניעת חשיפת המערכת לאיומים חדשים.
- יישום בקרת שינויים **(Change Management)** המתעדת את העדכונים שבוצעו.

4.19.16. ניטור ותגובה לאיומים בזמן אמת

על הספק לשלב יכולות ניטור ותגובה בסביבת הפיתוח והיישום:

4.19.16.1. ניטור בזמן אמת :

- מעקב רציף אחר תעבורת נתונים וביצועי מערכת באמצעות כלים לניטור יישומים.**(APM)**
- שימוש במנגנוני **Alerting** המתריעים בזמן אמת על חריגות או ניסיונות חדירה.

4.19.16.2. תגובה מהירה :

- ניהול מרכז תגובה לאירועי סייבר **(SOC)** המיועד לטיפול במתקפות ממוקדות על אפליקציות וממשקים.
- ביצוע ניתוח **Post-Mortem** לאחר כל אירוע אבטחה לשיפור מערך ההגנה.

4.19.17. ניהול פרויקטים בסביבת פיתוח מאובטחת

הספק יתחזק תהליך מובנה לניהול פרויקטים הכולל:

4.19.17.1. מעקב אחר אבני דרך קריטיות:

- הגדרת לוחות זמנים לתכנון, פיתוח, בדיקות ופריסה, תוך עמידה בסטנדרטים שנקבעו מראש.
- תיעוד התקדמות כל שלב בתהליך הפיתוח, כולל אישורים מבקרי אבטחה.

4.19.17.2. בקרת איכות לאורך מחזור החיים:

- הטמעת תהליכי בקרת איכות המבטיחים עמידה בדרישות האבטחה בשלבי הפיתוח, ההטמעה והתחזוקה.
- הפקת דוחות תקופתיים המסכמים את מצב האבטחה ומידת

ההתקדמות לעמידה ביעדי הפרויקט.

4.19.18. <u>ניהול סיכונים בתהליך הפיתוח</u>

ניהול סיכונים בתהליך הפיתוח הינו חלק בלתי נפרד ממחזור החיים המאובטח:

4.19.18.1. זיהוי סיכונים מוקדם:

- ניתוח סיכונים בכל שלב בתהליך הפיתוח, החל משלב האפיון ועד לתחזוקה השוטפת.
- שימוש במתודולוגיות **Threat Modeling** לזיהוי חולשות מערכתיות אפשריות.

4.19.18.2. מעקב ותיעוד סיכונים:

- ניהול רישום סיכונים דינמי המתעדכן לאורך כל מחזור החיים של הפרויקט.
- ביצוע ניתוח מעמיק של סיכונים שהתממשו והפקת לקחים לצמצום סיכונים עתידיים.

4.19.19. <u>חדשנות ואימוץ טכנולוגיות הגנה מתקדמות</u>

שימוש במערכות הגנת סייבר בעלות מנוע יוריסטי מובנה (מנוע היוריסטי מובנה להגנת סייבר הוא רכיב בתוכנת אבטחה שמטרתו לזהות איומים ונוזקות חדשות שעדיין לא קיימים להם חתימות או דפוסי פעולה מוכרים).
על הספק להבטיח כי טכנולוגיות מתקדמות יוטמעו בתהליך הפיתוח:

4.19.19.1. שימוש בבינה מלאכותית ולמידת מכונה:

- יישום פתרונות מבוססי **AI** לזיהוי איומים פוטנציאליים ולבקרת קוד.
- ניטור אוטומטי של דפוסי תעבורה חריגים בזיהוי מוקדם של איומים.

4.19.19.2. אימוץ פתרונות ענן מאובטחים, ככל שרלוונטי:

- שימוש בתשתיות ענן עם הגנה מובנית, הכוללות הצפנה (תיושם הצפנה לפי תקן **NIST FIPS 140-2/3**). לרבות שילוב פרוטוקולי הצפנה חסינים מפני מחשוב קוונטי **Post-quantum cryptography - PQC)**, גיבויים ותהליכי בקרת גישה מתקדמים.
- שילוב טכנולוגיות לניהול זהויות וגישה בענן **(IAM)**.

4.19.20. <u>סיכום ותיעוד הפיתוח</u>

בסיום תהליך הפיתוח, על הספק להפיק תיעוד מקיף הכולל:

- תיאור מלא של המערכת, כולל התשתיות, הממשקים והפרוטוקולים בהם נעשה שימוש.
- תיעוד כלל בדיקות האבטחה שבוצעו, כולל תוצאות והמלצות לשיפורים עתידיים.
- מסמך תאימות הכולל אישור עמידה בתקנים ורגולציות רלוונטיות.

4.20. תהליך זיהוי, אימות ובחינת הרשאות

4.20.1. הספק יבצע זיהוי לקוחות, משתמשים וגורמים אחרים במערכת הסליקה בהתאם להוראות ואישור הממונה כפי שיהיו מעת לעת ובכפוף לסטנדרט הטכנולוגי שיפורסם על ידי הממונה.

4.20.2. זיהוי משתמשים יעשה תוך שימוש באמצעי זיהוי חזק הכולל אמצעי חומרה המאפשר זיהוי חד ערכי או בכפוף להוראות הממונה. זיהוי גורם אחר מטעם המשתמש יבוצע בנפרד, אלא אם ברשות המשתמש מערכת לזיהוי חד ערכי של עובדיו העושים שימוש בחיבור למערכת הסליקה מטעמו וביכולתו של המשתמש לנטר את השימוש של עובדיו במערכת הסליקה למניעת שימוש שלא בהתאם להרשאה שבה מחזיק העובד או שימוש בניגוד למטרת מתן ההרשאה, והכל בכפוף להוראות תקנות אבטחת מידע ולהיוועצות עם הממונה על הגנת הפרטיות.

4.20.3. תהליכי ההצטרפות למערכת הסליקה יכללו מסגרת הרשמה ראשונית **(Onboarding)** מתקדמת **(Paperless)**.

4.20.4. לעניין זה זיהוי חזק הינו זיהוי המבוסס על שני גורמים לפחות מבין אלה:

- תכונה פיזיולוגית ייחודית של המשתמש **(Something you are)**;
- פריט הנמצא ברשות המשתמש **(Something you have)**;
- פריט מידע הידוע למשתמש **(Something you know)**;

4.20.5. זיהוי לקוח במערכת ייעשה באופן שיבטיח את אימות זהותו והרשאתו לשם קבלת מידע ו/או העברת בקשות לביצוע פעולות בטרם העברת בקשות הלקוח לקבלת מידע או לביצוע פעולות אל הגוף המוסדי.

4.20.6. הספק יאפשר לפחות את כל השיטות הבאות לזיהוי ראשוני של לקוח לשם רישום והתחברות למערכת הסליקה:

4.20.6.1. זיהוי לקוח באמצעות אימות פרטי הזיהוי הכלולים בתעודת זהות חכמה.

4.20.6.2. זיהוי לקוח באמצעות אימות פרטי תעודת הזהות לרבות תאריך הנפקת התעודה למול מרשם משרד הפנים.

4.20.6.3. זיהוי לקוח המבוסס על מסירת פרטים מזהים אודותיו ("שאלות סבתא"), אשר יאומתו מול שני מאגרי מידע חיצוניים לפחות, ומסירת סיסמה ראשונית ומזהה.

4.20.6.4. זיהוי לקוח המבוסס על תעודת זהות הלקוח, כאשר סיסמא ראשונית ומזהה יישלח ללקוח באמצעות חשבון **iPost** המנוהל בדואר ישראל על שם הלקוח או באמצעות דואר רשום בהתאם לכתובת הלקוח הרשומה במרשם האוכלוסין, לבחירת הלקוח.

4.20.6.5. זיהוי המבוסס על מסירת צירוף מספר תעודת הזהות, מספר כרטיס אשראי אישי הנמצא ברשות הלקוח ושלוש הספרות בגב כרטיס האשראי.

4.20.6.6. זיהוי לקוח המבוסס על קישור ישיר מתוך אזור מאובטח באתר אינטרנט של צד שלישי שהוא גורם ממשלתי לאחר שזוהה על ידי אותו צד שלישי בזיהוי המבוסס על זיהוי ראשוני.

4.20.6.7. זיהוי חד ערכי אחר, אשר אושר על ידי הממונה מראש ובכתב.

4.20.7. זיהוי לקוח באופן שוטף במערכת הסליקה לאחר קבלת אמצעי הזיהוי הראשוני כמפורט לעיל, יעשה באמצעות צירוף מספר תעודת זהות, קוד מזהה שהונפק בתהליך הראשוני וסיסמא חד פעמית (**OTP**) שתישלח ללקוח לפני כל כניסה למערכת הסליקה, באמצעי לבחירתו של הלקוח בעת הרישום למערכת הסליקה מבין אלה: טלפון נייד/דואר אלקטרוני

4.20.8. מערכת הסליקה תאפשר ללקוח, לאחר זיהויו במערכת, לעדכן את ערוץ ההתקשרות המועדף עליו למשלוח הסיסמה החד פעמית (**OTP**) כאמור לעיל. לקוח ששכח את המזהה שהונפק לו יחויב בזיהוי ראשוני או הליך שחזור מזהה באמצעות פרטים מזהים נוספים שנמסרו למערכת הסליקה בעת הרישום הראשוני לצורך עדכון פרטים ("שאלות סבתא" ייעודיות).

4.20.9. הספק יפעל לשיפור ועדכון שיטות הזיהוי של לקוחות ומשתמשים בהתאם להתפתחויות הטכנולוגיות.

4.20.10. זיהוי משתמשים וגורמים אחרים אשר יפעלו מול המערכת שלא באמצעות הפורטל אלא כמערכת הפונה למערכת, יבוצע בהתאם ובכפוף לסטנדרט הטכנולוגי שיפרסם הממונה ולהוראות הממונה בהקשר זה.

4.21. תהליך אימות ייפוי כוח של בעל רישיון

4.21.1. מערכת הסליקה תעביר כל ייפוי כוח של בעל רישיון אשר הועבר אליה אל הגוף המוסדי נשוא הבקשה, לאחר שביצעה בקרה לתקינות ושלמות וכן בקרה להתאמת ייפוי הכוח לבקשה הנלווית אליו.

4.21.2. מערכת הסליקה תטפל בבקשת מידע מכלל הגופים המוסדיים שהעביר בעל רישיון בשם לקוח, רק אם הציג בפניה ייפוי כוח תקף בנוסח שבנספח א' לחוזר ייפוי כוח, אשר תואם את פרטי הזיהוי של הלקוח שלגביו נתקבלה בקשת המידע כאמור, והכל בכפוף לתקנות אבטחת מידע וחוזר ייפוי כוח.

4.21.3. מערכת הסליקה תבצע בדיקת תקינות ואימות בסיסי לכל ייפוי כוח המועבר באמצעותה, לרבות הרשאת לקוח לבעל רישיון בהתאם להוראות חוזר ייפוי כוח.

פרק 5 – מימוש

5.1. כללי

5.1.1. פרק זה מפרט את אופן מימוש דרישות המכרז להפעלת מערכת הסליקה הפנסיונית והתאמתה, בהתאם לפרק זה ובפרט לתכנית העבודה.

5.1.2. הספק ישתף פעולה עם הממונה וכל גורם מטעמו, שיתוף פעולה זה יכלול העמדת כל המידע הנדרש, וביצוע הפעולות לפי הנחיות הממונה וכל גורם אחר מטעמו. העמדת מידע הנדרש על ידי המזמין, תיעשה לא יאוחר מחמישה ימי עסקים ממועד בקשת המידע על ידי המזמין וכל עיכוב בהעברת המידע יינתן בהסכמת המזמין בלבד.

5.1.3. מבלי לגרוע מדרישות אחרות במכרז, הספק הזוכה יכשיר את אנשיו לרמת מומחיות בעבודה עם מערכת הסליקה.

5.1.4. יובהר, כי אין בהוראות פרק זה לעניין מינוי בעלי תפקידים אצל הספק כדי לגרוע מהוראות סעיף 31ז לחוק הייעוץ הפנסיוני שהחיל את ההוראות לפי סימן א'1 לפרק ד' בחוק הפיקוח על הביטוח לעניין אורגנים ובעלי תפקידים אחרים במבטח, כמפורט בסעיף 31ז כאמור, על אורגנים ובעלי תפקידים כאמור בחברה להפעלת מערכת סליקה פנסיונית מרכזית.

5.1.5. יובהר, כי על מנכ"ל החברה ומנהל הפרויקט להקדיש את עיקר זמנם לתפקידם ולא לעסוק בעיסוק אחר אלא באישור הממונה;

5.2. ניהול הפרויקט

בתוך 30 ימים מיום חתימת ההסכם, על הספק הזוכה למנות בעלי תפקידים ניהוליים שונים בחברה שתוקם על ידו להפעלת מערכת הסליקה לפי מכרז זה, על פי הפירוט שלהלן, אשר יובאו לאישור הרשות בטרם מינויים. לגבי בעלי התפקידים הנדרשים בתנאי הסף, אלה יוצעו במסגרת ההצעה על ידי המציעים, וימונו על ידי הספק הזוכה מיד עם החתימה על הסכם ההתקשרות. בעלי התפקידים שימונו לפי סעיף זה יובאו לאישור הרשות, ויהיו מועסקים ישירות על ידי החברה.

להלן פירוט בעלי התפקידים, מהות תפקידם והכישורים הנדרשים מהם:

5.2.1. **מנכ"ל הספק**

5.2.1.1. הספק ימנה מנכ"ל מטעמו בכפוף לאישור הממונה ובהתאם לדרישות המפורטות בתנאי הסף למכרז בפרק 1. המנכ"ל יועסק על ידי הספק ולא על ידי ספק משנה.

5.2.1.2. תפקידו של המנכ"ל יהיה אחראי על הניהול השוטף של החברה, להתוות מדיניות ותוכנית אסטרטגית ולהוציאן לפועל. להיות אחראי על עמידה בדרישות המכרז ובפעילות התקינה והשוטפת של המערכת. ניהול

ההנהלה, מינוי ופיקוח על המנהלים בחברה, קביעת סדרי עדיפויות והצבת יעדים פנימיים, ייצוג החברה מול לקוחות, שותפים עסקיים הממונה תקשורת,אחראי על דיווחים לדירקטוריון ולוודא את יישום החלטות הדירקטוריון.

5.2.2. מנהל הפרויקט מטעם הספק

5.2.2.1. הספק ימנה מנהל פרויקט מטעמו בכפוף לאישור הממונה. מנהל הפרויקט יועסק על ידי הספק ולא על ידי ספק משנה.

5.2.2.2. מנהל הפרויקט מטעם הספק ירכז וינהל את כל השירותים שיינתנו מטעם הספק במסגרת מימוש המכרז, ויישא באחריות הכוללת לכל השירותים המסופקים במסגרת מכרז זה, הן ביחס לשירותים הניתנים לרשות והן ביחס לשירותים הניתנים ללקוחות ומשתמשי מערכת הסליקה, לרבות ניהול שוטף של צוות העובדים הפועל מטעם הספק וספקי המשנה. מנהל הפרויקט מטעם הספק יהיה אחראי לכל צוותי הפרויקט (אפיון, פיתוח, תפעול, תחזוקה, הדרכה, תמיכה וכדומה).

5.2.2.3. מנהל הפרויקט מטעם הספק יכול לשמש כמנכ"ל החברה אשר תוקם לצורך הפעלת מערכת סליקה פנסיונית, וזאת בכפוף לאישור הממונה.

5.2.2.4. מנהל הפרויקט יהווה איש הקשר המרכזי אצל הספק עבור הממונה, ויהיה זמין למפגשים קבועים או משתנים עם נציגי הממונה, בהתאם לדרישתו.

5.2.2.5. הכישורים והידע הנדרשים ממנהל הפרויקט – מפורטים בתנאי הסף למכרז בפרק 1.

5.2.3. צוות ניהול הפרויקט

נוסף על מנהל הפרויקט כאמור, הספק יידרש למנות בעלי תפקידים שונים בחברה שתוקם על ידו לשם הקמת מערכת הסליקה והפעלתה לפי מכרז זה, בהתאם למבנה החברה המוצע על ידו. בעלי התפקידים שימונו לפי סעיף זה יובאו לאישור המזמין, ויהיו מועסקים ישירות על ידי הספק ולא על ידי ספק משנה.

5.2.3.1. ממונה אבטחת המידע

5.2.3.1.1. ממונה אבטחת המידע יהיה הגורם האחראי על הקביעה של כלל מדיניות אבטחת מידע ויישומה במערכת הסליקה, באמצעים השונים המותקנים במערכת ובארכיטקטורת הפתרון, זרימת המידע במערכת ומבנה בסיסי הנתונים.

5.2.3.1.2. ממונה אבטחת המידע יהיה אחראי על היישום ועמידת הספק הזוכה באופן שוטף בדרישות אבטחת המידע אשר מפורטות בפרק 4 אבטחת מידע לעיל ובהתאם להוראות הדין.

5.2.3.1.3. ממונה אבטחת מידע יהא בעל ניסיון וכישורים המתאימים לניהול אבטחת מידע בהיקף של המערכת המאופיינת במכרז זה. הכישורים והידע הנדרשים ממונה אבטחת המידע – מפורטים בתנאי הסף למכרז בפרק 1.

5.2.3.2. **מנהל פיתוח טכנולוגי**

5.2.3.2.1. מנהל הפיתוח יהיה אחראי על פיתוח השירותים הנדרשים במכרז זה. מנהל הפיתוח יהא אחראי על ניהול שוטף של צוותי פיתוח, צוותי **QA** ובדיקות אוטומציה תוך יישום מתודולוגיות ונהלי פיתוח ושימוש בכלי הנדסת תוכנה.

5.2.3.2.2. מנהל הפיתוח יהא בעל ניסיון וכישורים המתאימים לניהול פיתוח בהיקף של המערכת המאופיינת במכרז זה, הכישורים והידע הנדרשים ממנהל הפיתוח – מפורטים בתנאי הסף למכרז בפרק 1.

5.2.3.3. **מנהל תשתיות ותקשורת**

5.2.3.3.1. מנהל תשתיות ותקשורת יהיה אחראי על תפעול תשתיות המערכת והקמת תשתיות חדשות, על פי הנדרש במכרז, בדגש על עמידה בדרישות טכנולוגיה ואבטחת מידע.

5.2.3.3.2. הכישורים והידע הנדרשים ממנהל תשתיות ותקשורת יהיו לפחות:

א. תואר ראשון במדעי המחשב, הנדסה או מדעים מדויקים, עדיפות לתואר שני במקצועות אלה.

ב. בעל ניסיון של 8 שנים לפחות בתחום התקשורת, אמצעי הגנה ואבטחת מידע.

ג. בעל ניסיון מעשי בתכנון והקמת מערכות תשתית, הכולל ניסיון בהגדרת ממשקים טכנולוגיים מבוססי **API** וכן ידע בניהול ממשקי כספות.

ד. בעל ניסיון של לפחות 5 שנים בטיפול שוטף בתשתיות תקשורת ואבטחה של מתקן המכיל מרכיבים דומים לאלה של המערכת.

ה. ניסיון בניהול של פעילות תשתיות ותקשורת בעלת היקף ומורכבות דומים לאלה הניתנים על ידי המערכת.

5.2.3.4. ארכיטקט/מהנדס מערכות בכיר

5.2.3.4.1. ארכיטקט המערכת יהא אחראי על תכנון, עיצוב והכתבת השיטות ונהלי הפיתוח של מערכת הסליקה. ארכיטקט המערכת יהא בעל ניסיון וכישורים המתאימים לתכנון ועיצוב מערכות בהיקף דומה למערכת המאופיינת במכרז זה.

5.2.3.4.2. <u>הכישורים והידע הנדרשים מארכיטקט המערכת יהיו לפחות</u>:

א. תואר ראשון במדעי המחשב, הנדסה או מדעים מדויקים. עדיפות לתואר שני במקצועות האמורים;

ב. ניסיון של 10 שנים לפחות בפיתוח טכנולוגיות מגוונות;

ג. בעל ניסיון מעשי בהובלה טכנית של פרויקט אחד מתמשך לפחות בהיקף של 30 שנות אדם ומעלה, בחמש השנים האחרונות.

5.2.3.5. ממונה הגנת הפרטיות

5.2.3.5.1. ממונה הגנת הפרטיות יהיה אחראי על קביעת מדיניות הגנת הפרטיות, יישומה ואכיפתה, בין היתר בהתאם להוראות המכרז והדין. נושא תפקיד זה יהא בעל כישורים וניסיון מתאימים בהיקף לאחריות על הגנת הפרטיות במערכת בהיקף דומה למערכת המאופיינת במכרז זה.

5.2.3.5.2. הכישורים והידע הנדרשים ממונה הגנת הפרטיות יהיו לפחות:

א. תואר ראשון רלוונטי.

ב. ידע מעמיק בדיני הגנת הפרטיות, הבנה הולמת בטכנולוגיה ואבטחת מידע, והיכרות עם תחומי הפעילות של מערכת הסליקה, בשים לב לאופי עיבוד המידע, נסיבותיו, היקפו ומטרותיו.

ג. ניסיון מקצועי <u>רלוונטי</u> של 5 שנים בחברה עם פעילות בעלת היקף ומורכבות דומים, לרבות מבחינת היקף השירותים ומספר המשתמשים.

5.2.3.5.3. ממונה אבטחת המידע וממונה הגנת הפרטיות, יכולים להיות אותו אדם, בהינתן עמידתו בתנאים המפורטים לתפקידים אלו, משאבים מספקים, היעדר ניגוד עניינים, ובאישור מראש של הממונה.

5.2.3.6. מנהל ה-**Back Office**

5.2.3.6.1. מנהל ה-**Back Office** יהיה אחראי על ניהול התהליכים השוטפים והשונים במערכת הסליקה ובפרט לאלו הנוגעים לסליקה של כספים, וכן יהווה הגורם המקשר בין מס״ב והבנקים למערכת הסליקה, ובין המערכת למשתמשיה השונים. מנהל ה-**Back Office** יהא בעל הכישורים והניסיון המתאימים לניהול ה-**Back Office**.

5.2.3.6.2. הכישורים והידע הנדרשים ממנהל ה-**Back Office** יהיו לפחות:

א. ניסיון של לפחות 5 שנים בתפקיד דומה במוסד פיננסי;

ב. ניסיון של לפחות 5 שנים בעבודה מול גופים מוסדיים, והיכרות עם תהליכי הסליקה והמוצרים הפנסיוניים השונים בתחום החסכון ארוך הטווח.

5.2.4. **מנגנון להחלפת צוות ניהול הפרויקט**

5.2.4.1. הספק רשאי להחליף במהלך תקופת ההתקשרות, את כל אחד מבעלי התפקידים המנויים על צוות הפרויקט לעיל, לרבות מנהל הפרויקט, בהודעה בכתב לרשות לפחות 60 יום מראש וכן למנות מחליף בעל כישורים וניסיון כנדרש לעיל, , תוך 45 יום ממועד ההודעה.

5.2.4.2. מבלי לגרוע מהאמור בסעיף 5.1.4 לעיל המזמין רשאי להתנגד למועמד מחליף והספק יידרש להגיש מועמד אחר. בכל מקרה, אין להשאיר משרה מאלה המנויות תחת סעיף זה, לא מאוישת.

5.2.4.3. הספק יהיה אחראי לקיום חפיפה מלאה בין המחליף לבעל התפקיד היוצא, והכל על חשבונו של הספק.

5.2.4.4. הרשות תהא רשאית, בכל עת, לדרוש מן הספק להחליף מי מצוות ניהול הפרויקט, והספק מתחייב לעשות כן בתוך 30 ימי עבודה. הרשות לא תפצה את הספק או העובד בכל פיצוי שהוא.

5.2.5. **ספקי משנה**

5.2.5.1. הספק יהיה האחראי הבלעדי על מתן השירותים בהתאם לדרישות מכרז זה, הן בגין השירותים אשר יסופקו על ידי הספק והן בגין השירותים אשר יסופקו על ידי ספקי משנה מטעמו, לרבות עמידה בלוחות הזמנים למתן השירותים ועמידת ספק המשנה בתקני אבטחת המידע והגנת הפרטיות כפי שנדרשים במכרז זה ולפי הוראות כל דין.

5.2.5.2. מובהר כי שירותים הניתנים במסגרת פרק השירותים (להלן – **שירותי הליבה של המערכת**) ינתנו על ידי הספק הזוכה בלבד, אלא אם כן ניתן לכך אישור בכתב ומראש מהממונה. ככל שניתן אישור מהממונה להתקשרות עם ספק משנה, הספק הזוכה לא יהיה רשאי להפסיק את ההתקשרות או להחליף את ספק המשנה, ללא אישור מראש של הרשות.

5.2.5.3. כל התקשרות אחרת בין הספק הזוכה לספק משנה תועבר לידיעת הממונה, אשר יהיה רשאי לבטלה.

5.3 צוות הפרויקט הרחב

5.3.1 כללי

5.3.1.1 כלל העובדים המועסקים במסגרת מתן השירותים לפי המכרז, בין אם על ידי הספק ובין אם על ידי ספק משנה, יחתמו על הסכמי סודיות והיעדר ניגוד עניינים.

5.3.1.2 במקרים חריגים, הרשות תהא רשאית, , לדרוש מן הספק להחליף מי מצוות הפרויקט, והספק מתחייב לעשות כן בתוך 30 ימי עבודה. הרשות לא תפצה את הספק או העובד בכל פיצוי שהוא.

5.3.2 הכשרת צוות העובדים

5.3.2.1 הספק יכשיר כל עובד חדש בהתאם לתפקידו, תהליך ההכשרה יתייחס אל רכישת הידע הרלוונטי, לרבות בתחום הטכנולוגי, הרגולטורי והתפעולי.

5.3.2.2 הספק יבצע הכשרות וידאג לשימור הידע בקרב עובדיו, וכן לשמירה על רמה מקצועית גבוהה והכל בהתייחס לנקודות שלהלן:

5.3.2.2.1 השתתפות עובדי הספק בסדנאות, כנסים מקצועיים והכשרות בתחומים רלוונטיים, ככל ויידרש.

5.3.2.2.2 ביצוע הכשרות פנימיות וטכנולוגיות לשיפור מיומנויות הצוותים.

5.3.2.2.3 ניהול ההון האנושי, ובתוך כך:

א. תוכניות לשימור עובדים מוכשרים וקריטיים לתפקוד המערכת;

ב. תהליכים להערכת ביצועים ושיפור מתמיד של עובדי הצוות;

ג. אמצעים לעידוד חדשנות בקרב העובדים.

5.4 ניהול הפרויקט, פיקוח ובקרה

5.4.1 ניהול הפרויקט

5.4.1.1 תפעול מערכת הסליקה, אחזקתה ופיתוחה על ידי הספק הזוכה יהיו כפופים לפיקוח ובקרה מטעם הממונה, באופן אשר יאפשר לרשות להיות מיודעת בפעילותה השוטפת של מערכת הסליקה בהתאם ליעדים ולתוכניות העבודה כפי שהוגדרו בתחילת ההתקשרות, ויעודכנו במהלך הפעילות השוטפת. למזמין תהיה אפשרות לקבוע את האופן והתדירות בו יעדכן הספק באשר לפעילותה של מערכת הסליקה לשם פיקוח ובקרה.

5.4.1.2 <u>מפקח הפרויקט מטעם המזמין</u>

5.4.1.2.1 המזמין ימנה מפקח פרויקט מטעמו אשר יהווה איש הקשר לספק.

5.4.1.2.2 מפקח הפרויקט יפעל כנציג מטעם הרשות מול הספק, מנהליו, ספקי המשנה וצוותי הספק בכל הנוגע למתן השירותים נשוא מכרז זה, ויהיה מוסמך לקבל החלטות במסגרת ההתקשרות.

5.4.1.2.3 הספק יישמע להנחיות ודרישות מפקח הפרויקט או כל גורם אחר מטעמו והמפקח יהווה, מבחינת הספק, כתובת לפנות אליה לכל צורך אשר נובע מההתקשרות ובמהלכה.

5.4.1.2.4 מפקח הפרויקט, או כל גורם אחר מטעמו, יקיים פגישות עם כל גורם מטעמו של הספק, על פי דרישתו וצרכיו, ויהיה רשאי להשתתף בכל פורום או פגישה מקצועית של הספק, ככל שימצא לנכון.

5.4.1.3 <u>מנהלת הפרויקט מטעם הרשות</u>

5.4.1.3.1 עם תחילת שלב ב' של תכנית העבודה (מתן השירותים וקבלת אחריות הספק על המערכת) תוקם מנהלת פרויקט בראשותו של מפקח הפרויקט מטעם הרשות, אשר בה יהיו חברים צוות ניהול הפרויקט וכל גורם נוסף, אשר יתבקש על ידי מפקח הפרויקט.

5.4.1.3.2 תפקידה של המנהלת יהיה לעקוב, להציג, להגיש המלצות, ולדווח למפקח הפרויקט אודות מצב הפרויקט, התקדמות השלבים בתכנית העבודה, וכל נושא נוסף שיתבקש על ידי המפקח.

5.4.1.3.3 למען הסר ספק, ומבלי לפגוע בזכותו של המפקח לקבלת החלטות במסגרת ההתקשרות ועל פי דין, מפקח הפרויקט יהיה הסמכות הבלעדית לקבלת החלטות גם באשר לסוגיות שיועלו במסגרת המנהלת.

5.4.1.3.4 מנהלת הפרויקט תתכנס אחת לחודש, או בתדירות אחרת שתקבע על ידי מפקח הפרויקט מטעם הרשות.

5.4.1.3.5 המנהלת תציג בפני מפקח הפרויקט דיווח שוטף אודות הנושאים הבאים:

א. שלבי מימוש ועמידה בתכנית העבודה, לרבות מעקב אחר התקדמות הפרויקט בהיבטי לו"ז לביצוע משימות ופעילות שוטפת;

ב. עמידה בדרישות הפונקציונליות ובאבני הדרך שהוגדרו בתכנית העבודה;

ג. התקדמות מסמכי האפיון הנדרשים בתכנית העבודה, שלבי הפיתוח וההפעלה השונים ומבדקי המסירה והקבלה;

ד. אירועים חריגים אשר התרחשו כגון תקלות קריטיות, השבתות, אירועי סייבר וכדומה;

ה. עדכונים על שינויים בכללי המערכת ובנהלי העבודה של הספק;

ו. מנהלת הפרויקט תבצע מעקב אחר ניהול הסיכונים בפרויקט, מבלי לגרוע מאחריות הספק כמפורט במכרז זה;

ז. סטטוס העמידה ברמת השירות של הספק, בהתאם להוראות פרק 6 **SLA**;

ח. מידע אודות היקף השירותים הניתנים על ידי מערכת הסליקה;

ט. סטטוס אודות שירותים חדשים שעתידים להיכנס, לרבות תהליכי אינטגרציה מול השוק.

5.4.1.3.6 דיווח במסגרת המנהלת אינו פוטר את הספק מאחריותו על פי דרישות המכרז ועל פי דין.

5.4.1.3.7 כל התכתובות בין מנהל הפרויקט ואנשיו למזמין לאורך התפעול השוטף ייעשו בעברית, למעט סימולים טכניים המקובלים בתחום מערכות המידע והחיסכון הפנסיוני.

5.4.2 פיקוח

5.4.2.1 פעילות הספק תהיה כפופה לפיקוחו השוטף של המזמין. המזמין רשאי לבדוק את פעילות הספק ומי מטעמו בכל עת.

5.4.2.2 הספק ישתף פעולה עם מפקח הפרויקט מטעם המזמין או כל גורם אחר מטעמו. שיתוף פעולה זה יכלול העמדת כל המידע הנדרש, וביצוע הפעולות לשם פיקוח המזמין לפי הנחיות הממונה.

5.4.2.3 הספק יהא אחראי למימון עלות יועצים שיסייעו בפיקוח מטעם המזמין בהיקף של 5,000 שעות ייעוץ של יועץ בכיר לכל תקופת ההתקשרות (במהלך תקופות האופציה יהיה זכאי המזמין לשימוש ב-1,250 שעות לכל תקופת אופציה). יובהר למען הסר ספק, כי למזמין תהיה סמכות לנצל את סך השעות האמור במהלך תקופת ההתקשרות על פי שיקול דעתו בהודעה בכתב לספק. עלות שעת ייעוץ תחושב בהתאם להוראת תכ"ם - הספקת שירותי מחשוב למשרדי ממשלה מס' 16.2.11 (תעריפי גג) או תעריפי התקשרות עם נותני שירותים חיצוניים מס' ה.8.1.1.1, על פי העניין.

5.4.2.4 מובהר בזאת, כי אין בסעיף 5.4.2.3 לעיל מלגרוע מסמכות הממונה לערוך ביקורות על פעילות הספק ולהטיל את הוצאות הביקורת הספק בהתאם להוראות סעיף 97 בחוק הפיקוח על הביטוח כפי שהוחל על מערכת הסליקה בסעיף 31יח לחוק הייעוץ.

5.4.2.5 הספק יהא אחראי למימון גורם חיצוני בלתי תלוי אשר יובא לאישור הרשות לצורך בחינת מוכנות הספק הזוכה למתן השירותים ולמעבר משלב החפיפה לשלב מתן השירותים (שלב ב' בתכנית העבודה).

5.4.2.6 הספק יהא אחראי לביצוע מבחני קבלה לפני הפעלת כל שירות חדש שיופעל, הרשות יכולה לדרוש כי יישום דרישה זו תתבצע על ידי גורם חיצוני (במימון הספק), בדגש על מעבר לטכנולוגית **API**.

5.4.2.7 למען הסר ספק, האמור לעיל אינו פוטר את הספק מאחריותו לבצע בקרה פנימית שוטפת על עמידתו בהוראות המכרז ובהוראות הדין.

5.4.2.8 הספק יכין תכנית בדיקות מקיפה למערכת הסליקה שתתופעל על ידו, אשר לפיה תבוצע הבדיקה טרם ההפעלה המבצעית של המערכת, מבלי לגרוע מבדיקות אחרות הנדרשות על ידי הספק, ובכלל זה הבדיקות הנדרשות בפרק 3 - טכנולוגיה. בנוסף, יכול המזמין לבצע בדיקה מטעמו

או לדרוש מהספק לערוך בדיקות נוספות, לרבות אימות הנתונים שיוצגו על ידי הספק מהבדיקות שיערוך. הספק יציג למזמין את תוצאות הבדיקות.

5.4.2.9 יובהר כי אין באמור כדי לגרוע מכל סמכות הנתונה על פי דין לממונה לפקח על הספק בכל בדיקה נוספת או לתת לספק הוראות.

5.4.3 שגרות ניהול דיווחים ובקרה

5.4.3.1 דיווחים

5.4.3.1.1 דיווחי הספק יועברו לידי הרשות לכל אורך תקופת ההתקשרות ואינם מחליפים פגישות בתדירות שתיקבע או כל חובה אחרת, לרבות העברת דוחות, הקבועה במסמכי המכרז ובדין.

5.4.3.1.2 הספק יעביר לרשות אחת לרבעון או בכל תקופה אחרת שתורה הרשות, באמצעות הפורטל הייעודי לרשות או בכל דרך דיווח שתוגדר על ידה, לאורך כל תקופת הפעילות את הדוחות שלהלן:

א. דוח ריכוז פעילות הכולל את תיאור העבודה המבוצעת – כולל התקדמות למול תכנון מקורי על פי תכנית העבודה;

ב. דוח על משאבי כוח אדם המועסקים (כולל ספקי משנה, ככל ורלוונטי);

ג. דוח על עדכונים ו\או שדרוגים שבוצעו במערכת;

ד. אירועים חריגים אשר התרחשו במהלך התקופה, ובכלל זה ניתוח מקרה של אירועים חריגים ב-**SLA**;

ה. דוחות ניהול הסיכונים בהתאם למפורט בסעיף 5.7 להלן;

ו. דוח אודות ממצאי הבקרות והבדיקות שבוצעו על ידי הספק, הממונה רשאי להגדיר את אופן הדיווח האמור;

ז. דוח כספי שנתי מלא של החברה שיתקבל עד ל-1 לחודש מאי (או תאריך אחר אשר יוגדר על ידי הרשות) בשנה שלאחר השנה אליה מתייחס הדוח.

5.4.3.1.3 אחת לשנה, במועד שייקבע על ידי הממונה, יעביר הספק דוח תקציר מנהלים אשר מסכם עבור הרשות את כלל פעילות המערכת נכון לאותה השנה.

5.4.3.1.4 הרשות רשאית לדרוש מהספק להפיק עבורה דוחות נוספים מכל סוג, בלוחות הזמנים שייקבעו על ידה, ואין באמור כדי לגרוע מסמכות הרשות לבקש מהספק כל מידע אחר על פי הוראות הדין.

5.4.3.1.5 דוחות כמפורט בסעיף 5.4.3.1.2 יוגשו עד ה-10 לחודש העוקב לאחר תום כל תקופת דיווח, אלא אם יוגדר אחרת על ידי הממונה.

5.4.3.1.6 קבלת הדוחות על ידי הרשות אינה מהווה הסכמה לנאמר בהם ו/או ויתור מצד הרשות על זכות מזכויותיה במסגרת התקשרות זו.

5.5 נוהל עבודה

הספק הזוכה יקיים את נהלי המערכת במהלך תקופת החפיפה, ויערוך נוהל עבודה הנוגע לכללי ההתנהלות בכל תקופת ההתקשרות בינו לבין לקוחות המערכת ומשתמשיה (להלן – **נוהל עבודה**), תוך הבחנה בין סוגי הלקוחות והמשתמשים השונים ושלבי תכנית העבודה. נוהל העבודה בין הספק ללקוחות והמשתמשים יועבר לממונה, לכל המאוחר, חודש טרם סיום תקופת החפיפה עם הספק היוצא נוהל יתעדכן על-ידי הספק מעת לעת ויועבר טרם כל עדכון לממונה.

5.6 כללי המערכת

5.6.1 הספק יגבש ויפרסם כללים שיבטיחו את יציבותה, יעילותה ותפקודה התקין של מערכת הסליקה הפנסיונית ואת טיב השירות הניתן ללקוחות ומשתמשיה ובכלל זה את האמצעים לאכיפת הכללים האמורים, על פי הדרישות המפורטות במכרז זה ובחוק הייעוץ הפנסיוני ויעדכן אותם בהתאם לשלבי תכנית העבודה והעלייה לאוויר של מערכת הסליקה וכן עם כל שינוי או עדכון גרסה.

5.6.2 כללי המערכת יהוו את הכללים להפעלת מערכת הסליקה וכן יכללו את ההתאמות והשינויים הנדרשים לצורך חיבור למערכת והעברת מסרים ושדרים באמצעותה. כללי המערכת יאושרו על ידי הממונה טרם פרסומם ויפורסמו בפורטל האינטרנט. כללי המערכת יעודכנו מעת לעת ויפורסמו ללקוחות ומשתמשי המערכת, בעקוב אחר שינויים אל מול כללים שעודכנו או בוטלו לצורך תיעוד ובקרה. טרם פרסומם, כללי המערכת יפורסמו כטיוטה להערות הציבור לתקופה של 21 ימים לכל הפחות, או לתקופה קצרה יותר באישור הממונה. הספק יאפשר בכל עת, גישה ללקוחות ולמשתמשים לכללי מערכת קודמים שבוטלו או שעודכנו לצרכי תיעוד ובקרה.

5.7 ניהול סיכונים והבטחת איכות (QA)

5.7.1 הערכה וניהול סיכונים של הפרויקט

5.7.1.1 הספק יערוך סקר סיכונים במטרה לזהות את כלל הסיכונים להם הספק והמערכת חשופים, להעריך את משמעויות החשיפה לסיכונים שזוהו ולתת המלצות לניהול החשיפה לסיכונים והפחתתם.

סקר הסיכונים יתייחס לכלל הסיכונים המתייחסים למערכת הסליקה ולכל הפחות לסיכונים הבאים:

5.7.1.1.1 סיכון תפעולי, סיכון ציות ואי עמידה בהוראות הדין, סיכון מיקור חוץ, סיכון אסטרטגי, סיכון תדמית.

5.7.1.1.2 הערכת סיכוני טכנולוגיה, אבטחת מידע והגנת הסייבר, הגנת הפרטיות, המשכיות עסקית והתאוששות מאסון, תעשה גם כמפורט בפרק 3 הטכנולוגיה ובפרק 4 אבטחת מידע.

5.7.1.1.3 זיהוי הסיכונים שעלולים להוביל לחריגות משמעותיות בתהליך ההיערכות לרבות לוח הזמנים למתן השירותים בהתאם לתוכנית הפעולה, עמידה בדרישות ה-**SLA**, היעדר משאבים ומקורות מימון/הון הנדרשים להמשך ההיערכות או הפעילות השוטפת וכיו"ב;

5.7.1.1.4 תהליך העברת האחריות על מערכת הסליקה מהספק הקיים;

5.7.1.1.5 מעבר המערכת לטכנולוגיית **API**;

5.7.1.1.6 פרק הזמן בו תינתן תמיכה בטכנולוגית **API** וטכנולוגית כספות במקביל;

5.7.1.1.7 סיכונים שעלולים למנוע אפשרות לעמוד בדרישות היישומיות כמפורט במכרז זה;

5.7.1.1.8 סיכונים שעלולים להוביל לאי עמידה בדרישות הטכנולוגיות במכרז זה, או לקיום של תשתיות בלתי מספקות;

5.7.1.2 סקר הסיכונים יערך לפי פרקטיקות ומתודולוגיות מקובלות, יכסה את כל התהליכים העסקיים מקצה לקצה ויכלול התייחסות פרטנית לכל הסיכונים המהותיים להם חשוף הספק בכל תהליך ושלב, תוך התייחסות לסיכון מובנה וסיכון שיורי, ותוך התייחסות לתוכנית הפעולה להתמודדות עם כל סיכון שתכלול, בין היתר, בקרות קיימות והמלצות לצמצום הסיכון (להלן – תכנית ניהול סיכונים).

5.7.1.3 התוכנית תועבר לממונה, לכל המאוחר, חודש בטרם סיום תקופת החפיפה (שלב א' בתכנית העבודה).

5.7.1.4 התוכנית תעודכן על ידי הספק הזוכה, ותוגש אחת לשנה, עם השינויים המחייבים, חודש לפני מעבר לפי כל אחד מהשלבים בהתאם לתכנית העבודה, או אחת לכל תקופה אחרת, עליה יחליט הממונה, הכל לפי שיקול דעתו הבלעדי.

5.7.1.5 יובהר, כי כל עדכון לתוכנית ניהול הסיכונים יועבר למפקח הפרויקט, וכי לרשות יש זכות לדרוש מהספק לבצע שינויים בתוכנית לניהול הסיכונים במידת הצורך ולפי שיקול דעתה.

5.7.1.6 בשל היות המערכת, מערכת קריטית, תוכנית ניהול הסיכונים תכלול גם תוכנית מגירה/יציאה שתופעל ככל שהספק לא יוכל להמשיך במתן השירותים כנדרש בהוראות או במתכונת הנדרשת על ידי הרשות או מכל סיבה אחרת.

5.7.1.7 הספק יעדכן את תוכנית ניהול הסיכונים כחלק מההיערכות לקראת הפעלת כל שלב נוסף, בהתאם לשלבי תכנית העבודה. הספק ידווח ויבחן באופן שוטף את עמידתו בתוכנית זו ואת התאמתה לסיכונים האפשריים (להלן - דוח ניהול סיכונים).

5.7.2 הבטחת איכות (QA)

5.7.2.1 הספק יערוך תכנית להבטחת האיכות (**QA**) של מערכת הסליקה באופן שוטף לאורך כל תקופת ההתקשרות ויפעל על פיה. תכנית הבטחת האיכות תוגש למפקח הפרויקט. התוכנית תתבסס על הכלים והשיטות המנויים בסעיף 3.16 לעיל.

5.7.2.2 תכנית הבטחת האיכות תתייחס לנושאים הבאים לפחות:

5.7.2.2.1 תכנון תהליך הבטחת האיכות, תדירות בדיקות הבטחת האיכות, חזרות על הבדיקות ודיווח על תוצאותיהן;

5.7.2.2.2 הבטחת האיכות בתהליך הפיתוח;

5.7.2.2.3 תהליך ביצוע בדיקות, לרבות בדיקות מסירה, בדיקות קבלה ובדיקות של משתמשים;

5.7.2.2.4 בדיקות פונקציונליות, בדיקות עומסים, בדיקות מערכת וזמני תגובה;

5.7.2.2.5 בדיקה שוטפת של השירותים שניתנים על ידי מערכת הסליקה ובאמצעות ממשקי המשתמש השונים כאמור בפרק 2 למכרז זה.

5.7.2.3 תכנית הבטחת האיכות תכלול הסבר לכל משימות הבטחת האיכות, לרבות בקרת תיעוד, בקרת קוד, בדיקות יחידה (**unit test**), בדיקות שילוב, ובדיקות מערכת.

5.7.2.4 הספק ידווח לממונה על יישום תכנית הבטחת האיכות אחת לרבעון.

5.8 מימוש כולל של המערכת

5.8.1 תכנית עבודה רב-שנתית להפעלת המערכת על ידי הספק הזוכה

5.8.1.1 הספק הזוכה יציג תכנית עבודה, המבוססת על השלבים המפורטים מטה ועל נוהל ההפרדות מהספק הקיים המצורף כנספח ב.2 לחלק ב' (להלן – **נוהל ההיפרדות מהספק הזוכה**), לאישורו של הממונה.

5.8.1.2 הספק יהיה אחראי לוודא כי היערכות המשתמשים לפעילות מול מערכת הסליקה והתחברות אליה, תואמת את לוחות הזמנים המפורטים בתכנית העבודה ויהיה אחראי להתריע בפני הממונה במקרה של בעיה בעמידה בלוחות הזמנים מיד עם זיהוי הבעיה.

5.8.1.3 לוחות הזמנים בתכנית העבודה יהיו כפופים להוראות הממונה בנוגע למתכונת היישום ומועדים, והספק יאשר מול הממונה כל שינוי בתוכנית.

5.8.2 תכנית עבודה שנתית להפעלת המערכת על ידי הספק הזוכה

5.8.2.1 בתום כל שנה קלנדרית עד ליום 31 בדצמבר לכל שנה, הספק יציג לרשות תכנית עבודה מפורטת לשנת העבודה הבאה.

5.8.2.2 תכנית העבודה השנתית תכלול, בין היתר, התייחסות למימוש דרישות המכרז, יישום אסדרות חדשות שפורסמו, הוספה או גריעה של שירותים, שדרוגים ושיפורים במערכת, לוחות זמנים בתכנית העבודה ומעקב אחר ביצוע משימות בתוכניות העבודה של השנה הקודמת.

5.8.3 להלן שלבי תכנית העבודה:

5.8.3.1 יודגש כי בכל שלב משלבי תכנית העבודה הרשות יכולה לדרוש מהספק הזוכה להגיש לה מסמכים רלוונטיים, לרבות נהלים, מסמכי מדיניות, מסמכי איפיון הפיתוח, מצב שלבי הפיתוח, תוכניות, לוחות זמנים וכו', לפי שיקול דעתה הבלעדי.

5.8.3.2 עוד יודגש, כי הפעילויות המפורטות בטבלה זו הינן הפעולויות העיקריות שעל הספק הזוכה לבצע במסגרת ההתקשרות; יתר הפעילויות הנדרשות במסגרת מסמכי המכרז או על מנת ליישם את דרישות המכרז יפורטו על ידי הספק הזוכה במסגרת הצגת תכנית העבודה הרב שנתית למזמין.

שלב	פעילות	מועד אחרון לביצוע	ציר זמן
שלב מקדים	קבלת הודעת זכיה		T-30
	חתימה על הסכם התקשרות	עד 30 ימים ממועד הזכייה	T
	מינוי בעלי התפקידים הנדרשים בתנאי הסף	מיד עם החתימה על הסכם ההתקשרות	
	הגשת בקשה לקבלת רישיון והמצאת היתר שליטה לממונה (תוך עמידה בכל הדרישות בפרק 1, כגון הקמת חברה להפעלת מערכת סליקה, העמדת הון עצמי וכו')	עד 30 ימים ממועד הזכייה	
שלב א' – תקופת חפיפה עם הספק הקיים (עד 180 ימים) 1) חפיפה עם הספק הקיים לצורך קבלת האחריות על תפעול ותחזוקת המערכת וזאת בהתאם לקבוע בנוהל ההפרדות מהספק הקיים (מצורף כנספח ב.5) (בשלב זה הגורם שנותן שירות ללקוחות והמשתמשים הוא הספק הקיים בלבד) 2) מוכנות לקבלת אחריות על תפעול המערכת ותמיכה בטכנולוגית כספות,	מינוי אנשי צוות הניהול הנוספים כמפורט בסעיף 5.2	תוך 30 ימים מיום חתימת ההסכם	T+30
	הצגת תכנית עבודה רב שנתית לממונה	תוך 45 ימים מיום חתימת ההסכם	T+45
	כתיבת מסמכי מדיניות ונהלים כדוגמת: מסמך הגנת הפרטיות ואבטחת מידע ונוהל אבטחת המידע, כמפורט בפרק אבטחת מידע, מסמך ארכיטקטורה מלא עבור תשתיות מערכת הסליקה הקיימת וכד'. תכנית ניהול סיכונים, נוהל	לכל המאוחר, חודש טרם סיום תקופת החפיפה עם הספק היוצא.	

שלב	פעילות	מועד אחרון לביצוע	ציר זמן
והיערכות לתמיכה בטכנולוגית **API**	עבודה, נוהל שירות ותמיכה וכו'		
	הקמת והכשרת מערך תמיכה ושירות, כמפורט בסעיף 2.5.8 לעיל	חודש בטרם המעבר לשלב ב'	**T**+150
	הגשת תכנית פעולה מפורטת למעבר המערכת לטכנולוגיית **API**	עד 180 יום ממועד ההתקשרות	**T** +180
	הכנת מסמך אפיון מפורט לשירותים הראשונים שיועברו לטכנולוגית **API**	עד 180 יום ממועד ההתקשרות	
	ביצוע בדיקות תוכנה (לרבות בדיקות מסירה, אינטגרציה וקבלה)	בטרם המעבר לשלב ב' ועד 180 יום ממועד ההתקשרות	
	קבלת האחריות על הפעלה ותחזוקה של המערכת ואישור עלייה לאוויר לאחר ביצוע בדיקות מוכנות על ידי גורם חיצוני בלתי תלוי שאושר על ידי הרשות	כתנאי למעבר לשלב ב' ועד 180 יום ממועד ההתקשרות	
שלב ב' – מתן השירותים לפי מסמכי דרישות המכרז והאסדרה שבתוקף אחריות מלאה על המערכת ותמיכה בטכנולוגיית כספות, במקביל למעבר הדרגתי לטכנולוגיית **API** ביחס לשירותים שעברו לטכנולוגיית **API** תמיכה בשתי הטכנולוגיות במקביל	הכנת **Roadmap** למערכת, כולל צפי לגרסאות חדשות, פיתוחים חדשים ועוד	מיד עם קבלת האחריות על המערכת	
	הכנת מסמך אפיון מפורט לכל השירותים במסגרת המעבר לטכנולוגיית **API**	בהתאם ללוחות הזמנים שייקבעו על ידי הרשות עם המעבר לשלב ב'	
	ביצוע בדיקות תוכנה (לרבות בדיקות מסירה, אינטגרציה וקבלה)	60 יום לאחר סיום הפיתוח	
	עלייה לאוויר של השירותים החדשים		
	הדרכות למשתמשים		

שלב	פעילות	מועד אחרון לביצוע	ציר זמן
	השונים ביחס לשירותים החדשים שבשלב זה		
	העברת סיכום שלב ב׳ הכולל תובנות והצעות לשיפור לקראת שלב ג׳ לרשות	מועד סיום שלב ב׳	
שלב ג׳ – מתן כלל השירותים בהתאם למסמכי המכרז והאסדרה ותמיכה מלאה בטכנולוגיית **API**	מעבר של כלל שירותי המערכת לטכנולוגיית **API** וסיום השימוש בטכנולוגיית כספות. עדכון של כל נהלי העבודה הרלוונטיים	בהתאם ללוחות הזמנים שיוגדרו באסדרה בהתאמה לתהליכים ולדרישות לוחות הזמנים שלב ב׳ לעיל	

5.8.3.3 שלב נוסף – סליקה ישירה של כספים על ידי המערכת: יבוצע בהתאם למפורט בסעיף 2.5.5 לעיל ככל ותינתן הודעת הממונה לעניין הפעלת שירות של סליקה ישירה של כספים.

5.9 תקופת החפיפה עם הספק הקיים

5.9.1 הספק הזוכה ינקוט בכל הצעדים והאמצעים על מנת לקבל עליו את האחריות על מערכת הסליקה באופן מיטבי ובהקדם האפשרי, ובהתאם ללוח הזמנים הקבוע באשר לתקופת החפיפה שהיא פרק הזמן ממועד הזכייה במכרז ועד קבלת אחריות להפעלה מלאה של שירותי מערכת הסליקה על ידי הזוכה כאמור בתכנית העבודה, כפי שמפורט בשלב א׳ בתכנית העבודה.

5.9.2 במהלך תקופת החפיפה, על הספק הזוכה ליישם את תהליכי ההיפרדות מהספק הקיים, ועל פי הנחיות הרשות, כמפורט להלן:

5.9.2.1 משך תקופת החפיפה – 180 ימים (למזמין שמורה הזכות לקצר או להאריך תקופה זו, הארכה תהיה ב- 90 ימים נוספים, לכל היותר).

5.9.2.2 בתוך שבועיים ממועד מסירת הודעה על סיום ההתקשרות, יקים הספק הזוכה צוות העברה אשר יעבוד מול נציגי הספק הקיים ו/או נציגי המזמין ככל שיבחר למנות נציגים לשם כך. הספק הזוכה יקים 6 צוותי העברה ייעודיים במשותף עם הספק הקיים, לצורך העברת המידע והתפקידים השונים בין הספקים. בתוך כך יוקמו הצוותים שלהלן:

5.9.2.2.1 **צוות ניהול** – אחראי על תכנון מפרט של תהליך ההיפרדות וניהולו, תאום פעילויות הצוותים השונים ואישורן, מעקב אחרי לוחות זמנים והעברת הנהלים השונים ונוהל ניהול הסיכונים הקיים כיום במערכת הסליקה הפנסיונית;

5.9.2.2.2 **צוות אבטחת מידע** – אחראי על הכנת תכנית אבטחת מידע לתהליך ההיפרדות ומעבר של המערכת בין הספקים, העברת הידע והיכולות, לרבות כל המסמכים הרלוונטיים הדרושים לעבודת מערכת הסליקה;

5.9.2.2.3 **צוות משפטי** – אחראי על ניהול כלל הנושאים המשפטיים והחוזיים בין הספקים, בין השאר, הסבת חוזי צדדי ג' לטובת הספק הזוכה, העברת עובדים רלוונטיים, במידת הצורך והעברת כל מידע משפטי רלוונטי;

5.9.2.2.4 **צוות תשתיות** – אחראי על סיוע בהעברת התשתיות בין הספקים, והכל על פי החלטות המזמין ובתאום מלא בין הספקים, כל זאת תוך מתן סיועי טכני ועדכון התיעוד של כלל התשתיות;

5.9.2.2.5 **צוות פיתוח** – אחראי על העברת קוד המקור של המערכת, תוך כדי קביעת הדרכות מתאימות לראשי הצוותים. ככל וקיימים פרויקטים בפיתוח, יועברו גם הם;

5.9.2.2.6 **צוות תפעול ושירות** – אחראי על העברת הידע והיכולות של מערך השירות והתמיכה, ובכלל זה מוקד הטכני, סוגיות גביה וכו'. במסגרת העברת הידע תעבור חפיפה גם בעניין התהליכים המתבצעים במערך.

5.9.2.3 בתוך 15 ימים מיום הקמת הצוותים, כל צוות יכין תכנית עבודה ייעודית לו, אשר תאושר על ידי הממונה. כל צוות יקיים פגישות חד שבועיות בכדי לעקוב אחר התקדמות תכנית העבודה.

5.9.2.4 תינתן אפשרות לספק הזוכה לקבל גישה סבירה לעובדי הספק הקיים או לספקי המשנה מטעמו לצורך בחינת אפשרות לגייסם או להתקשר עמם.

5.9.2.5 הספק הזוכה ייערך להסבת הסכמים אשר היו לספק הקיים עם צדדים שלישיים על שמו, ככל שספק הזוכה מעוניין בכך והדבר אפשרי, בכל הנוגע לתחזוקה ולשירותים הנוגעים לתפעול המערכת.

5.9.2.6 הספק הזוכה ייערך לקבלת הרישיונות והזכויות הדרושות לצורך הפעלת מערכת הסליקה הפנסיונית, וכל מסמך או הסכם הרלוונטי אליהם.

5.9.2.7 הספק הזוכה ייערך לקבלת משימות פיתוח שנותרו פתוחות מהספק הקיים.

5.9.2.8 לספק הזוכה שמורה הזכות לרכוש או לשכור ציוד שנרכש או הושכר על ידי הספק הקיים לצורך הפעלת המערכת (תמחור הציוד ייעשה בהתאם לשוויו ההוגן, ככל שתהיה מחלוקת ימנה הממונה שמאי בלתי תלוי, עלות ניתוק הציוד והעברתו תהיה על הספק הזוכה), ככל שקיים הסכם SLA נלווה לציוד, יועבר גם הוא לאחריות הספק הזוכה.

5.9.2.9 **זכאות לתמורה הכספית בגין המערכת** - במהלך תקופת החפיפה יהיה זכאי הספק הקיים בלבד לכלל התמורה הכספית; החל ממועד קבלת אחריות מלאה על המערכת (בכפוף לאישור של הרשות לכך) יהיה זכאי לכלל התמורה הכספית - הספק הזוכה בלבד.

5.9.2.10 **תקופת התמיכה** - הספק הזוכה זכאי לקבלת תמיכה מהספק הקיים במהלך השנה הראשונה, החל ממועד קבלת האחריות על המערכת וזאת בתשלום על פי עלויות הספק הקיים לשירותים זהים או דומים, לפי העניין, בתוספת של 15%, ובלבד שעדכן בכך את הממונה טרם קבלת שירותי התמיכה.

5.10 תפעול

5.10.1 תפעול שוטף

5.10.1.1 המערכת תתופעל על ידי הספק באתרי הספק ובאחריותו. הספק יחזיק משרד קבוע, המאויש בשעות העבודה המקובלות, לשם מתן שירות זמין ללקוחות ולממונה לאורך כל תקופת ההתקשרות.

5.10.1.2 מנהל הפרויקט מטעם הספק יקיים מפגשי עבודה בישראל בתדירות שנתית לפחות (או בתדירות אחרת, על פי קביעת הממונה), עם גופים מוסדיים ובעלי רישיון יועץ פנסיוני או נציגות שלהם, נציגות מעסיקים ו/או לשכות שירות לשכר אשר יוגדרו על ידי הממונה. הפגישות כאמור יתועדו בפרוטוקול פגישה.

5.10.2 אחריות כוללת לתחזוקת המערכת

5.10.2.1 הספק יישא באחריות כוללת לאיכותם ולתקינותם של כל רכיבי המערכת, ובכלל זה אחריות שוטפת לתפעולה השוטף של המערכת,

תחזוקתה, ותיקון כל תקלה או בעיה בה, וזאת החל מתום שלב א', כמתואר בתכנית העבודה, וללא תמורה נוספת מלבד התמורה המפורטת בפרק 7 - מודל התמחור להלן.

5.10.2.2 אחריות זו של הספק תכלול את כל סוגי התקלות ובכל הרמות, ובכלל זה: תקלות תוכנה, ליקויים בעיצוב או באפיון, ליקויים בתיעוד, בעיות ביצועים וכו'. כמו כן, הספק יהיה אחראי לפיתוח רכיבים חדשים ולשיפור רכיבים קיימים לפי בקשת המזמין. לרשות שיקול דעת בהסרת האחריות והחבות כאמור או בצמצומה בכפוף לדין.

5.10.2.3 האחריות הבלעדית לתיקון תקלות תהיה על הספק והוא האחראי על פתרונן מול הגורמים הרלוונטיים ויעשה כל מאמץ כדי לוודא שהפתרון יתממש בהקדם האפשרי.

5.10.2.4 הספק ישתף פעולה עם גורמים נוספים על מנת לפתור כל בעיה במערכת, כזו אשר מקורה במערכת וכזו שלא, ויעשה כמיטב יכולתו כדי לסייע לפתור את הבעיה בהקדם האפשרי.

5.10.3 **בדיקות המערכת ועדכוני גרסאות**

5.10.3.1 הספק יגיש לממונה תוכניות מפורטות לבדיקת מערכת הסליקה (להלן – **תוכניות בדיקה**) כחלק מתכנית העבודה השנתית, לרבות בדיקות תוכנה בכפוף לעקרונות בפרק 3 טכנולוגיה. בהתאם ללוחות הזמנים המפורטים בתכנית העבודה. הממונה רשאי לדרוש שינויים בתוכניות הבדיקה השונות לפני אישורן והפעלתן. על מקרי הבדיקה לכלול את כל המקרים הגבוליים והמשמעותיים, כולל מקרי הצלחה ומקרי כישלון.

5.10.3.2 מבחני הקבלה יתבצעו על המוצר המוגמר לאחר שאישר הספק כי המערכת נבדקה על ידו וכי ביצע את התיקונים הנדרשים בעקבות מבחני המסירה שביצע הוא עצמו. הספק יביא לאישור הממונה טרם ביצוע מבחני הקבלה את תיק מבחני הקבלה (תרחישים מפורטים) וכן יביא לעיון הממונה את תוצאות מבחני המסירה שבוצעו על ידי הספק. מבחני הקבלה יתייחסו לכלל ממשקי המשתמש, התהליכים והשינויים הרלוונטיים לגרסה הנבדקת.

5.10.3.3 תוצאות מבחני הקבלה והתוכנית לתיקון הליקויים יועברו לעיון הממונה, עם סיום מבחני הקבלה וטרם העלאת הגרסה לאוויר. יחד עם זאת, הספק ידווח מידית לממונה על כל ליקוי מהותי שיש בידו

בכדי לעכב את העלאת הגרסה בצירוף לו"ז לתיקון הליקוי. אין באמור לגרוע מכל סמכות הנתונה לממונה על פי המכרז והדין.

5.10.4 השבתה יזומה של מערכת הסליקה ועדכון גרסאות

5.10.4.1 ככלל התחזוקה, התפעול השוטף ועדכון הגרסאות של מערכת הסליקה לא יפגעו בזמינות המערכת. על אף האמור לעיל, במקרה של השבתת פעילות יזומה של מערכת הסליקה לצרכי תחזוקה, ההשבתה תיעשה תוך עמידה ביעדי זמינות המערכת המפורטים בסעיף 6.3.1 לעיל.

5.10.4.2 השבתת פעילות מערכת הסליקה לצרכי תחזוקה, תיקון תקלות ועדכון גרסאות באופן יזום, תעשה אך ורק בסופי שבוע (מיום חמישי לאחר השעה 19:00 ועד יום ראשון העוקב בשעה 7:00). השבתה כאמור תיעשה בשעות בהן הפעילות במערכת הנמוכה ביותר. אלא אם הממונה יאשר מועדים אחרים.

5.10.4.3 מבלי לגרוע מהאמור לעיל, השבתת פעילות יזומה של מערכת הסליקה תיעשה לאחר קבלת אישור הממונה ולאחר שניתנה ללקוחות המערכת התראה מוקדמת של 10 ימי עסקים לפחות.

5.10.5 עדכניות טכנולוגית

5.10.5.1 הספק יהיה אחראי לעדכניות הטכנולוגית והתפעולית של כל הציוד, התוכנה, החומרה, התשתיות והתקשורת המרכיבים את המערכת באופן שיאפשר מתן שירות מיטבי ומאובטח תוך שמירה על פרטיות הלקוח ועמידה בדרישות ה-**SLA** הנוגעות לרמת השירות במתן השירותים לכל אורך תקופת ההתקשרות.

5.10.6 תכנון נפח העבודה (Capacity Planning)

5.10.6.1 הספק יאפשר גישה זמינה ונוחה למערכת הסליקה לכלל הלקוחות והמשתמשים, בו-זמנית וינקוט בכל האמצעים הנדרשים להבטחת עמידה ברמת השירות כמפורט בפרק 6 **SLA**.

5.10.6.2 הספק יינטר באופן שוטף את תפוקות וביצועי המערכת באמצעות מערכות ממוכנות המיועדות לכך. המעקב ישמש לשם היערכות למצבים אפשריים של עומס יתר, אשר עלולים לפגוע ברמת השירות.

5.10.6.3 על הספק יהיה להתאים את קיבולת המערכות התומכות לנפח הפעילות על מנת להימנע ככל הניתן ממצבים של עומס יתר על המערכת אשר ישפיעו על איכות השירות.

5.11 סיום התקשרות ונוהל היפרדות

5.11.1 עם קבלת הודעה מהרשות בכתב על סיום ההתקשרות, הספק יידרש לפעול בהקדם וללא דיחוי, כמפורט להלן:

5.11.1.1 לפעול בהתאם למפורט בנוהל ההיפרדות מהספק הזוכה המצורף כנספח ב.2 לחלק ב', ובמסגרת זו להעביר לספק שיחליף את הספק הזוכה או לרשות או למי מטעמה (להלן – **הספק המחליף**) בהתאם להוראות הממונה, באופן מסודר את כל הנתונים, התוצרים, המידע והידע שהצטברו אצלו במהלך הפעילות, ואת כל התוצרים שנוצרו במהלך הפרויקט, כשהם מעודכנים, קריאים ובפורמטים שהוגדרו ואושרו מראש על ידי הרשות.

5.11.1.2 לשתף פעולה באופן מלא עם הרשות, עם מפקח הפרויקט מטעמה ועם הגורם שיוגדר כמחליפו, ולפעול לפי נוהל ההיפרדות, כדי לאפשר את ההתארגנות, ההחלפה והמשכה התקין של הפעילות לאחר סיום ההתקשרות עם הספק.

5.11.1.3 לאפשר לנציגי הרשות ועם הגורם שיוגדר כמחליפו, להיפגש עם כל בעל תפקיד בפרוייקט (וככל שיתאפשר, גם בעל תפקיד לשעבר בפרוייקט), לצורך ביצוע חפיפה ו/או מיפוי ותיעוד של הידע והמידע שברשות הספק.

5.11.1.4 להמשיך לטפל בכל המשימות שבאחריותו, עד לסיום ההתקשרות וסיום העברת המידע והידע, כאמור.

5.11.1.5 בסיום ההיפרדות, על הספק למחוק ולהשמיד כל העתק של המידע שברשותו, בהתאם להוראות כל דין והרשות.

5.11.2 **נוהל היפרדות מהספק הזוכה בסיום ההתקשרות**

5.11.2.1 התהליכים והאמצעים שיינקטו במקרה של סיום ההתקשרות בין הספק הזוכה לבין המזמין, כמו גם המשמעויות הפיננסיות של סיום ההתקשרות, מוגדרים בנוהל היפרדות. מטרת נוהל ההיפרדות הינה לאפשר העברת רכיבי המערכת ותפעול המערכת באופן מסודר מהספק הזוכה לרשות ו/או לספק המחליף בסיום ההתקשרות נשוא מכרז זה.

5.11.2.2 נוהל ההיפרדות (נספח ב.2) יתעדכן אחת לשנה על ידי הספק או בפרק זמן אחר, לפי החלטת הרשות.

פרק 6 – SLA

6.1 כללי

6.1.1 פרק זה מגדיר מדדי שירות בהם נדרש הספק לעמוד במסגרת מתן השירותים.

6.1.2 הספק יהיה האחראי הבלעדי לזמינותה המלאה של מערכת הסליקה, בכל ימות השנה, כולל שבתות וחגים בכל תקופת ההתקשרות.

6.1.3 הספק יהיה האחראי הבלעדי לזמינות כלל השירותים הנלווים שניתנים על ידו בהתאם לתנאי מכרז זה במועדים הקבועים בו.

6.1.4 הספק נדרש לעמוד ב- 6 מדדי שירות, על פי המפורט להלן:

- זמינות מערכת הסליקה;
- זמני תיקון תקלות;
- זמני ביצוע של הוראות הממונה;
- זמני ביצוע טכניים של פעולות המערכת;
- איכות שירות הלקוחות;
- פרק הזמן להתאוששות מאסון.

6.1.5 ביחס לכל מדד להלן יפורטו היעדים, תוך ציון דרישת המינימום ואופן המדידה ויוגדר אופן קביעת ציון העמידה ביעד לכל מדד.

6.1.6 אירוע או תקלה המשפיעים על מספר מדדים, או סדרת אירועים הקשורים זה בזה, ימדדו מול מדד השירות המחמיר ביותר.

6.1.7 כמו כן, יוגדר מנגנון פיצוי מוסכם בהתייחס לאי עמידה ביעדים של מדדי השירות, בהתאם לחישוב רבעוני, כמפורט בסעיף 6.5 להלן.

6.1.8 על אף האמור לעיל, פירוט מדדי השירות אינו גורע מחובתו של הספק לעמוד בכל דרישות הדין ומכרז זה בכל הנוגע ללוחות זמנים למתן שירותי המערכת והשירותים הנלווים.

6.1.9 הספק אחראי למדידת רמת השירות ולבקרה ומעקב אחר רמת השירות, באמצעות כלים ממוכנים.

6.1.10 הממונה יהיה רשאי להחליט על עדכון מדדי השירות והיעדים וזאת בהתאם לתוצאות השנה שחלפה, מתוך מטרה לשפר את רמת השירות ו/או בעקבות שדרוגים טכנולוגיים המאפשרים שיפור ביצועים ו/או בעקבות שינויים בשירותים הניתנים על ידי מערכת הסליקה. עדכון כאמור יבוצע אחת לשנה במידת הצורך, הכל על פי החלטת הממונה.

6.2 דוחות מעקב

6.2.1 הספק יהיה אחראי למדידת רמת השירות (להלן – **דוח רמת שירות**) בכל אחד מהמדדים המפורטים בסעיף 6.1.4 לעיל, למעט בשנה הראשונה לפעילות שתחל בתום תקופת החפיפה ועד לתום השנה הקלנדרית במסגרתה ידווח אחת לחודש בתחילת כל חודש לגבי החודש שחלף. על אף האמור, דוח רמת השירות המתייחס למדד התאוששות מאסון יימדד אחת לשנה בלבד. הדוחות כאמור יונגשו לממונה בפורטל הייעודי לרשות, לכל המאוחר, בתוך 10 ימי עסקים מסיום המועד עליו הם מדווחים.

6.2.2 מתכונת הדוחות תאושר על ידי הממונה, ותכלול הצגה גראפית של מדידת כל אחד ממדדי רמת השירות. עבור כל מדד, יציג הספק את דרך או שיטת המדידה וניתוח הגורמים שהביאו לרמת השירות והתפלגות, בחלוקה לפרקי זמן (ימים, שבועות, חודשים ורבעון – במידה ורלבנטי). הדוח יכלול, עבור כל מדד, הצגת ערכים מצטברים מתחילת השנה והשוואה לתקופה מקבילה.

6.3 מדדי שירות

להלן פירוט מדדי השירות:

6.3.1 <u>זמינות מערכת הסליקה:</u>

השירותים אותם מספקת המערכת ללקוחותיה ובכלל זה השירותים הניתנים באמצעות פורטל האינטרנט, יהיו זמינים ללקוחות והמשתמשים 24 שעות ביממה בכל ימות השנה, למעט השבתות שאושרו על ידי הרשות.

6.3.1.1 **מדידת זמינות המערכת:**

זמינות המערכת נמדדת ביחס לפרק זמן של רבעון. "שעות הזמינות של המערכת ברבעון" יחושבו לפי "סך השעות ברבעון" בניכוי "שעות אי-זמינות ברבעון" (השעות בהן המערכת לא הייתה זמינה כתוצאה מתקלה משביתה, כמפורט להלן). שיעור הזמינות הוא שעות הזמינות של המערכת ברבעון לחלק למספר סך השעות ברבעון.

6.3.1.2 **יעד הזמינות:**

יעד הזמינות של המערכת יהיה לא פחות מ- 99.5% מהזמן. כך למשל, ברבעון בו סך השעות הוא 2,190 שעות, על המערכת להיות זמינה לפחות 2,179 שעות על מנת לעמוד ביעד בהצלחה. לפי דוגמה זו, יעד זה יאפשר, לכל היותר, 11 שעות אי-זמינות ברבעון. יובהר כי, אין האמור בכדי לגרוע מרציפות פעילות המערכת במהלך כל הרבעון.

6.3.1.3 שעות אי זמינות יכללו גם שעות של השבתה יזומה של המערכת אשר אושרה מראש על ידי הרשות. אף על פי כן, השבתה יזומה אחת ברבעון אשר אושרה על ידי הרשות לצורך תחזוקה או שדרוג של המערכת, על פי החלטת הממונה יכולה שלא תובא במניין שעות אי-הזמינות לצורך החישוב.

6.3.1.4 אופן מתן הציון של יעד הזמינות

לעניין העמידה ביעד הזמינות של המערכת, נקבע אופן מתן הציון שלהלן:

א. אם המערכת עמדה ביעד הזמינות - ציון 100.

ב. אם המערכת הייתה זמינה רק 80% מהזמן - ציון 0 (קרי, לפי הדוגמה לעיל, הייתה זמינה במשך 1,752 שעות בלבד).

ג. אם המערכת הייתה זמינה פרק זמן שבטווח שבין פרקי הזמן המפורטים בסעיפים א' ו-ב' לעיל - ציון יחסי (קרי, לפי הדוגמה לעיל, זמינות של 2,000 שעות תזכה בציון של 91.7).

6.3.2 **<u>עמידה בזמני תיקון תקלות</u>**

6.3.2.1 סוגי התקלות

התקלות יסווגו ל-3 סוגי תקלות:

א. תקלה משביתה - תקלה המשביתה את כלל המערכת או משביתה פונקציה המהווה חלק מהותי מתהליך העבודה במערכת. מבלי לגרוע מהאמור לעיל, תקלה משביתה תיחשב גם אחת מאלה:

- תקלה שמונעת עבודה סדירה של כל הלקוחות או משתמשי המערכת בערוץ גישה בטכנולוגיה ספציפית (למשל ב- **API** או בכספות).
- תקלה המונעת עבודה סדירה של כל הלקוחות או המשתמשים מסוג מסוים.
- תקלה המונעת השלמת בקשה או פעולה שחלה עליה חובת שימוש במערכת (בהתאם לחוזר חובת שימוש), לרבות קבלת מענים וצפייה בהם.
- תקלה המשבשת את פעולת הסליקה הכספית ו/או דיווח על הפקדות.

- תקלת אבטחת מידע המסכנת את הפרטיות של לקוחות המערכת.
- האטה משמעותית של המערכת ביחס אל רמת הביצועים הנדרשת על פי מכרז זה והוראות הממונה.
- תקלה שתוגדר כתקלה משביתה על ידי הממונה.

ב. תקלה מהותית - היא תקלה המשפיעה על קבוצה משמעותית של לקוחות ומשתמשים. לצורך מדידת השפעת התקלה נקבע ניקוד, כמפורט להלן:

- גוף מוסדי - 30 נקודות
- משתמש שהוא מתפעל הסדרים פנסיוניים או מערכת התומכת בשירותי בעלי רישיון - 6 נקודות
- לקוח או בעל רישיון יחיד שאינו גוף מוסדי - 1 נקודות

תקלה מהותית היא תקלה לה מיוחסת השפעה של 30 נקודות לפחות.

ג. תקלה אחרת - כל תקלה שאינה תקלה משביתה או תקלה מהותית.

ד. אם תקלה שמסווגת כתקלה אחרת, חוזרת על עצמה יותר מפעמיים ברבעון, אזי מהפעם השלישית ואילך היא תסווג כתקלה מהותית.

ה. אם תקלה שמסווגת כתקלה מהותית חוזרת על עצמה יותר מפעמיים ברבעון, אזי מהפעם השלישית ואילך היא תסווג כתקלה משביתה.

ו. לעניין תקלות חוזרות, כפי שמפורטות לעיל, תקלה שחוזרת על עצמה יותר מפעם אחת, תיבחן ללא קשר לזהות הלקוח או המשתמש אלא לפי מהות התקלה.

6.3.2.2 **דיווח לממונה אודות תקלות:**

הספק יעביר דיווח מידי למזמין, הכולל תיאור של מהות התקלה והיקפה, ועדכון שוטף עד לסיום הטיפול בתקלה, עבור סוגי התקלות הבאות:

א. תקלה המשביתה את פעולת מערכת הסליקה למשך רבע שעה או יותר;

ב. תקלה המשביתה את הפעילות של גוף מוסדי במערכת למשך שעה או יותר;

ג. תקלה המשביתה את החיבור או פעילות של סוג משתמש מסוים שאינו גוף מוסדי למשך שלוש שעות או יותר;

ד. תקלה המשביתה או המונעת את החיבור של יותר מ-1% מהלקוחות או 10% מסוג כלשהו של משתמשים למשך יותר מ-4 שעות או יותר.

6.3.2.3 **מועדי תחילת הטיפול בתקלות**:

א. מועד תחילת הטיפול בתקלות יבוצע מיד עם הגילוי או הדיווח על התקלה למערכת הסליקה, לפי המוקדם.

ב. על אף האמור לעיל, מועד תחילת הטיפול בתקלה אחרת (שאינה מהותית או משביתה) אשר התגלתה או דווחה שלא בשעות העבודה המקובלות, יכול להתבצע מיד עם תחילתו של יום העבודה הבא.

6.3.2.4 זמני הטיפול המקסימאלי בתקלות לפי חומרתן:

דרגת החומרה	מועד מקסימאלי לסיום הטיפול * (שעות)
תקלה משביתה	12
תקלה מהותית	24
תקלה אחרת	72

* הטיפול בתקלות ייעשה באופן רציף החל ממועד הגילוי או הדיווח על התקלה למערכת הסליקה, לפי המוקדם, ועד לפתרונה.

6.3.2.5 דרך חישוב מדד טיפול בזמני התקלות

מדד זה יחושב כממוצע משוקלל של אופן העמידה ביעד המתייחס לזמני התיקון של התקלות השונות לפי חומרתן (בכל שורה) כמפורט בטבלה לעיל:

הציונים לחישוב העמידה ביעד יחושבו כדלהלן:

א. תקלה שתוקנה במסגרת הזמן המקסימאלי לתיקונה - ניקוד של 100 נקודות.

ב. תקלה שתוקנה בכפל הזמן המקסימאלי לתיקונה - ניקוד של 0 נקודות.

ג. ניקוד של תקלה שתוקנה בין פרק הזמן המקסימלי לבין כפל פרק זמן זה, יחושב באופן יחסי.

ד. המדד הוא הציון המשוקלל של כלל התקלות ברבעון, כאשר המשקל לחישוב המדד יהיה כדלקמן:

- הציון הממוצע שיינתן על טיפול בכלל התקלות המשביתות – 50%
- הציון הממוצע שיינתן על טיפול ביתר התקלות (שאינן משביתות) – 50%

ה. ציון משוקלל של 95 ומעלה ייחשב כציון 100 במדד; מתחת ל-95 יינתן ציון באופן יחסי.

ו. כך למשל, אם ברבעון מסוים יתרחשו 20 תקלות, על פי פילוח זה - 2 תקלות משביתות, ו-18 תקלות שאינן משביתות (מהותיות ואחרות) - כאשר כלל התקלות טופלו בתוך מסגרת הזמן המקסימלי לטיפול (כלומר, מזכות בציון 100), מלבד תקלה משביתה אחת שטופלה תוך 15 שעות (ולא תוך 12 שעות שהוא הזמן המקסימלי לטיפול). הציון של התקלה המשביתה הוא 75

במקרה כזה, הניקוד המשוקלל במדד טיפול בזמני התקלות ברבעון זה יחושב כך:

[(100*1+75*1)/2]*50%+[(100*18)/18]*50%=93.75

בדוגמה זו, הציון שייתנן לספק במדד יהיה 93.75/95 = 98.7, בהתאם לסעיף ה' לעיל.

6.3.3 <u>זמני ביצוע של הוראות הממונה</u>

מדד זמני ביצוע הפעולות יחושב כממוצע משוקלל של אופן העמידה ביעדים של זמני הביצוע של הפעולות כמפורט בטבלה להלן:

פעולות	זמן מקסימלי לביצוע	ציון	משקל יחסי
רישום בעל רישיון יחיד למערכת מרגע הגשת הבקשה (מתייחס לרישום למערכת לראשונה)	3 שעות	95% ומעלה מהפעולות עומדות בזמן בתקן = ציון 100 75% ומטה מהפעולות עומדות בזמן בתקן = ציון 0	16.66%

פעולות	זמן מקסימלי לביצוע	ציון	משקל יחסי
קליטת קובץ לשידור בממשק מעסיקים (או דחייתו עם פירוט השגיאה) מרגע טעינתו בפורטל האינטרנט	20 דק	95% ומעלה מהפעולות עומדות בזמן בתקן = ציון 100 75% ומטה = ציון 0	16.66%
שליחת חיווי ללקוח או משתמש לאחר קליטת בקשה	30 דקות	95% ומעלה מהפעולות עומדות בזמן בתקן = ציון 100 75% ומטה = ציון 0	16.66%
שליחת הבקשה לגוף המוסדי מרגע קבלתה ממשתמש או מהלקוח	20 דקות	95% ומעלה מהפעולות עומדות בזמן בתקן = ציון 100 75% ומטה = ציון 0	16.66%
שליחת מענה ללקוח או משתמש מרגע קבלת המידע מהגוף המוסדי	20 דקות	95% ומעלה מהפעולות עומדות בזמן בתקן = ציון 100 75% ומטה = ציון 0	16.66%
סה"כ			**100%**

6.3.3.1 הרשות רשאית לשנות ולעדכן את הפעולות המנויות לעיל ואת זמני הביצוע בהתאם להתקדמות ביישום תכנית העבודה וביחס לטכנולוגיה הרלוונטית.

6.3.3.2 דרך חישוב מדד זמני ביצוע פעולות

א. הבסיס לחישוב בכל שורה מבטא את כמות הפעולות שבוצעו על ידי המערכת באותו הרבעון.

ב. ציון כל שורה יחושב על פי כלל הפעולות שעמדו ביעד לעומת סך כל הפעולות שבוצעו.

ג. אם 95% ומעלה מהפעולות בשורה עמדו ביעד – הניקוד עבור השורה יהיה 100.

ד. אם 75% ומטה מהפעולות בשורה עמדו ביעד – הניקוד עבור השורה יהיה 0.

ה. הניקוד עבור שורות בהן הפעולות עמדו בטווח בין 75% ל-95%, יחושב באופן יחסי. כך למשל, עמידה של 85% מהפעולות ביעד תזכה את השורה בניקוד של 50.

ו. הציון במדד הוא הסכום של [ניקוד בכל שורה] כפול [משקל יחסי של כל שורה המדד].

ז. הרשות רשאית לשנות את המשקלים, ולעדכן את הפעולות המנויות לעיל ואת זמני הביצוע בהתאם להתקדמות ביישום תכנית העבודה וביחס לטכנולוגיה הרלוונטית.

6.3.4 זמני ביצוע טכניים של פעולות המערכת

6.3.4.1 מדד זה יחושב כממוצע משוקלל של אופן העמידה ביעדים של זמני הביצוע בפעילויות הבאות כמפורט בטבלה להלן:

פעולות טכניות	זמן מקסימלי לביצוע	ניקוד	משקל יחסי
טעינה ומעבר בין דפים באתר ובאפליקציה	3 שניות	95% ומעלה מהפעולות עומדות בזמן בתקן = ניקוד 100 75% ומטה מהפעולות = ניקוד 0	10%
שאילתת חיפוש בנתוני מערכת הסליקה	5 שניות	95% ומעלה מהפעולות עומדות בזמן בתקן = ניקוד 100 75% ומטה = ניקוד 0	20%
העברת משוב ללקוח על קבלת הבקשה למידע או ביצוע פעולה במערכת הסליקה	5 שניות	95% ומעלה מהפעולות עומדות בזמן בתקן = ניקוד 100 75% ומטה = ניקוד 0	20%
אחזור פרטי בקשה מפורטים	5 שניות	95% ומעלה מהפעולות עומדות בזמן בתקן = ניקוד 100 75% ומטה = ניקוד 0	20%
הפקת דוחות לבקשת לקוח או משתמש באמצעות הפורטל	10 שניות	95% ומעלה מהפעולות עומדות בזמן בתקן = ניקוד 100 75% ומטה = ניקוד 0	20%
מענה לבירור בנושא גביית דמי השימוש או סליקת כספים	2 ימי עסקים	95% ומעלה מהפעולות עומדות בזמן בתקן = ניקוד 100 75% ומטה = ניקוד 0	10%
סה"כ			**100%**

6.3.4.2 הרשות רשאית לשנות את המשקלים, לעדכן את הפעולות המנויות לעיל ואת זמני הביצוע בהתאם להתקדמות ביישום תכנית העבודה וביחס לטכנולוגיה הרלוונטית.

6.3.4.3 דרך חישוב מדד זמני ביצוע טכניים של פעולות המערכת

א. הבסיס לחישוב כל שורה מבטא את כמות הפעולות שבוצעו על ידי המערכת באותו הרבעון.

ב. ניקוד כל שורה יחושב על פי כלל הפעולות שעמדו ביעד לעומת סך כל הפעולות שבוצעו.

ג. אם 95% ומעלה מהפעולות בשורה עמדו ביעד – הניקוד עבור השורה יהיה 100.

ד. אם 75% ומטה מהפעולות בשורה עמדו ביעד – הניקוד עבור השורה יהיה 0.

ה. הניקוד עבור שורות בהן הפעולות עמדו בטווח בין 75% ל-95%, יחושב באופן יחסי.

ו. לכל שורה נקבע משקל כמפורט בטבלה , באופן שיאפשר מדידה של הציון הכולל עבור מדד זה בהתאם לסך המשקולות.

ז. הרשות תוכל לעדכן את המשקלים , הפעולות והזמנים לביצוע לעיל, על פי שיקול דעתה.

6.3.5 **<u>מדד איכות שירות הלקוחות</u>**

מערך השירות והתמיכה יספק מענה מלא כנדרש בפרק 2 השירותים. על הספק למלא אחר דרישות העמידה בזמני המענה לכל אחד משלושת סוגי המדדים, על פי הפירוט שלהלן:

א. מדד זמני המענה בערוצים השונים

6.3.5.1 <u>מענה טלפוני</u>

א. <u>הדרישה המינימאלית</u>: מענה על לפחות 80% מהשיחות בתוך 60 שניות (מסיום **IVR**).

ב. <u>הניקוד</u>:

1) עמידה מלאה בסעיף א' תזכה בניקוד 100.

2) מענה על מתחת ל-50% מהשיחות כנדרש בסעיף א לעיל, יזכה בניקוד 0.

3) הניקוד בטווח שבין 50% ל-80%, יחושב באופן יחסי.

6.3.5.2 <u>תקשורת כתובה</u>

6.3.5.2.1 <u>מענה לפנייה באמצעות יישומון **WhatsApp**</u> (או יישומון אחר/נוסף, באישור הממונה)

א. <u>הדרישה המינימאלית</u>: מענה אנושי ראשוני על לפחות 80% מהפניות בתוך 4 דקות (מסיום **IVR**).

ב. <u>הניקוד</u>:

1) עמידה מלאה בסעיף א' תזכה בניקוד 100.

2) מענה על מתחת ל-50% מהפניות כנדרש בסעיף א לעיל, יזכה בניקוד 0.

3) הניקוד בטווח שבין 50% ל-80%, יחושב באופן יחסי.

6.3.5.2.2 <u>מענה לפנייה באמצעות דוא"ל ובאמצעות פורטל האינטרנט</u>

א. <u>הדרישה המינימאלית</u>: מענה אנושי ראשוני על לפחות 90% מהפניות עד לסוף יום העסקים הבא.

ב. <u>הניקוד</u>:

1) עמידה מלאה בסעיף א' תזכה בניקוד 100.

2) מענה על מתחת ל-50% מהפניות כנדרש בסעיף א לעיל, יזכה בניקוד 0.

3) הניקוד בטווח שבין 50% ל-90%, יחושב באופן יחסי.

ב. מדד שביעות רצון

6.3.5.3 לשם בדיקת מדד זה, הספק יפיץ סקרי שביעות רצון למשתמשים וללקוחות אשר פנו למערך השירות והתמיכה, בכל אחד מערוצי התקשורת וסוגי הפניות הקיימים, לפי העניין ובהתאם לקבוע בנוהל שירות ותמיכה, כמפורט בסעיף 2.5.8.14 בפרק השירותים.

6.3.5.4 אחת לרבעון יסוכמו תוצאות הסקרים ויינתן ניקוד על פי המפורט בסעיף זה.

6.3.5.5 הסקר שיישלח יכלול ציון לכל סעיף, כאשר 1 הוא הנמוך ביותר ו- 5 הוא הגבוה ביותר, והציון בסקר ייקבע על פי הממוצע של כלל סעיפיו.

6.3.5.5.1 <u>סקר שביעות רצון מהמענה והטיפול במוקד</u>:

א. <u>הדרישה המינימאלית</u>: מתן ציון ממוצע של 4 ומעלה על ידי לפחות 90% מהנשאלים.

ב. <u>הניקוד</u>:

1) עמידה מלאה בסעיף א' תזכה בניקוד 100.

2) מתן ציון של 4 ומעלה על ידי 60% ומטה מהנשאלים, יזכה בניקוד 0.

3) הניקוד בטווח שבין 60% ל-90%, יחושב באופן יחסי.

6.3.5.5.2 <u>סקר שביעות רצון מאופן מתן השירותים שניתנים למשתמשים וללקוחות על ידי מערכת הסליקה</u>:

א. <u>הדרישה המינימאלית</u>: מתן ציון ממוצע של 4 ומעלה על ידי לפחות 90% מהנשאלים.

ב. <u>הניקוד</u>:

1) עמידה מלאה בסעיף א' תזכה בניקוד 100.

2) מתן ציון של 4 ומעלה על ידי לפחות 60% ומטה מהנשאלים, יזכה בניקוד 0.

3) הניקוד בטווח שבין 60% ל-90%, יחושב באופן יחסי.

ג. מדד FCR של המוקד

מדד זה מודד את הפניות אשר נסגרו במהלך ההתקשרות הראשונה עם הלקוח או המשתמש, כלומר פניות שבהם הלקוח או המשתמש קיבל מענה מלא ופתרון במהלך ההתקשרות הראשונה שלו עם המוקד.

א. <u>הדרישה המינימאלית</u>: סגירת פניות ב-**FCR** של לפחות 75% מהפניות שהתקבלו במוקד.

ב. <u>הניקוד</u>:

1) עמידה מלאה בסעיף א' תזכה בניקוד 100.

2) סגירת פניות ב-**FCR** של 50% ומטה מהפניות שהתקבלו במוקד, תזכה בניקוד 0.

3) הניקוד בטווח שבין 50% ל-75%, יחושב באופן יחסי.

ג. <u>להלן טבלה המרכזת את מדדי איכות שירות הלקוחות</u>:

הפרמטר	מפורט בסעיף	ניקוד	משקל
זמני מענה בשיחות טלפוניות	6.3.5.1	80% מהשיחות נענו תוך דקה = ניקוד 100, 50% ומטה מהשיחות נענו תוך דקה = ניקוד 0	16.66%
זמני מענה לפנייה באמצעות יישומון **WhatsApp**	6.3.5.2.1	80% מענה אנושי לפניות תוך 4 דקות= ניקוד 100, 50% ומטה = ניקוד 0	16.66%
זמני מענה באמצעות דוא"ל ופורטל האינטרנט	6.3.5.2.2	90% מענה אנושי ראשוני עד לסיום יום עסקים הבא = ניקוד 100, מתחת ל- 50% ניקוד 0	16.66%
שביעות רצון מהמענה והטיפול במוקד	6.3.5.5.1	90% ומעלה לפי ציונים גבוהים בסקלה 5-1 = ניקוד 100, 60% ומטה = ניקוד 0	16.66%
שביעות רצון מהשירותים שניתנים ללקוחות על ידי מערכת הסליקה	6.3.5.5.2	80% ומעלה לפי ציונים גבוהים בסקלה 5-1 = ניקוד 100, 60% ומטה = ניקוד 0	16.66%
מדד **FCR** של המוקד	ג'	75% ומעלה ע"פ תיעוד השיחות = ניקוד 100, 50% ומטה =ניקוד 0	16.66%
סה"כ			**100%**

6.3.5.6 הציון הכולל במדד זה הוא שיקלול של הניקוד בכל שורה, במשקל היחסי של השורה

6.3.5.7 הרשות תוכל לעדכן את המשקלים המדדים והיעדים לעיל מדי רבעון.

6.3.6 <u>התאוששות מאסון</u>

6.3.6.1 יעד התאוששות מאסון מבטא התאוששות מלאה של מערכת הסליקה, למצב שהיה לפני האסון.

6.3.6.2 מוכנות להתאוששות מאסון תיבדק אחת לשנה בתרגיל התאוששות מאסון, במהלכו תופסק פעילות מערכת הסליקה באתר הראשי ויופעל פתרון הגיבוי באתר הגיבוי החלופי. טרם התרגיל יעדכן הספק את הרשות אודות מועד קיומו של התרגיל ואודות תוכנו וממצאיו בסיומו.

6.3.6.3 הציון יהיה 100 אם זמן ההתאוששות בתרגיל יהיה קטן או שווה ל-5 שעות.

6.3.6.4 הציון יהיה 0 אם זמן ההתאוששות יהיה גדול מ-24 שעות.

6.3.6.5 הציון עבור זמן התאוששות שהוא בטווח הזמן שבין 5 שעות ל-24 שעות יחושב באופן יחסי. כך למשל, זמן התאוששות של 10 שעות מזכה בציון 73.68.

6.3.6.6 ככל ויקבל הספק ציון של 60 ומטה, יידרש הספק לתקן ולשפר כשירות ולבצע תרגיל התאוששות חוזר, תוך פרק זמן שיוגדר על ידי הממונה.

6.3.7 <u>שקלול מדדים לצורך קביעת פיצוי מוסכם:</u>

לצורך קביעת פיצוי מוסכם, ככל ויידרש, יילקחו בחשבון המדדים הבאים על פי המשקולות להלן:

המדד	משקל
זמינות מערכת הסליקה	20%
זמני טיפול בתקלות	20%
זמני ביצוע של הוראות הממונה	25%
זמני ביצוע טכני של פעולות במערכת	10%
מערך השירות והתמיכה	25%
סה"כ	**100%**

6.4 עקרונות לעניין הפיצוי המוסכם

6.4.1 לממונה שיקול דעת בכל הקשור להטלת פיצוי כספי ולהיקפו. בכל מקרה שבו יוטל על הספק לשלם פיצוי מוסכם, יערוך מנהל הפרויקט מטעם הממונה הודעת חיוב מתאימה, בה יצוינו פרטי הפיצוי המוסכם והסיבות להטלתו לרבות פרטי העברת התשלום. הספק רשאי לערער בפני הממונה על קבלת דרישת התשלום, ובמסגרת זו יוצגו על ידי הספק הנסיבות השונות הנלוות לסטייה במדדי השירות בפני נציגי הממונה. החלטת הממונה לעניין גובה הפיצוי לאחר הערעור תהיה סופית בעניין. יובהר כי הפיצוי המוסכם אינו גורע מסמכות הממונה לפעול בהליכי אכיפה ועיצומים נוספים בכפוף לחוק.

6.4.2 סכום הפיצוי המוסכם המרבי, אותו יוכל להטיל הממונה על הספק יעמוד על 10 מיליון ₪ לשנה; ככל שגובה הפיצוי המוסכם יעלה על היקף זה, יהיה הממונה רשאי להודיע לספק על הפסקת ההתקשרות עמו תוך 30 ימים, בכפוף לשימוע.

6.4.3 פיצויים מוסכמים שיוטלו על הספק לפי תנאי מכרז זה או הוראות החוק ישולמו על ידי הספק עצמו ולא יגבו מדמי השימוש העתידיים מהלקוחות או המשתמשים.

6.4.4 סכומי הפיצויים יוצמדו למדד, כאשר שער הבסיס ייקבע לפי השער ביום חתימת הצדדים על הסכם ההתקשרות ומועד ההצמדה יהיה נכון למועד הודעת הממונה לספק על פיצוי מוסכם שהוא סופי ולא ניתן לערעור.

6.4.5 יובהר כי אין בהטלת פיצוי כספי כדי לגרוע מאחריות נזיקית שעשויה להיות מוטלת על מערכת הסליקה לפצות בגין נזקים שנגרמו ללקוח או למשתמש או לממונה כתוצאה מהשירות שניתן על ידי מערכת הסליקה.

6.4.6 <u>שימוש בכספי הפיצויים</u>

6.4.6.1 הספק ימנה נאמן על חשבונו, באישור הממונה, לניהול כספי הפיצויים אשר יועברו לקרן שתנוהל בנאמנות. מינוי נאמן לכספי הפיצויים, ככל שיגבו, יעשה לראשונה תוך חודש ימים מיום קביעת גובה הפיצוי על ידי הממונה והעברת הודעת החיוב.

6.4.6.2 סך התשלומים שייגבו מהספק כפיצוי בהתאם לתנאי מכרז זה, יועברו לקרן שתנוהל על ידי הנאמן, למעט במקרה שבו צוין במפורש שהפיצוי יועבר לידי גורם אחר.

6.4.6.3 הנאמן יעביר למנהל הפרויקט מטעם הממונה דיווח אחת לרבעון על סך הכספים שנצברו בקרן, ועל פירוט סכומי הקנסות המרכיבים את היתרה ותאריכי תשלום הקנסות.

6.4.6.4 הממונה רשאי להחליט על שימוש בכספי הקרן כאמור לטובת ביצוע שדרוגים ותוספות למערכת הסליקה שאינם כלולים במסגרת תנאי מכרז זה או לטובת מתן הנחות למשתמשים.

6.5 חישוב הפיצוי המוסכם

6.5.1 הפיצוי המוסכם יחושב באופן רבעוני, כך שבכל סוף רבעון ינגיש הספק לממונה בפורטל הייעודי את סיכום שקלול המדדים העדכני שחושב על ידו. במסגרת זאת יעביר הספק, בהתאם לדרישת הרשות, כל מידע, נתונים, דוחות וכו', המתייחסים למדדים. למען הסר ספק, בהינתן וקיימת מחלוקת לעניין אופן הניקוד ה ההחלטה בנוגע לציון תיקבע על ידי הרשות בלבד.

6.5.2 דרך חישוב הפיצוי המוסכם: כל חריגה בנקודה (1%) מציון 100% בשקלול המדדים כמפורט בטבלה בסעיף 3.7 לעיל, תחייב את הספק בפיצוי מוסכם בגובה של 150,000 ₪ צמוד למדד המחירים לצרכן ובתוספת מע"מ כחוק.

6.5.3 כך למשל, <u>לצורך דוגמה בלבד</u>:

המדד	ציון	משקל	ציון משוקלל
זמינות המערכת	100	20%	20
זמן טיפול בתקלות	100	20%	20
זמני ביצוע- ע"פ הוראות הממונה	100	25%	25
זמני ביצוע- ע"פ מפרט טכני	95	10%	9.5
מערך השירות והתמיכה	100	25%	25
סה"כ		**100%**	**99.5**

במקרה זה, הציון הסופי יהיה 99.5, הפיצוי המוסכם ייקבע על סך של 75,000 ₪ בתוספת מע"מ כחוק.

פרק 7 – מודל התמחור

7.1 רקע

פרק זה מתאר את התמורה הכוללת לה זכאי הספק הזוכה במסגרת מתן השירותים על פי מכרז זה. התמורה היא בגין כלל הדרישות המפורטות במכרז, לרבות תפעול, תחזוקה ופיתוח של מערכת הסליקה, תמיכה בדרישות הטכנולוגיות, דרישות אבטחת המידע, דרישות חוזיות ועוד. הספק הזוכה יהיה זכאי לקבלת תמורה זו וזו בלבד, והכל בהתאם למפורט בפרק זה.

7.2 הצעת מחיר של הספק

7.2.1 בהתאם לסעיף 1.7.4 לעיל, במסגרת הצעת המחיר שאותה יגיש המציע במכרז זה, נדרש המציע להציע אחוז הנחה רוחבי שמתייחס למחירון אשר נקבע על ידי הממונה ומצ"ב למכרז זה כנספח ב.3 – מחירון השירותים (להלן – **המחירון שבנספח**). המחירון שבנספח מתייחס לתעריפי המקסימום לפעולות מערכת הסליקה, כאשר לתעריפים אלה יש להוסיף מע"מ כחוק.

7.2.2 הצעת המחיר תחייב את המציע לאורך כל תקופת ההתקשרות ותקופות האופציה, בכפוף למנגנון עדכון המחירים המפורט בסעיף 7.3.8.16 להלן.

7.3 התמורה לספק – כללי

7.3.1 מחירון השירותים עבור כל שירות שעל בסיסו תקבע התמורה שלה זכאי הספק הזוכה במסגרת מתן השירותים על פי מכרז זה, נקבע על ידי הממונה ומפורט בחוזר תשלומים, כפי שיעודכן מעת לעת.

7.3.2 במקביל לפרסום מכרז זה, הממונה יפרסם עדכון לחוזר תשלומים - שיפרט את התמורה בהתאם למודל התשלום העדכני שיקבע בהתאם למציע הזוכה.

7.3.3 התמורה מורכבת מהכנסה מדמי שימוש קבועים המשולמים על ידי הגופים המוסדיים, וכן מדמי שימוש עבור פעולות המשולמים על ידי לקוחות ומשתמשי המערכת. יובהר כי תעריף בגין בקשת מידע או ביצוע פעולה כולל את עלות העברת המענה למבקש המידע.

7.3.4 הזכאות לתמורה תחל מסיום מועד השלמת תקופת החפיפה (החל משלב ב' בתכנית העבודה), ולאחר אישור הממונה לעניין קבלת אחריות מלאה של הספק הזוכה על המערכת. ככל שמועד קבלת האחריות המלאה של הספק הזוכה על המערכת תהיה מוקדמת יותר כך הזכאות לתמורה תהיה מוקדמת יותר.

7.3.5 התמורה המפורטת בפרק זה תהיה התמורה הבלעדית שלה יהיה זכאי הספק בגין השירותים לפי מכרז זה, וקבלתה מותנת בעמידת הספק בהתחייבויותיו לפי מכרז זה, לרבות הסכם ההתקשרות.

7.3.6 ככל שבתקופת ההתקשרות יתווסף שירות נוסף, אם ביוזמת הספק באישור הממונה או על פי דרישת הממונה, יכולה שתקבע תמורה נוספת בגין השירות הנוסף באישור הממונה.

7.3.7 <u>דמי שימוש קבועים - גופים מוסדיים</u>

7.3.7.1 דמי שימוש קבועים בסך של כ-7.5 מיליון ₪ לשנה סה"כ, בתוספת מע"מ כחוק, ישולמו בכל שנה למערכת הסליקה על ידי כלל הגופים המוסדיים באופן יחסי, בהתאם לחלוקה שתיקבע על ידי הממונה במסגרת חוזר תשלומים, ויעודכנו אחת לשנה בהתאם לשינוי שיעור מדד המחירים לצרכן, כאשר מדד הבסיס הינו חודש ינואר 2027 והמדד המעודכן הינו המדד הידוע של חודש מרץ באותה שנה.

7.3.7.2 דמי השימוש הקבועים ישולמו על ידי הגופים המוסדיים, אחת לשנה. התשלום יועבר במהלך חודש מאי בגין אותה שנה קלנדרית. במידה והספק הזוכה יחל את פעילותו באמצע רבעון, דמי השימוש הקבועים ישולמו על ידי הגופים ביום העסקים הראשון בשבוע השני שלאחר תחילת פעילותו. תשלום כאמור יהיה באופן יחסי למועד תחילת הפעילות לגבי אותו רבעון.

7.3.7.3 בנוסף לדמי השימוש הקבועים, גוף מוסדי ישלם <u>גם דמי שימוש עבור פעולות (השירותים בהם יעשה שימוש)</u>, כמפורט בסעיף 7.3.8 להלן.

7.3.8 <u>דמי שימוש עבור פעולות ובקשות מידע – לקוחות ומשתמשי המערכת</u>

7.3.8.1 כלל לקוחות מערכת הסליקה ומשתמשיה ישלמו דמי שימוש בעד ביצוע פעולות או בקשות מידע באמצעות המערכת, למעט העברת מידע בין גופים מוסדיים אגב ניוד כספים.

7.3.8.2 מחירון הפעולות הסופי ייקבע על ידי הממונה בהתאם להצעת הספק הזוכה (המגלמת את אחוז ההנחה הרוחבי למחירון שבנספח) (להלן – **המחירון הסופי**).

7.3.8.3 המחירון הסופי יחייב את הספק הזוכה ואת כלל לקוחות המערכת ומשתמשיה.

7.3.8.4 על אף האמור לעיל, במהלך ההתקשרות על פי המכרז, הספק יהיה רשאי להציע שינוי למחירים שבמחירון הסופי או להציע תעריף לשירות או פעולה חדשה שהתווספו במהלך תקופת ההתקשרות. לממונה הסמכות לקבוע אם לאמץ את השינוי המוצע, כולו או חלקו, או אם לקבוע מחיר אחר לפעולות שלא נכללו במחירון הסופי, והחלטתו בעניין זה תחייב את הספק.

7.3.8.5 תשלום דמי שימוש על ידי הלקוחות והמשתמשים השונים, יתבסס על מחיר פעולה לפי המחירון הסופי אשר יוכפל במספרי הפעולות שיבוצע בכל סוג פעולה על ידי כל לקוח ומשתמש במערכת.

7.3.8.6 יובהר, כי דמי שימוש עבור פעולה שהיא הפקדת כספים או העברה של מידע שנלווה להפקדת כספים לגוף מוסדי מסוים, המתייחסת לכמה מהרכיבים של המוצר הפנסיוני (כגון הפקדה לרכיב חיסכון ולרכיב ביטוח ריסק), תיחשב פעולה בודדת לצורך חישוב דמי השימוש.

7.3.8.7 תשלום דמי השימוש עבור פעולה יהיה בלתי תלוי בערוץ אשר שימש למתן ההוראה לביצוע הפעולה (כך למשל מחיר הפעולה יהיה קבוע בין אם הפעולה בוצעה באמצעות פורטל האינטרנט ובין אם בהוראה הועברה בממשק באמצעות כספות או API).

7.3.8.8 תשלום דמי השימוש עבור פעולה שיזם לקוח או משתמש שאינו גוף מוסדי, ואשר לא הושלמה בשל תקלה שנגרמה באשמת הלקוח או המשתמש, יחול במלואו על הלקוח או המשתמש לפי העניין. במקרה כזה, הספק יציע למשתמש כאמור לבצע פעולה חוזרת במחיר מופחת בשיעור של 50% ממחיר הפעולה בהתאם למחירון הסופי.

7.3.8.9 הספק הזוכה לא יחייב תשלום דמי שימוש עבור פעולה שיזם לקוח או משתמש שאינו גוף מוסדי, ואשר לא הושלמה בשל תקלה שנגרמה באשמת הספק.

7.3.8.10 הספק רשאי לקבוע הנחות למחירי הפעולות המנויות במחירון הסופי ובלבד שהסיבה בגינה ניתנה ההנחה לא תפלה בתנאיה לקוח או משתמש אחר במערכת, וכן קיבל לכך אישור מראש מהממונה. הממונה רשאי לאשר הנחות שאינן עומדות בתנאי זה, על פי שיקול דעתו.

7.3.8.11 המחירון הסופי יופיע כנספח בחוזר תשלומים, ויפורסם על ידי הספק הזוכה בפורטל האינטרנט בתוספת מע"מ כחוק.

7.3.8.12 המחירון הסופי יעודכן אחת לשנה לגבי השירותים הקיימים, ביום העסקים הראשון לחודש אפריל של אותה השנה ; העדכון הראשון יהיה לאחר השלמת שנה קלנדרית מלאה (ינואר עד דצמבר), ממועד השלמת תקופת החפיפה (החל משלב ב' בתכנית העבודה), ולאחר אישור הממונה לעניין קבלת אחריות מלאה של הספק הזוכה על המערכת. (לשם הבהרה : במידה ותקופת החפיפה הסתיימה ב 2/26 אזי העדכון הראשון יהיה ב 1/4/28). <u>לשם הבהרה :</u> מחירון שנת 2028 יהיה בתוקף מה 1/4/28 ועד 31/3/29, מחירון שנת 2029 יהיה בתוקף מה 1/4/29 ועד 31/3/30 וכו'.

7.3.8.13 הרשות תאשר את עדכון המחירון לפני כניסתו לתוקף ופרסומו בפורטל האינטרנט לכלל לקוחות ומשתמשי המערכת.

7.3.8.14 בחישוב תעריפי הפעולות המופיעים במחירון לאחר הפעלת מנגנון העדכון, יעוגל מחיר כל פעולה עד לאגורה הבודדת הקרובה בהתאם לכללי העיגול המקובלים.

7.3.8.15 <u>עדכון המחירון הסופי יתבסס על הנתונים הבאים:</u>

7.3.8.15.1 **שיעור השינוי במדד המחירים לצרכן** – בדיקה תתבצע אחת לשנה, כאשר מדד הבסיס יהיה שער המדד בחודש ינואר 2027 (אשר יפורסם באמצע פברואר 2027) ו**עליה בהיקף הפעילות של מערכת הסליקה** – בדיקה תתבצע אחת לשנה, כמפורט להלן.

7.3.8.15.2 יובהר כי הממונה יהיה רשאי שלא להפעיל את מנגנון עדכון המחירים בגין עליה בהיקף פעילות של מערכת הסליקה לפי שיקול דעתו.

7.3.8.15.3 בכל מקום שבו ישנה סתירה בין הנוסחה המספרית לבין ההסבר בכתב שלצידה, תגבר הנוסחה.

7.3.8.16 <u>הנוסחה לעדכון המחירים</u>

$$P\_i\_t = P\_i\_base * (C_t * Z_t)$$

i = השירות הספציפי

P_i = המחיר (בש״ח לפעולה) לשירות **i**, לא כולל מע״מ.

P_ i _base = מחיר השירות (בש״ח לפעולה) בתחילת מתן השירותים ע״י הספק, לא כולל מע״מ.

t = שנה מסוימת

P_i_t = המחיר המקסימלי לשירות **i** לאחר עדכון המחירים בשנה **t**, לא כולל מע״מ.

CPI_base = מדד המחירים לצרכן של ינואר 2027 אשר יפורסם באמנצע חודש פברואר 2027.

CPI_t = מדד המחירים לצרכן הידוע בחודש מרץ בשנה **t**.

C_t = מקדם עדכון בגין שינוי במדד המחירים לצרכן, כמפורט בסעיף 7.3.8.17 להלן.

Z_t = מקדם לעדכון היקף הפעילות, כמפורט בסעיף 7.3.8.18 להלן

7.3.8.17 <u>אופן חישוב מקדם עדכון בגין מדד:</u>

C_t = CPI_t/CPI_base

7.3.8.18 <u>אופן חישוב מקדם עדכון היקף פעילות</u> :

7.3.8.18.1 **MRbase** = סך ההכנסות הנגזרות מהיקף הפעילות בשירותים עליהם חלה חובת שימוש במערכת הסליקה בשנה הקלנדרית <u>המלאה</u> הראשונה לפעילות הספק הזוכה (לפי המחירון הסופי) כלומר סך הכנסות יחושבו החל מ-1 בינואר הראשון לפעילות המערכת תחת הספק הזוכה ועד 31 בדצמבר. ההכנסות יחושבו כסכום של המחירון של כל פעולה כפול מספר פעולות מסוג זה בשנה החולפת.

7.3.8.18.2 **MRt** = סך ההכנסות הנגזרות מהיקף הפעילות בשירותים עליהם חלה חובת שימוש במערכת הסליקה בשנה **t**. סך הכנסות יחושבו עבור חודשים ינואר עד דצמבר באותה השנה. התחשיב יבוצע לפי [מחירון הפעולה כפול מספר הפעולות שבוצעו] בכל פעולה שבחובת שימוש.

7.3.8.18.3 **Dt** = שינוי בהכנסות מערכת הסליקה לעומת ה – **Rbase**

$$\mathbf{Dt} = \boldsymbol{M}\mathbf{Rt}/\mathbf{MRbase}$$

7.3.8.18.4 **Z** = מקדם היקף הפעילות

$$\mathbf{Z\_t} = \mathbf{0.4} + (\mathbf{0.6}/\mathbf{Dt})$$

7.3.8.18.5 במידה והמכפלה $(\boldsymbol{C_t} * \boldsymbol{Z_t})$ לחלק למכפלה בשנה האחרונה בה בוצע עדכון במחירון - $(\boldsymbol{C_{t\_update}} * \boldsymbol{Z_{t\_update}})$ גדולה מ- 0.98 וקטנה מ 1.02 אזי לא יבוצע עדכון למחירים בשנה זו.

7.3.8.18.6 כאשר **t_update** = מועד העדכון הקודם של מחירון השירותים.

7.3.8.18.7 מחירון השירותים המעודכן ייכנס לתוקף מתאריך 1.4 ועד לעדכון המחירים הבא.

7.4 התמורה בעת סיום ההתקשרות

ככל שהוחלט על סיום ההתקשרות בטרם סיום תקופת ההתקשרות או בטרם סיום תקופות האופציה, לא ישולמו לספק תשלומים נוספים בגין תקופה שלאחר סיום ההתקשרות או האופציה כאמור. כך, למשל, אם תופסק ההתקשרות לאחר 35 ימים מתחילת הרבעון, כאשר ברבעון זה ישנם 90 ימים, ישלמו הגופים המוסדיים את חלקם היחסי בתשלום הקבוע עבור 35 ימים.

רשימת נספחים לחלק ב'

מס' נספח	שם נספח
נספח ב.1	סליקה ישירה של כספים
נספח ב.2	נוהל היפרדות מהספק הזוכה
נספח ב.3	מחירון השירותים
נספח ב.4	מצב קיים – מערכת הסליקה

נספח ב.1 – סליקה ישירה של כספים

1. <u>דרישות כלליות מרכזיות שצריכות להילקח בחשבון לצורך מתן שירות של סליקה ישירה על ידי חיבור למערכת זהב:</u>

1.1 מתן שירות של סליקה ישירה מחייב הצטרפות של מערכת הסליקה למערכת התשלומים זה"ב (זיכויים והעברות בזמן אמת) ופתיחה של חשבון בבנק ישראל.

1.2 בין משתתפי מערכת זה"ב נמנים כלל התאגידים הבנקאיים, מסלקות ייעודיות וגופים חוץ בנקאיים אשר קיבלו אישור התחברות למערכת. כללי מערכת זה"ב מסדירים את מערכת הקשרים, לרבות הקשר העסקי והפונקציונאלי, בין המשתתפים במערכת זה"ב לבין מערכת זה"ב, בין משתתפים אלה לבין בנק ישראל כמפעיל מערכת זה"ב וכן בין משתתפים אלה לבין עצמם. בכפוף לאישור בנק ישראל להשתתפות מערכת הסליקה במערכת זה"ב, הספק יחתום עם בנק ישראל על הסכם להשתתפות במערכת זה"ב.

1.3 התחברות למערכת זה"ב ופתיחת חשבון בבנק ישראל, כאמור, מחייבים קבלת אישור מבנק ישראל בהתאם לכללים שמפורסמים על ידו בנושא, המחייבים, בין השאר, עמידה בדרישות המרכזיות הבאות:

1.3.1 יכולות טכנולוגיות נדרשות המאפשרות לעמוד בכללי מערכת זה"ב;

1.3.2 עמידה בתנאי ההמשכיות העסקית המוצגים בכללי מערכת זה"ב, כולל הסדרי גיבוי מספיקים (Adequate Contingency Arrangements);

1.3.3 עמידה בדרישות הקשורות לממשק SWIFT-, המוצגות בכללי מערכת זה"ב;

1.3.4 עמידה בדרישות האבטחה, המוצגות בכללי מערכת זה"ב;

1.3.5 עמידה בכל דרישה נוספת המופיעה בכללי מערכת זה"ב;

1.4 העברת הוראות תשלום בין מערכת זה"ב למערכת הסליקה תעשה בכפוף למבנה המסר ולרשימת מסרי התשלום המאושרים, אשר כוללים לפחות את כל הפרטים המנדטוריים, כגון מספר IBAN עבור הוראות מסוימות, ועשויים לכלול גם פרטים אופציונליים - בהתאם לסוג הוראת התשלום ובהתאם למפרט הקבוע בכללי מערכת זה"ב ולהוראות אחרות בכללים אלה, והכל בהתאם לכללי מערכת זה"ב כפי שיעודכנו מעת לעת.

1.5 סליקת כספים במערכת זה"ב תבוצע בין חשבונות של נותני שירותי תשלום המשתתפים במערכת זה"ב, כאשר מידע נלווה לשם עדכון רישום תנועות זכות וחובה של משתמשי מערכת הסליקה המעורבים בפעולת סליקת הכספים, בחשבונות התשלום שלהם המנוהלים באותם נותני שירותי תשלום (נכון למועד זה בתאגידים הבנקאיים) המשתתפים במערכת זה"ב, יועבר במסגרת קבצי הסליקה בצמידות לסליקת הכספים באמצעות מערכת זה"ב.

1.6 הספק יידרש לערוך נוהל סליקה ישירה של כספים אשר יגדיר את תהליכי הסליקה מול מערכת זה"ב, מול נותני שירותי התשלום המשתתפים במערכת זה"ב ובכלל זה התאגידים הבנקאיים, ומול משתמשי מערכת הסליקה, לרבות גופים מוסדיים, ובתיאום עמם. הנוהל יידרש להתייחס, בין השאר, למקרה של כשל בהשלמת פעולת הסליקה,

פעולות מערכת הסליקה במקרה של כשל כזה והמנגנונים למזעור האפשרות לכשל. הנוהל יועבר לאישור הממונה בטרם הפעלת שירות סליקה ישירה.

2. <u>דרישות אבטחת מידע מרכזיות שצריכות להילקח בחשבון לצורך מתן שירות של סליקה ישירה על ידי חיבור למערכת זהב:</u>

2.1 **הצפנה ותשתית מאובטחת:**

- יש ליישם הצפנת נתונים מתקדמת (AES-256 לפחות) לכל התקשורת עם מערכת זה"ב, הן בתעבורה והן במצב אחסון
- שימוש בתשתית PKI לניהול מפתחות ואימות זהויות במערכת

2.2 **זיהוי ואימות משתמשים:**

- אימות דו-שלבי (MFA) למשתמשים המתחברים למערכת
- שימוש בתעודות דיגיטליות לאימות והזדהות חזקה

2.3 **ניהול גישה ומגבלות:**

- הגדרה מדוקדקת של הרשאות גישה למשתמשים בהתבסס על עקרונות Least Privilege
- מעקב אחר גישת משתמשים וביקורות שוטפות לוודא עמידה במדיניות הארגון

2.4 **בקרת גישה לרשת ולמערכות:**

- הפרדה מוחלטת בין סביבות עבודה פנימיות לסביבות המחוברות למערכת זה"ב
- שימוש בחומות אש, מערכות מניעת חדירה (IPS), וניהול רשת סגורה לגישה למערכת

2.5 **ניטור ובקרת פעילויות:**

- התקנה והפעלה של SIEM לניטור תעבורת הרשת ולזיהוי חריגות
- שמירת לוגים של כל הפעולות המבוצעות במערכת לתקופה של לפחות 5 שנים

2.6 **תוכניות המשכיות עסקית והתאוששות מאסון:**

- פיתוח תוכנית להתאוששות מלאה של המערכת בזמן חירום תוך עמידה בדרישות RTO ו-RPO של בנק ישראל
- שמירה על סביבות גיבוי זמינות ומעודכנות

2.7 **דרישות חיבור ל-SWIFT CUG ISRAEL**

- יישום תוכנית האבטחה של (SWIFT CSP)
- יישום בקרות חובה (Mandatory Security Controls) בהתאם ל-CSP, הכוללות:
  - שמירה על סביבה סגורה (Secure Zone)

- ניהול זהויות והרשאות משתמשים
- ניטור פעילויות חריגות וזיהוי איומים
- הגשת דוחות תאימות שנתיים ל-SWIFT באמצעות KYC-SA (Know Your Customer Security Attestation)

2.8 **בקרות תעבורה לרשת SWIFT:**

- שימוש בפתרונות Network Security להגבלת גישה לרשת SWIFT
- הצפנת תעבורת נתונים בין מסופי SWIFT לבין מערכת זה"ב

2.9 **הקשחת תשתיות ותהליכי עדכון:**

- התקנת עדכוני תוכנה ואבטחה למערכות המחוברות ל-SWIFT
- בדיקות פגיעות תקופתיות לסביבות SWIFT ו-Secure Zone

2.10 **ניהול מפתחות קריפטוגרפיים:**

- שימוש במכשירי HSM (Hardware Security Module) לניהול מפתחות ולביצוע הצפנות
- שמירה על מפתחות הצפנה באחסון מאובטח, תוך עמידה בתקנים כמו FIPS 140-2

2.11 **הגנת תחנות עבודה ומסופים:**

- יישום פתרונות אנטי-וירוס מתקדמים והקשחת תחנות עבודה
- ניטור שוטף של פעילות מסופים לזיהוי והתמודדות עם מתקפות מתקדמות (APT)

2.12 **תיעוד, תאימות ובדיקות אבטחה**

- על הספק לספק תיעוד מלא של תהליכי האבטחה הקשורים למערכות זה"ב ו-SWIFT, כולל דוחות תקופתיים על עמידה בדרישות האבטחה
- ביצוע בדיקות חדירה (Penetration Testing) לפחות פעם בשנה למערכות המחוברות
- שהספק יחויב בדיווח מידי על אירוע אבטחת מידע, פגיעה בפרטיות או כשל טכנולוגי לרשות, הרשות רשאית להורות לספק לדווח על האירוע לגורמים נוספים, בהתאם לנסיבות ולשיקול דעתה. במידה ויתרחשו אירועי אבטחה משמעותיים על הספק לדווח בצורה מיידית למנהלי המערכת ולרגולטור, תוך פרסום דוח סיכום ותוכנית תיקון.

נספח ב.2 – נוהל היפרדות מהספק הזוכה

1. עד לסיום תקופת ההתקשרות בפועל, לרבות בתקופת החפיפה מול הספק המחליף (כהגדרתו בסעיף 5.11.1 בפרק 5 - המימוש לעיל), הספק הזוכה יהיה הבעלים של מערכת הסליקה. הספק הזוכה יעביר לספק המחליף את הבעלות על המערכת במסגרת יישום נוהל היפרדות (נספח ב.2) ללא כל תמורה, מלבד הציוד הפיזי אשר יירכש או יושכר, כפי שיפורט להלן.

2. עם מתן ההודעה על סיום ההתקשרות מנציגי הרשות, הספק הזוכה מתחייב לבצע כל פעולה שתידרש לשם העברת הבעלות על המערכת ומתחייב לסייע ולשתף פעולה עם הספק המחליף ככל שיידרש.

3. בגין איחור במועד זה ללא אישור מראש של הרשות, מכל סיבה שהיא, הספק הזוכה ישלם לרשות קנס פיגורים בסך של ממוצע היקף המחזור הכספי השנתי של הספק בשלוש השנים שקדמו להודעה, חלקי 365 ובמכפלת ימי האיחור. יובהר כי סעיף זה הינו סעיף יסודי לזכיית המציע במכרז וכי מציע, עם הגשת הצעתו, מוותר על כל טענה ו/או דרישה בנושא.

4. אישור על השלמת נוהל ההיפרדות וההחלטה על מוכנות הספק המחליף לקבלת האחריות על הפעלת המערכת תהיה נתונה לממונה בלבד ולפי שיקול דעתו הבלעדי.

5. במהלך תקופת ההיערכות להיפרדות הספק הזוכה ישתף פעולה ויבצע חפיפה לצוות הספק המחליף ולאנשי הממונה על מערכת הסליקה, על כלל מרכיביה.

6. נוהל ההיפרדות יעודכן אחת לשנה על ידי הספק הזוכה, ויוגש לאישור הרשות. הרשות רשאית לדרוש לעדכן את נוהל ההיפרדות בכל עת, בהתאם לצרכים המשתנים של מערכת הסליקה והספק הזוכה יבצע העדכון בהתאם להנחיות שיינתנו.

7. נוהל ההיפרדות מפרט את המשימות ואבני הדרך, לוחות הזמנים, מבנה צוותי העבודה והאחריות לשתי תקופות: תקופת ההיערכות להיפרדות ותקופת התמיכה לאחר השלמת ההיפרדות כהגדרתן בנוהל.

8. תקופת ההיערכות

תקופה שלא תעלה על 180 ימים, מיום מתן הודעה על סיום ההתקשרות ועד לסיום ההתקשרות בפועל והשלמת המשימות בנוהל ההיפרדות. על אף האמור, למזמין שמורה הזכות להאריך את תקופת ההיערכות בפרק זמן נוסף, על פי שיקול דעתו.

8.1. הספק הזוכה יהיה מחויב להמשך פעילות רציפה של מערכת הסליקה והשירותים ללקוחות והמשתמשים, וזאת עד למועד העברת האחריות והבעלות על המערכת לספק המחליף.

8.2. הספק הזוכה ימשיך לעמוד ברמת השירות המוגדרת במכרז זה.

8.3. הספק הזוכה יוודא כי הספק המחליף קיבל את כל הכלים הנדרשים לשם הפעלת המערכת וידאג כי העברת השירותים תיעשה בצורה מסודרת, יעילה ומלאה.

9. <u>תיאור כולל של פעילות ורכיבי המערכת</u>

9.1. הספק הזוכה יגיש לממונה, עד 14 ימים מיום ההודעה על סיום ההתקשרות, מסמך מפורט הכולל את כל המידע אודות פעילות מערכת הסליקה. הממונה רשאי לדרוש מהספק להשלים מידע נוסף, על פי שיקול דעתו ולהעביר את המסמך למי מטעמו.

9.2. המסמך כאמור יכלול את כלל המידע אודות מערכת הסליקה, לרבות:

- **רכיבי המערכת** – לרבות רכיבי תוכנה, חומרה, תשתיות, גיבוי, קוד מקור, סיסמאות, רשימת רישיונות, רשימת ספקי המשנה, פרטים אודות מוקד התמיכה, פרטים אודות הפעלת פורטל האינטרנט, כללי ונהלי המערכת וכל מידע נוסף הנחוץ לשם הפעלת המערכת.
- **תיק מערכת** – הכולל נהלי עבודה, העברות לייצור, שגרות תחזוקה, תרגול המשכיות עסקית, וכן התיעוד ששמר הספק בגינם.
- **ארכיטקטורת הרשת** – תיק מערכת המפרט את ארכיטקטורת הרשת, טופולוגיה של שרתים, אחסון, בסיסי נתונים. הכולל אתר ראשי ואתר התאוששות מאסון.
- **ארכיטקטורה לוגית** – תיק מערכת המפרט אפיון תהליכים, תרשים ישויות מרכזיות, פונקציות ולוגיקות מרכזיות, דוחות.
- **ממשקים** – תרשים אינטגרציה שמפרט הכלים והממשקים, הקשר בין הפתרון לבין צדדי ג', מערכות משיקות, מקורות מידע וכו'
- **סקרי אבטחת מידע** – לרבות דוחות חוסן, תמונת מצב של כלל הליקויים, פערים שנותרו פתוחים ותיעוד נדרש.
- **Road Map** – מפת דרכים למוצר, גרסאות עתידיות, רשימת **backlog** של דרישות לשיפור ושינויים.
- **תקלות הידועות לספק** – רשימת באגים ותקלות פתוחות לפי סיווג וחומרה.
- **הודעות** – רשימה של הודעות/מסרים/קבצים, תדירות העברה, נפח הודעה, טכניקת העברה (אצווה/זמן אמת), צד שולח, צד מקבל, טריגר או תזמון.
- **מפרט ציוד** – מפרט של ציוד קצה, מחשבים אישיים, מסכים, מדפסות, ציוד אבטחה, תוכנות למחשבים אישיים, תוכנות משרד.
- **סקרים של ספקים מהותיים** – ביקורות דוחות וסקרים שנעשו על צדדי ג' וספקים מהותיים.
- **יועצים** – התקשרויות עקיפות הנדרשות לתפעול השוטף, שירותי כ"א, משרדי ייעוץ, משפטי, רו"ח, בינוי, טכנולוגיה וכו'.

- **רשימת מצבת עובדים של הספק ה**זוכה – ללא צורך בציון פרטיהם המזהים, אלא על פי מקצועות, תוך ציון תפקידם במערכת, שעות העבודה, כוננויות וכל מידע רלוונטי נוסף. יש לבצע הפרדה בין מערכי הפיתוח, תשתיות, תפעול וגורמי **Back Office**.

10. <u>הקמת צוותי העברה</u>

10.1. בתוך שבועיים ממועד מסירת הודעה על סיום ההתקשרות, יקים הספק הזוכה צוות העברה אשר יעבוד מול נציגי הספק הקיים ו/או נציגי המזמין ככל שיבחר למנות נציגים לשם כך. עיסוקם הבלעדי של נציגי הספק בצוות ההעברה לאורך תקופת ההיערכות יהיה ביישום נוהל ההיפרדות. הספק הזוכה והספק הקיים ימנו נציגים לצוותים מקצועיים שונים, אשר יבצעו את החפיפה על פי לוז, הכולל אבני דרך, שייקבע על ידי צוות ההעברה המנהל, ויפעלו במקביל זה לזה. נושאי פעילות הצוותים יהיו, בין היתר:

- צוות ניהולי

<u>אחריות</u>: צוות הניהול יהיה אחראי על תכנון מפורט של תהליך ההיפרדות, ניהול תהליך ההיפרדות, תיאום פעולות צוותי ההיפרדות השונים, מעקב אחר לוחות הזמנים והתקדמות הביצוע. נציגי הספק המחליף ישתתפו בישיבות מנהלת הפרויקט.

<u>חברי הצוות</u>: צוות זה יכלול את נציגי הרשות, מנהל תהליך ההיפרדות מטעם הספק הזוכה ונציג ניהולי מטעם הספק הקיים. מנהל הפרויקט של הספק יעמוד בראש הצוות מטעם הספק הזוכה, אלא אם כן תחליט הרשות אחרת.

- צוות אבטחת מידע והגנת הפרטיות

<u>אחריות</u>: הצוות יהיה אחראי על הכנת תכנית אבטחת מידע לתהליך ההיפרדות ומעבר המערכת לניהול הספק הזוכה, וכן על העברת הידע והיכולות, החל באבטחת מידע פיסית, ומאפייני הגנת הפרטיות הקיימים במערכת וכלה בהגנה על המערכות השונות של המערכת.

<u>חברי הצוות</u>: הממונה על הגנת הפרטיות והממונה על אבטחת המידע מטעם הספק הזוכה, נציג רלוונטי מהספק המחליף. בראש הצוות יעמוד הממונה על אבטחת מידע מטעם הספק הזוכה, אלא אם כן תחליט הרשות אחרת.

- צוות משפטי

<u>אחריות</u>: הצוות יהיה אחראי על ניהול כלל הנושאים החוזיים בין הספק הזוכה לבין הרשות ו/או הספק המחליף, חוזים של הספק הזוכה מול ספקי משנה, וכן העברת עובדים במידת הצורך.

<u>חברי הצוות</u>: נציגים משפטיים מטעם הספק הזוכה ומטעם הספק המחליף, הרשות רשאית להעמיד נציג משפטי מטעמה, על פי שיקול דעתה הבלעדי.

- צוות תשתיות

אחריות: הצוות יהיה אחראי על העברת התשתיות לטובת הרשות ו/או הספק המחליף, בהתאם לרצון הרשות ובתיאום עמה ועם הספק המחליף. כמו כן, על מתן סיוע טכני ועדכון התיעוד של כלל התשתיות ואופן פעולתן. במידת הצורך, יעסוק צוות זה בהעברת רכיבי התשתיות.

חברי הצוות: נציגי הספק הזוכה והספק המחליף, הרשות רשאית להעמיד נציג מטעמה, על פי שיקול דעתה הבלעדי, בראש הצוות מטעם הספק הזוכה יעמוד מנהל **IT**.

- צוות פיתוח

אחריות: הצוות יהיה אחראי על העברת הקוד של המערכת שפותחה עבור פעילות המערכת. תתבצע העברה של כלל הפרויקטים הנמצאים בפיתוח אצל הספק הזוכה. כמו כן יסופקו הדרכות של ראשי הצוותים של כל מודול.

חברי הצוות: מנהל הפיתוח מטעמו של הספק הזוכה, מנהל פיתוח מטעם הספק המחליף, הרשות רשאית להעמיד נציג מטעמה, על פי שיקול דעתה הבלעדי. ראשי הצוותים של המודולים השונים במערכת, יזומנו לדיונים במידת הצורך. העומד בראש צוות הפיתוח יקבע ע"י הרשות.

- צוות תפעול ושירות

אחריות: הצוות יהיה אחראי על העברת הידע והיכולות של מוקד התפעול של המערכת ובכלל זה מערך השירות הטכני, סוגיות גביה וכו'. הספק הזוכה יאפשר לנציגי הרשות גישה אל מוקד השירות של המערכת. במקביל, תתבצע העברת תיעוד של תהליכים המתבצעים במערך התפעול והשירות של המערכת.

חברי הצוות: מנהל התפעול של הספק הזוכה יעמוד בראש הצוות מטעמו, נציג הספק המחליף ונציג הרשות. מנהל המוקד ומנהל התשתיות יזומנו לדיונים במידת הצורך. העומד בראש צוות תפעול ושירות יקבע ע"י הרשות.

10.2. יובהר, הרשות רשאית למנות נציגים מטעמה אשר יתלוו למי מהצוותים ואף יעמדו בראשם, על פי החלטתה.

10.3. כל צוות אמון על כתיבת תכנית חפיפה מסודרת ומפורטת אשר תעמוד בדרישות שלהלן:

- התוכנית תכתב במשותף ע"י נציגי הספק הזוכה ונציגי הספק המחליף בכל אחד מהצוותים.
- תכנית העבודה של כל אחד מצוותי העבודה תוגש לצוות הניהול עד 15 ימים מיום הקמתו של כל צוות.
- תכנית העבודה תכלול אבני דרך לביצוע, לוח זמנים מפורט וכן גורם אחראי לביצוע כל משימה.
- מעקב אחר ביצוע: יתקיימו פגישות שבועיות בין נציגי הרשות והצוות הניהולי כדי לעקוב אחר התקדמות החפיפה ופתרון בעיות ככל שיעלו. בסיום כל פגישה ייכתב סיכום

אשר יפרט את המשימות שהוטלו בה, כולל אחראי לביצוע ותאריכי יעד לביצוע, וינוהל מעקב אחר המשימות וביצוען.

11. סיום פיתוח בעת היפרדות

11.1. המזמין רשאי לקבוע כי הספק הזוכה ישלים פרויקטים בפיתוח שאושרו על ידי המזמין או יעבירם לספק המחליף לשם השלמת הפיתוח, הכל על פי שיקול דעתו הבלעדי ובמסגרת התמורה הקבועה במכרז זה, ללא כל תמורה נוספת.

11.2. משימות אשר הוחלט על ידי הרשות כי יעברו לספק המחליף יועברו לטיפול הספק המחליף באופן מסודר אשר יכלול את כל המסמכים הרלבנטיים, אפיונים, תסריטי בדיקה, מבחני מסירה, שורות קוד, ומסמכים רלבנטיים אחרים אשר נדרשים באופן סביר לצורך המשך הפיתוח.

12. **תקופת תמיכה**

12.1. הספק הזוכה יספק שירותי תמיכה לספק המחליף, במהלך תקופה של שנה לכל היותר מיום השלמת ההיפרדות והעברת האחריות לספק המחליף, וזאת ללא קשר לעילה לסיום ההתקשרות, הכל על פי דרישת הרשות. הספק הזוכה מתחייב לסייע ולשתף פעולה עם הצוות תוך התחייבות למתן שירות מקצועי לספק המחליף.

12.2. במהלך תקופת התמיכה לא יהא הספק הזוכה אחראי לרמת השירות שלה התחייב בתקופת ההסכם. האחריות למתן השירותים תהא באחריות הספק המחליף.

12.3. תעריפי השירותים לספק הזוכה בתקופת התמיכה יחושבו בהתאם להוראת תכ"ם - הספקת שירותי מחשוב למשרדי ממשלה מס' 16.2.11 (תעריפי גג) או תעריפי התקשרות עם נותני שירותים חיצוניים מס' ה.8.1.1.1, על פי העניין.

12.4. הספק הזוכה לא ימנע, בכל דרך שהיא, מעובדיו המעוניינים בכך, לתת למזמין או לספק המחליף שירותים לאחר סיום ההתקשרות, בכל דרך שהיא, ובכפוף להוראות כל דין.

12.5. הספק הזוכה לא ימנע, בכל דרך שהיא, מספק משנה, המספק למערכת הסליקה שירות או מוצר למימוש אחת או יותר מדרישות מכרז זה, להתקשר עם ספק אחר או עם המזמין למתן שירות או מוצר זהה או אחר לאחר סיום ההתקשרות, בכל דרך שהיא, ובכפוף להוראות כל דין.

13. תמורה ותמחור ציוד בעת הפרדות

13.1. מובהר כי הספק הזוכה לא יקבל כל תמורה נוספת מעבר לתמורה המוגדרת בפרק 7 מודל התמחור, בגין תהליך ההיפרדות.

13.2. החל ממועד השלמת תקופת ההיערכות והעברת האחריות לספק המחליף, התמורה בגין הפעלת המערכת תשולם לספק המחליף ולו בלבד.

13.3. במקרה של היפרדות הנובעת מהפרת התנאים הקבועים בהסכם ההתקשרות ובמכרז זה על ידי הספק הזוכה, יהא המזמין רשאי לקזז את עלות הנזקים ככל שנגרמו כתוצאה מהפרה

זו מהתמורה או מערבות הביצוע, והכל בכפוף לזכויות המזמין על פי ההסכם ובכפוף להוראות הדין.

13.4. הספק המחליף יחזיק בזכות (אך לא בחובה) לרכוש או לשכור כל ציוד הנרכש או נשכר על ידי הספק הזוכה, אשר משמש את הספק הזוכה, עובדיו או ספקי המשנה על מנת לספק את השירותים. ציוד זה יועבר במצב תקין, ויתומחר על פי השווי ההוגן שלו. במקרה בו מועבר ציוד אשר נרכש על ידי הספק הזוכה, יעביר הספק הזוכה הסכמי SLA או אחריות רלבנטיים. במקרה שבו הספק מעביר ציוד מושכר הוא יספק אישורים על ביצוע התשלומים עד למועד העברת השכירות, אישור כי חוזה השכירות עודנו בתוקף וכן את חוזה השכירות עצמו.

13.5. במקרה שבו הצדדים אינם מסכימים על השווי ההוגן של הציוד, כאמור לעיל, ימנה הממונה שמאי מכריע בלתי תלוי אשר יקבע את המחיר ההוגן. הוצאותיו של השמאי יחולקו שווה בשווה בין הצדדים, הספק הזוכה והספק המחליף.

14. עובדי הספק הזוכה וספקי משנה

14.1. על מנת לאפשר המשכיות הפעילות העסקית, יפעל הספק הזוכה, על מנת לוודא כי בעת סיום ההתקשרות, מכל סיבה שהיא, תעמוד אפשרות לספק המחליף להיכנס בנעליו של הספק הזוכה, בעבודתו מול ספקי משנה אשר מספקים מוצרים ושירותים, נשוא מכרז זה.

14.2. הספק הזוכה יעשה את מיטב המאמצים מול עובדיו ויוודא כי הסכמי העסקתם מאפשרים במקרה של סיום ההתקשרות בין הספק לרשות מעבר של עובדים לעבודה אצל הספק המחליף ובכך את המשך מתן השירותים על ידם, והכל בכפוף להוראות כל דין.

14.3. הספק הזוכה יאפשר לספק המחליף גישה סבירה לעובדיו לצורך ראיונות, מבדקים וגיוס. המזמין או הספק המחליף יבצע את הפעולות האמורות באופן שלא יפריע באופן בלתי נחוץ לעבודתו של הספק הזוכה או להתחייבויותיו.

14.4. הספק לא יתערב בהליך גיוס העובדים של הספק המחליף או בהליך התקשרות של הספק המחליף עם ספקי משנה, וכן לא ימנע בכל דרך שהיא מספק משנה להתקשר עם הספק המחליף לאחר סיום ההתקשרות, כולל הצעת מחיר נגדיות עבור מתן שירותים למזמין או בא כוחו.

14.5. הספק הזוכה יודיע לספק המחליף על הסכמים אשר נחתמו עם צדדים שלישים עובדיו, ספקי המשנה או ספקיו לצורך ביצוע העבודה. במסגרת זו יועברו תאריכי החתימה, התנאים, אופציות, היבטים כספים ואדמיניסטרטיביים והשלכת סיום הקשר בין המזמין לספק על המשך הסכמים אלו. כמו כן, יודיע הספק הזוכה על בעיות כספיות, תפעוליות, מקצועיות, טכניות, משפטיות או אחרות העשויות להשפיע על תקפותם של ההסכמים כאמור.

15. הסבת הסכמי זכויות השימוש בתוכנה

15.1. הספק הזוכה מתחייב להעביר את כל זכויות השימוש והבעלות שברשותו לספק המחליף, בהתאם לאמור במסמכי המכרז. יחד עם זאת, לגבי מוצר צד ג' המשמש את מערכת

הסליקה, הספק הזוכה יידרש להתחייב להעביר לספק המחליף את זכויות השימוש במוצר זה, ככל שהוא נדרש לצורך הפעלתה התקינה של מערכת הסליקה. כמו כן, הספק הזוכה לא יעשה שימוש במוצר צד ג' אשר לו בלבד יש זכויות שימוש בו ואשר לא ניתן יהיה להעביר את זכויות השימוש לספק המחליף או שלא יתאפשר לספק המחליף לרכוש זכויות שימוש אלה במחיר שוק סביר (ככל שמדובר על מוצר צד ג' שאינו זמין לכל דורש).

15.2. הספק הזוכה יעביר למזמין או לספק המחליף הסכמים (הכוללים תאריכי התקשרות, עלות תמורה שנתית, מנגנוני הצמדה, ככל וישנם) או מסמכים הקשורים לרישיונות או זכויות לעשות שימוש בכל תוכנה הדרושה לביצוע העבודה נושא מכרז זה ו/או לכל שירות מקצועי או ייעוץ הנדרש לשם כך. הספק הזוכה יעביר לספק המחליף את כלל התיעוד העדכני הנדרש לשימוש בתוכנות אלו.

15.3. הספק הזוכה יעביר תיעוד עדכני של כל קוד מקור, אפיונים, מסמכי עיצוב, תסריטי בדיקה, חומרי הדרכה או מסמכים רלבנטיים אחרים אשר נדרשים באופן סביר על ידי המזמין ו/או הספק המחליף לצורך המשך ביצוע העבודה נשוא מכרז זה.

15.3. לאורך תקופת ההיערכות הספק הזוכה יאפשר לכל גורם מטעם המזמין, גישה לשרתי מערכת הסליקה, שבהם מאוחסנים כל המסמכים והמידע הנדרשים לשם הפעלת המערכת והעברת הבעלות לגביה.

16. <u>שמירה על סודיות</u>

16.1. הספק הזוכה מתחייב כחלק מנוהל ההיפרדות, כי לא יותיר בידיו כל חומר, מידע, נתונים או תיעוד הנוגע למזמין ו/או למתן השירותים המנויים במכרז זה, בכל פלטפורמה שהיא, לרבות מידע השמור במערכת הסליקה או שהועבר בה וכי יתעד את תהליך השמדת הנתונים שהיו ברשותו, למעט נתונים או מסמכים אשר נדרש לשומרם בהתאם להוראות כל דין.

נספח ב.3 – מחירון השירותים

על המחירים יתווסף מע״מ כדין.

קוד קיים	פעולה	מחירון בסיס למכרז - ₪ לא כולל מע״מ
9100	מידע מכלל הגופים (טרום ייעוץ)	11
1700	העברת ייפוי כוח לחברה מנהלת	1
2100	בקשה לקבלת דוחות פרודוקציה מיצרן ספציפי חודשי מתמשך	0.35
9300	מידע על יתרות פיצויים למעסיק מחברה מסוימת	1
9303	בקשת מעסיק לקבלת מידע על יתרות פיצויים הרשומות לזכות עובד מסוים - מכל המוסדיים הרלוונטיים	1
2500	בקשה לביטול בקשה לפרודוקציה מיצרן ספציפי	0
1400	עדכון פרטים אישיים של עמית בכל המוצרים אצל יצרן מסוים	0
2200	בקשה לקבלת דוחות פרודוקציה מיצרן ספציפי רבעוני	1
2000	בקשה לקבלת דוחות פרודוקציה מיצרן ספציפי חד פעמי	1
2101	בקשה לקבלת דוחות פרודוקציה מיצרן ספציפי עבור מעסיק ספציפי חודשי מתמשך	0.35
1802	העברת מסמכים עבור עדכון מסלולים במוצר קיים של החוסך	1
1900	ביטול ייפוי כוח בכל המוצרים אצל חברה מנהלת	1
9401	בקשה לקבלת מידע בסיסי מכלל הגופים המוסדיים אגב הפקדת כספים פנסיוניים לצורך קבלת מידע בטרם ביצוע הפקדה ראשונה בעד לקוח שהוא עובד חדש של המעסיק	1
1402	עדכון מין ותאריך לידה של עמית בכל המוצרים אצל יצרן מסוים	0
1800	העברת מסמכים עבור הצטרפות החוסך למוצר חדש	1
9302	בקשת מעסיק לקבלת מידע על יתרות פיצויים בגין כלל העובדים – מכל המוסדיים הרלוונטיים	1
2300	בקשה לקבלת דוחות פרודוקציה מיצרן ספציפי חצי שנתי מתמשך	1
9301	מידע על יתרות פיצויים לעובד מחברה מסוימת	1
9101	מידע על כלל המוצרים בחברה מסוימת	1
2001	בקשה לקבלת דוחות פרודוקציה מיצרן ספציפי עבור מעסיק ספציפי חד פעמי	1
2400	בקשה לקבלת דוחות פרודוקציה מיצרן ספציפי שנתי מתמשך	1
1401	עדכון כתובת של עמית במוצר מסוים אצל יצרן מסוים	0
1901	ביטול ייפוי כוח במוצר מסוים אצל חברה מנהלת	1
9305	בקשה לקבלת מידע מיצרן מסוים על יתרות פיצויים הרשומות לזכות חוסך בגין תקופת עבודתו אצל מעסיק מסוים	1
9200	מידע על מוצר מסוים	1
9402	בקשת מעסיק לקבלת מידע בסיסי אודות מוצרים פעילים של עובדיו	1
1803	העברת מסמכים עבור עדכון הפקדות במוצר קיים של החוסך	1

קוד קיים	פעולה	מחירון בסיס למכרז - ₪ לא כולל מע"מ
1801	העברת מסמכים עבור עזיבת מקום עבודה של החוסך	1
9403	בקשת מעסיק לקבלת מידע בסיסי אודות מוצרים פעילים של עובד מסוים	1
1804	העברת מסמכים עבור שינוי הפרשות במוצר קיים של החוסך	1
2301	בקשה לקבלת דוחות פרודוקציה מיצרן ספציפי עבור מעסיק ספציפי חצי שנתי מתמשך	1
1810	העברת מסמכים מאת מעסיק לגוף מוסדי	1
1902	ביטול ייפוי כח לבעל רישיון לכל המוצרים בגוף מוסדי מסוים ביוזמת חוסך	1
1903	ביטול ייפוי כח לבעל רישיון במוצר פנסיוני מסוים של לקוח ביוזמת חוסך	1
2201	בקשה לקבלת דוחות פרודוקציה מיצרן ספציפי עבור מעסיק ספציפי רבעוני מתמשך	1
2401	בקשה לקבלת דוחות פרודוקציה מיצרן ספציפי עבור מעסיק ספציפי שנתי מתמשך	1
9102	בקשה לקבלת מידע על קרנות פנסיה חדשות	1
9201	בקשת מידע למוצר (מתמשך)	1
9306	בקשה לקבלת מידע על יתרות פיצויים הרשומות לזכות לקוח	1
	סליקת כספים אגב דיווח ממשק מעסיקים	0
	העברת מידע בין גופים מוסדיים אגב ניוד כספים	0
	ממשק מעסיקים	1
	בקשה לקבלת מידע ב) API -שאינה בקשת מידע 9100(	1
	פעולה חדשה שתתווסף ב API -	0.1
	הנפקת סרטיפיקט לשנה לגוף שאינו גוף מוסדי	4,000
	כספת	3,000
	הנפקת טוקן פיזי לשנה	350
	הנפקת טוקן אפליקטיבי לשנה	250

נספח ב.4 – מצב קיים

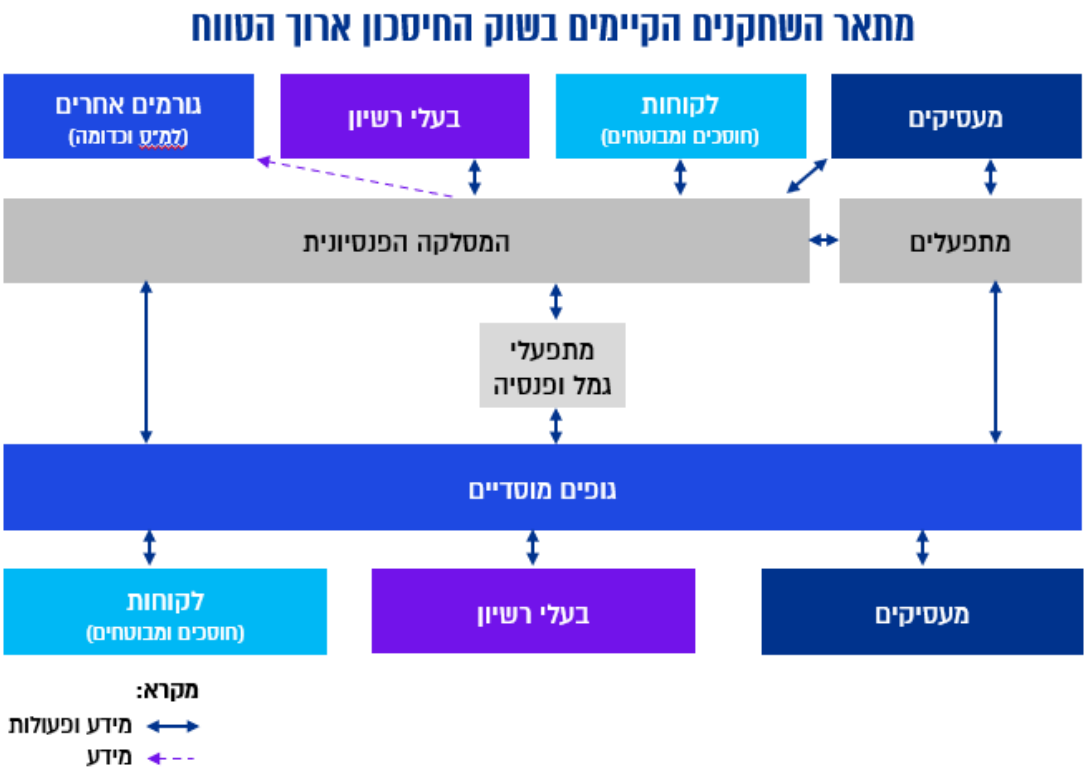
נספח זה מתאר את השירותים המרכזיים הניתנים כיום על ידי מערכת הסליקה, וכן את המערכות הטכנולוגיות המשמשות למתן השירותים. מטרת המידע המובא בנספח זה לאפשר למציע להעריך את פעילות מערכת הסליקה כיום מבלי לפגוע בסודות מסחריים של הספק הקיים.

1. <u>שירותים מרכזיים הניתנים על ידי מערכת הסליקה</u>

1.1. כללי

מערכת הסליקה מהווה תשתית טכנולוגית המקשרת בין השחקנים השונים בשוק החיסכון ארוך הטווח (לקוחות, משתמשים וגורמים אחרים). הגופים המוסדיים מחויבים להתחבר למערכת הסליקה, ואילו מערכת הסליקה מחויבת לספק שירותים לכלל השחקנים בשוק המעוניינים לפעול באמצעותה או מחויבים לפעול באמצעותה בהתאם לסעיף 31יא' לחוק הייעוץ הפנסיוני ולהוראות חוזר חובת שימוש (עשויים אפוא להיות מצבים שבהם אין חובה לפעול דרך מערכת הסליקה. כך, למשל, מעסיק אינו מחויב לפעול באמצעות מערכת הסליקה, אלא יכול לפעול באמצעות מתפעל מול גוף מוסדי ישירות).

התרשים שלהלן מתאר את האקוסיסטם הקיים ביחס לשחקנים בתחום החיסכון ארוך הטווח:



1.2. שירותי מערכת הסליקה:

1.2.1. השירותים שניתנים על ידי מערכת הסליקה ללקוחותיה ומשתמשיה, עוסקים בהעברת מידע, בקשות לקבלת מידע וביצוע פעולות לרבות קבלת המענה עליהן, וסליקת כספים, בהתאם לסעיף 31ט' לחוק הייעוץ הפנסיוני וכוללים:

א. העברת מידע על לקוח, לפי בקשתו, מכלל הגופים המוסדיים לכל בעל רישיון, לשם ביצוע ייעוץ פנסיוני או שיווק פנסיוני;

ב. העברת מידע הנוגע ללקוח, על פי בקשתו, לגבי מוצר פנסיוני או תכנית ביטוח, מכלל הגופים המוסדיים;

ג. העברת מידע הנוגע ללקוח, לפי בקשתו, מבעל רישיון לגוף מוסדי, לשם ביצוע עסקה בעבור הלקוח;

ד. העברת בקשה של לקוח לגוף מוסדי לביצוע פעולות בעבור הלקוח;

ה. העברת דוח יתרות מגוף מוסדי למעביד, לגבי הפקדות למרכיב הפיצויים שאינם באים במקום פיצויי פיטורים לפי סעיף 14 לחוק פיצויי פיטורים, התשכ"ג-1963, ובהתייחס לתקופת חבותו של המעביד;

ו. העברת מידע שאינה כאמור בפסקאות ג'-ה' כפי שקבע השר באישור ועדת העבודה הרווחה והבריאות של הכנסת, ובלבד שהעברה כאמור נעשית לבקשת לקוח, אגב עיסוק הנתון לפיקוחו של הממונה לפי כל דין;

ז. העברת משוב לבקרה בין המשתמשים במערכת על פעולות שבוצעו כאמור בסעיף ג'-ז' או בסעיף א' או העברת משוב לבקרה על פעולה שבוצעה כאמור בסעיף ב';

ח. העברת כספים בין גופים מוסדיים שונים לפי סעיף 23 לחוק הפיקוח על קופות גמל, והעברת מידע בין גופים אלה אגב העברת כספים כאמור, לפי הוראות אותו סעיף, וכן העברת מידע בין גופים מוסדיים לפי הוראות סעיף 24ב(א) לחוק הפיקוח על קופות גמל, לשם איתור כספים הרשומים על שמו של עמית לא מפקיד, כהגדרתו בסעיף 24ב(ג) לחוק האמור, בחשבונות בקרן פנסיה והעברתם לקרן הפנסיה שאליה הצטרף;

ט. הפקדת כספים בעד לקוח אצל גוף מוסדי, והעברת מידע אגב הפקדה כאמור, על ידי בעל רישיון או מעביד;

י. העברת כספים שאינה כאמור בפסקאות ח' ו- ט', כפי שקבע השר באישור ועדת העבודה הרווחה והבריאות של הכנסת, ובלבד שהעברה כאמור נעשית לבקשת לקוח, אגב עיסוק הנתון לפיקוחו של הממונה לפי כל דין;

העברת משוב לבקרה בין המשתמשים במערכת על פעולות שבוצעו כאמור בסעיפים ח'-י'.

1.2.2.בכל הקשור לפעולה של סליקת כספים - מערכת הסליקה, נכון למועד זה, מבצעת סליקה של הוראות התשלום עצמן המתייחסות להפקדות של מעסיק עבור עובדיו באמצעות מערכת מס״ב, כספק משנה, וזאת לאחר שמערכת הסליקה מעבירה למס״ב את הקובץ המרוכז של המעסיק לצורך ביצוע ההפקדות בפועל. בכל יתר הפעולות שקשורות להעברה של כספי לקוחות, נכון למועד זה, הוראות התשלום עצמן מועברות על ידי הלקוחות והמשתמשים באופן ישיר למערכת מס״ב (ובאמצעות מס״ב לגופים המוסדיים), כך שמערכת הסליקה מנהלת רק את קבצי המידע הנוגעים להוראות התשלום על מנת שניתן יהיה לשייך הוראות תשלום אלה לחשבונות הלקוחות בגופים המוסדיים.

1.2.3.יובהר בזאת כי אין בפירוט לעיל על-מנת לפרט את כל השירותים הקיימים, ועל המציע לעיין בסעיף 31ט לחוק הייעוץ הפנסיוני, בחוזר מבנה אחיד, בחוזר חובת שימוש ובחוזר ייפוי כוח לבעל רישיון.

1.2.4.להלן פירוט היקפי הפעילות בשירותים מרכזיים נבחרים אשר ניתנו על ידי מערכת הסליקה בשנים 2022-2024 (פעולות אלה מהוות כ- 90% מפעילות מערכת הסליקה בשנים אלה):

מספר פעולה	קוד אירוע / שנה	2022	2023	2024
		מס׳ פניות	מס׳ פניות	מס׳ פניות
1	**9100** - מידע מכלל הגופים - הדיווח לא כולל בקשות 9100 מתמשכות שהוגשו על ידי חוסכים וגם לא את בקשות ה״ריענון״ שלהם	2,422,551	2,620,328	2,893,152
2	**9102** - בקשה לקבלת מידע על קרנות פנסיה חדשות	907,972	925,091	972,216
3	**1700** - העברת ייפוי כוח לחברה מנהלת	378,911	470,920	507,907

מספר פעולה	קוד אירוע / שנה	2022		2023		2024	
		מס׳ פניות	מס׳ מענים בת.ז (לחודש)	מס׳ פניות	מס׳ מענים בת.ז (לחודש)	מס׳ פניות	מס׳ מענים בת.ז (לחודש)
4	**2100** - בקשה לקבלת דוחות פרודוקציה מיצרן ספציפי חודשי מתמשך	20,051	2,174,497	27,730	2,436,917	38,350	2,736,963

		2022	2023	2024
5	בקשה לניוד	1,843,983	1,781,970	2,009,036

1.2.5.כל שירותי המערכת ניתנים בהתאם להוראות הדין ובכלל זה הוראות הממונה הרלוונטיות, לרבות חוזר חובת שימוש המגדיר את השירותים שמחויבים להינתן באמצעות המערכת כאמור, וחוזר מבנה אחיד המגדיר, בין השאר, את הממשקים, התהליכים והטכנולוגיה שבה מועבר המידע בין השחקנים השונים (נכון למועד זה המידע מועבר באמצעות טכנולוגיית כספות בתקשורת א-סינכרונית כמפורט בחוזר). יובהר כי תעריפי השימוש של כל בקשה מוגדרים בחוזר תשלומים.

1.2.6.רשימת הממשקים בחוזר מבנה אחיד לפיהם ניתנים שירותי מערכת הסליקה, נכון למועד זה, היא:

1.2.6.1. <u>ממשק אחזקות</u> - קובע את מבנה הקובץ ופרטי המידע שעל גוף מוסדי להעביר ללקוח שביקש זאת באמצעות מערכת סליקה פנסיונית מרכזית או לבעל רישיון, על מנת להציג סטאטוס עדכני של נתוני לקוח, על מוצריו הפנסיוניים השונים (לרבות מידע לגבי צבירות החיסכון), נכון לתאריך חתך מסוים. קובץ כאמור יימסר במסגרת התקשרות למתן ייעוץ פנסיוני מתמשך או שיווק פנסיוני.

1.2.6.2. <u>ממשק טרום ייעוץ</u> - קובע את מבנה הקובץ ואת פרטי המידע שעל גוף מוסדי להעביר לבעל רישיון בשלב ההכנה למתן ייעוץ פנסיוני או שיווק פנסיוני לראשונה.

1.2.6.3. <u>ממשק ניוד</u> - קובע את מבנה הקובץ ואת פרטי המידע שיועברו בעת העברת כספים בין מוצרים פנסיוניים שונים ובין גופים מוסדיים שונים.

1.2.6.4. <u>ממשק אירועים</u> - קובע את מבנה הקובץ ואת פרטי המידע אשר נדרש להעביר לגופים המוסדיים, במטרה לאפשר הצטרפות, קליטה והפקה של מוצרים פנסיוניים באופן ממוכן, וכן את פרטי המידע שיועברו לצורך ביצוע שינויים במוצרים פנסיוניים שבידי לקוחות או בנתונים הרלוונטיים לניהול מוצרים פנסיוניים עבור לקוחות.

1.2.6.5. <u>ממשק אירועים – הקמה</u> - קובע את מבנה הקובץ ואת פרטי המידע אשר נדרש להעביר לגופים המוסדיים בכדי לאפשר הצטרפות, עדכון כיסוי ביטוחי בקרן פנסיה, מינוי מוטבים ושינוי מסלול ההשקעה במוצר קיים. כמו כן, הממשק מאפשר להעביר למעסיק את אופן פיצול כספים בין קופות הגמל של העובד, ולעניין גוף מוסדי המנהל קופת ביטוח גם את אופן פיצול הכספים בין הפוליסות הרשומות לזכות המבוטח.

1.2.6.6. <u>ממשק היזון חוזר ראשוני</u> - קובע את מבנה הקובץ ופרטי המידע שעל הגוף להשיב בנוגע לתקינותו הטכנית של ממשק שהעובר אליו, ולגבי גוף מוסדי, קובע גם את פרטי המידע הנוגעים לסטטוס הטיפול בפניה.

1.2.6.7. <u>ממשק פיצויים</u> - קובע את מבנה הקובץ ופרטי המידע שעל גוף מוסדי להעביר ללקוח או לבעל רישיון על פי בקשת הלקוח, בנוגע למרכיב

הפיצויים, ולגבי מעסיק, את פרטי המידע שגוף מוסדי יעביר לו לגבי מרכיב הפיצויים בהתייחס לתקופת חבותו לעובדיו.

1.2.6.8. ממשק מידע למעסיק - קובע את מבנה הקובץ ופרטי המידע שעל גוף מוסדי להעביר למעסיק בשלב קליטתו של עובד במקום עבודה חדש או לצורך טיוב המידע במערכות של המעסיק בנוגע למוצר שהועברו אליו על ידו הפקדות.

1.2.6.9. ממשק מעסיקים - קובע את מבנה הקובץ ופרטי המידע הנדרשים בגין תהליכי תשלום והפקדות לחיסכון פנסיוני, לרבות בעת פיצול הפקדות בין מוצרים פנסיוניים שונים. במסגרת ממשק זה מטופל גם נושא ההיזון החוזר למעסיקים.

1.2.6.10. ממשק דמי סליקה - קובע את מבנה הקובץ ואת פרטי המידע שעל סוכן הביטוח או גוף קשור בו להעביר לגוף מוסדי בגין שירותי תפעול הניתנים למעסיק.

1.2.6.11. ממשק פניות איכות מידע - קובע את מבנה הקובץ ומבנה אחיד לטיפול בפניית איכות מידע כהגדרתה בחוזר פניות איכות המידע.

1.2.7. במסגרת מתן השירותים, מערכת הסליקה מבצעת הליך זיהוי ואימות של לקוחות ומשתמשי המערכת מבצעת תהליך של זיהוי לקוחות ומשתמשים באופן שמבטיח את אימות זהותו של לקוח, ובכלל זה אימות קיומה של הרשאה של לקוח לבעל רישיון, לצורך קבלת מידע או העברת בקשות לביצוע פעולות אל הגוף המוסדי. תהליך זה כולל זיהוי ראשוני במערכת, המבוסס על אמצעי זיהוי חזק (כגון זיהוי המבוסס על מסירת מספר תעודת הזהות, בצירוף מספר כרטיס אשראי אישי הנמצא ברשות הלקוח ושלוש הספרות בגב כרטיס האשראי או סיסמא מזהה שתישלח ללקוח באמצעות חשבון **iPost** המנוהל בדואר ישראל על שם הלקוח); זיהוי שוטף המשמש לצורך שימוש במערכת, באמצעות צירוף מספר תעודת זהות ששימש לזיהוי הראשוני וסיסמא חד פעמית (**OTP**) שתישלח ללקוח לפני כל כניסה למערכת הסליקה באמצעי לבחירתו (כגון דוא"ל, טלפון); ואימות הרשאה לבעל רישיון (ככל שהבקשה הועברה על ידי בעל רישיון), לאחר שהמערכת בדקה את תקינות ההרשאה ווידאה שההרשאה מבעל הרישיון מתייחסת לפרטי הזיהוי של הלקוח והכל במתכונת המפורטת בחוזר ייפוי כוח.

1.2.8. כחלק מהפעלת מערכת הסליקה, קבע מפעיל המערכת הקיים לאחר קבלת אישורו המוקדם של הממונה, כללים לשימוש במערכת הסליקה, לתפקודה התקין וליישום ממשקי חוזר המבנה האחיד, וזאת בהתאם לסעיף 31י לחוק הייעוץ הפנסיוני. כללי המערכת מפורסמים בפורטל האינטרנט של מערכת הסליקה.

1.3. שירותים נלווים:

1.3.1. המערכת ומפעיל המערכת מספקים גם שירותים נלווים לשירותים האמורים לעיל, הכוללים, בין היתר, את השירותים שלהלן:

1.3.1.1. <u>הפעלה של פורטל אינטרנט</u> – המערכת מספקת פורטל אינטרנט המהווה ממשק למתן השירותים ללקוחות ומשתמשי המערכת וכן לצורך העברה של מידע לשחקנים השונים. הפורטל מתייחס באופן פרטני ללקוחות ולסוגי המשתמשים השונים ובכלל זה חוסכים, מעסיקים, בעלי רישיון וגופים מוסדיים. במסגרת שירות הפעלת הפורטל מתאפשרים שירותים בהתאמה לכל סוג משתמש ולקוח באזור האישי הייעודי, שבו בין היתר ניתן לבצע הרשמה לשירות, הפקת דוחות מידע, דיווח קבצי מעסיקים, הגשת פניות איכות מידע, העברת ייפויי כוח ועוד[5].

1.3.1.2. <u>בקרת איכות המידע</u> - המערכת מבצעת בקרות ובדיקות להבטחת איכות המידע המועבר במערכת ומהימנותו.

1.3.1.3. <u>מערכת גבייה</u> - המערכת מבצעת גבייה של דמי שימוש (קבועים ועבור ביצוע פעולות) מהלקוחות והמשתמשים השונים.

1.3.1.4. <u>תיעוד הפעילות</u> - המערכת מבצעת תיעוד של הפעילות בפן הטכנולוגי והמקצועי.

1.3.1.5. <u>שירותי תחזוקה ופיתוח</u> - מפעיל המערכת אחראי על תחזוקת המערכת, עדכון גרסאות, טיפול בתקלות, שמירה על עדכניות טכנולוגית, שיפורים ושדרוגים וכיוצא בזה.

1.3.1.6. <u>אינטגרציה</u> - מפעיל המערכת מפעיל סביבת ניסוי לטובת המערכת.

1.3.1.7. <u>הדרכות ללקוחות ומשתמשי המערכת</u> - מפעיל המערכת אחראי לקיום הדרכות ללקוחות ומשתמשי המערכת, לרבות הכנת מערך הדרכות כתוב.

1.3.1.8. <u>שירות לקוחות ותמיכה</u> - מפעיל המערכת מעמיד לרשות הלקוחות והמשתמשים מערך שירות ותמיכה שמורכב ממספר מוקדים ייעודיים.

2. <u>מערכות טכנולוגיות</u>

תשתיות הליבה של מערכת הסליקה וטכנולוגיות מרכזיות המשמשות אותה כיום:

<u>ארכיטקטורה רבת שכבות הכוללת:</u>

- Dynamics CRM - משמש כבסיס לניהול תיקים, משתמשים ותהליכי אירועים.
- ADI (Application & Data Integration) - מנועי עיבוד נתונים אצוותיים, (Batch) פועלים ברקע ואינם זמינים אונליין.
- פורטל משתמשים מבוסס (ADX Studio) נגיש לבעלי רישיון וללקוחות, מבצע אימותים באמצעות OTP או VIP .
- CyberArk / GoAnyWhere - מערך כספות להעברת ושמירת מסרים ונתונים מוצפנים.

[5] לפירוט ראו: אתר מערכת הסליקה הפנסיונית

- WS Bus + SSIS + WCF + DQS- רכיבי אינטגרציה ועיבוד זרימות נתונים.

<u>תשתיות תקשורת ורשת:</u>

- מופרדות לוגית ופיזית בין סביבת פיתוח, בדיקות, ייצור ו-DMZ.
- שימוש ב VLANs-ייעודיים, סגמנטים נפרדים לניהול.
- שילוב רכיבי Firewall, IPS, Anti-Bot, EDR, הקשחת תקשורת בפרוטוקולים מאובטחים בלבד (SSL, IPsec).

<u>רכיבי טכנולוגיות המידע העיקריים:</u>

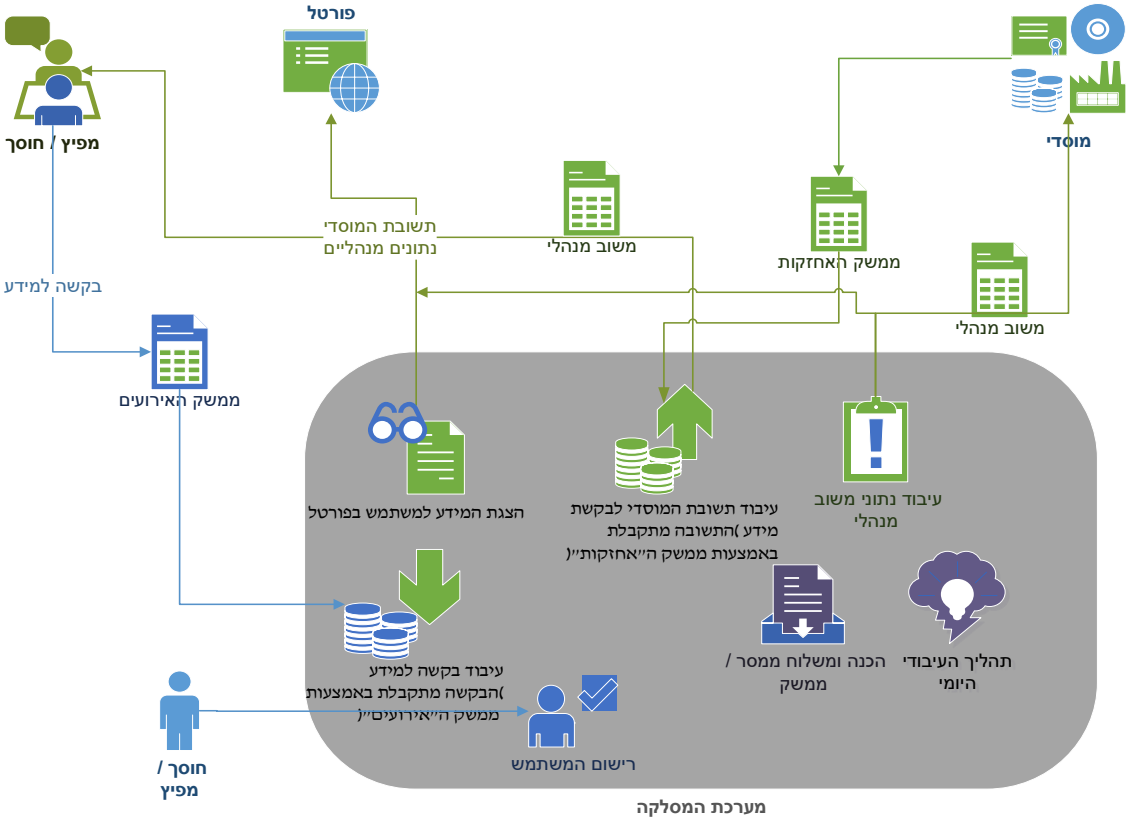
- Dynamics CRM Portal + ADX Studio
- AGForms
- SQL
- Windows Server
- CyberArk/GoAnyWhere
- WS Bus
- S.S.I.S (NBS)
- WCF, BRE, DQS
- AD
- SymantecVIP
- רשת תקשורת מערכת סליקה

תהליכי עיבוד המידע האישי במערכת הסליקה:

1. <u>במערכת קיימים שני תהליכי עיבוד מידע אישי מרכזיים:</u>
   - עיבוד בקשה למידע (הבקשה מתקבלת באמצעות ממשק "אירועים");
   - עיבוד תשובת הגוף המוסדי לבקשת מידע (התשובה מתקבלת באמצעות ממשק "אחזקות").
2. <u>בנוסף, קיימים חמישה תהליכי עיבוד נוספים (תהליכי שירות) אשר משרתים את התהליכים המרכזיים:</u>
   - רישום המשתמש;
   - עיבוד נתוני משוב מנהלי;
   - תהליך העיבוד היומי;

- הכנה ומשלוח ממסר / ממשק;
- הצגת המידע למשתמש בפורטל.

<u>תהליכי העיבוד במערכת הסליקה</u>:



*התהליכים המוצגים הינם תהליכים אסינכרוניים ללא תלות כרונולוגית או סדר פעולות ביניהם.

* מטרת האיור הינה להמחיש את קשרי הגומלין בין משתמשי ולקוחות המערכת ותהליכי העיבוד.

3. פירוט תהליכי העבודה

3.1 <u>עיבוד בקשה למידע (המידע מתקבל בממשק "אירועים")</u>

ממשק אירועים הינו ממשק ה"פניה" באמצעותו מועברות בקשות לקבלת מידע. הממשק מיוצר רק על ידי גורם הרשאי לפנות בשאלה (בעל רישיון, לקוח, מעסיק) ומיועד רק לגופים מוסדיים.

בשלב א', כולל הממשק נתונים אודות המידע בלבד, ובפרט, המידע המזהה של הלקוח נשוא הבקשה וסוג הבקשה (השאלה עצמה – כגון "בקשה למידע מכל הגופים המוסדיים").

תהליך העיבוד של הממשק כולל את: קבלת הממשק, בדיקות תקינות וחוקיות, החלטות על המשך הטיפול הנדרש (למי להעביר, מה להעביר, משוב לפונה וכד'), אחסון הממשק בבסיס

הנתונים, והקמת "תיק התכתבויות" במערכת ה - CRM במסגרתו יתועדו כל האירועים אשר יעברו במערכת הסליקה הקשורים לאותה הבקשה (נתונים על אודות המידע של האירועים).

החל משלב ב' ישמש אותו הממשק גם לפניה בבקשה לביצוע הוראה (כגון פתיחת חשבון חדש, ניוד חשבון בין קרנות וכד'). בשלב זה ובמסגרת הוראות מסוימות עשוי לעבור בממשק מידע אישי (כגון סכומי הפרשה מבוקשים בחשבון) ולכן מוקמת כבר בשלב א' תשתית להפרדת מידע מזהה בממשק.

3.2 <u>עיבוד תשובת המוסדי לבקשת מידע</u>

ממשק אחזקות הינו ממשק ה"תשובה" באמצעותו מוחזר המענה והמידע לבקשות לקבלת מידע. הממשק מיוצר רק ע"י גופים מוסדיים ומיועד לגורם אשר פנה בשאלה (בעל רישיון, לקוח, מעסיק).

ממשק האחזקות כולל מידע אישי מזוהה ומידע אישי מזהה של הלקוח נשוא הבקשה.

תהליך העיבוד של הממשק מבוסס על אותם העקרונות הקיימים בעיבוד בממשק ה"אירועים" וכולל את: קבלת הממשק, בדיקות תקינות וחוקיות, החלטות על המשך הטיפול הנדרש (למי להעביר, מה להעביר, משוב לפונה וכד'), אכסון הממשק בבסיס הנתונים, ועדכון "תיק התכתבויות" במערכת ה - CRM באירוע. יודגש כי העדכון במערכת ה – CRM הינו של נתונים אודות המידע בלבד (ממי מהגיע, מתי הגיע, באיזה קובץ הגיע וכד'). התהליך הינו אחד התהליכים הראשיים של מערכת הסליקה.

3.3 <u>רישום המשתמש</u>

רישום המשתמשים בעלי הרישיון למערכת הסליקה, הן לגישה באמצעות ממשקי ה-B2B והן לגישה באמצעות פורטל האינטרנט מתבצע בשני שלבים – רישום מוקדם (מתבצע האופן עצמאי ע"י בעל הרישיון בפורטל האינטרנט) והמשך הרישום והפעלה לשירות (מתבצע בשיתוף נציג מערכת הסליקה).

רישום הלקוחות למערכת הסליקה לגישה באמצעות פורטל האינטרנט בלבד, מתבצע באופן עצמאי על ידי הלקוחות. התהליך כולל זיהוי באמצעות צד שלישי: באמצעות פרטי כרטיס אשראי מול קרדיטגארד (הרשמה אונליין), או באמצעות משלוח סיסמה ראשונית בדואר רשום.

3.4 <u>עיבוד נתוני משוב מנהלי</u>

ממשק ההיזון החוזר הינו ממשק ה"Hand Shaking" באמצעותו מאשר מקבל ממשק את קבלת הממשק ואת תקינותו או מחזיר הודעות ונתוני שגיאה. הממשק מיוצר ע"י כל גורם המקבל ממשק בתקשורת B2B <u>לרבות מערכת הסליקה עצמה</u>, ומיועד לגורם אשר שלח את ממשק האירועים או האחזקות (ושוב, לרבות אל המערכת). הממשק אינו מופעל במקרה של בקשה או מידע המועבר למערכת הסליקה דרך פורטל האינטרנט.

הממשק כולל מידע מזהה של הלקוח נשוא הבקשה ונתונים על אודות המידע הקשורים לבקשה (מספר הבקשה, תקינות או אי תקינות, שגיאות בממשק וכד').

תהליך העיבוד של הממשק כולל את: קבלת הממשק, בדיקות תקינות וחוקיות, החלטות על המשך הטיפול הנדרש (למי להעביר, מה להעביר), ועדכון "תיק התכתבויות" במערכת ה - CRM באירוע.

3.5 תהליך העיבוד היומי

תהליך העיבוד היומי הינו מסגרת כללית לכל פעולות העיבוד העתיות אותן יש לבצע במערכת.

התהליך מופעל ע"י מתזמן המשימות וכולל סדרת פעולות לרבות השלמת הכנת ומשלוח כל הממסרים היוצאים (אשר לא נשלחו באופן מידי), הכנת תזכורות והתראות, מחיקת מידע בהתאם להוראות החוק ועוד.

התהליך מטפל בנתונים על אודות המידע הקשורים לבקשות המידע מהמערכת.

3.6 הכנת ומשלוח ממסר/ממשק (מכל סוג) למשתמש

תהליכי העיבוד של הממשקים אחראים על קבלת ההחלטות לאילו גורמים, באיזה מתכונת ובאיזו רמת דחיפות תועבר כל פניה או תשובה נכנסת לנמען/נים הרלוונטיים. התהליך מחליט גם אילו ממשקי היזון חוזר יועברו.

תהליך העיבוד אינו מטפל ישירות במשלוח אלא רושם את החלטותיו ב"טבלת ממסרים יוצאים".

בהתקיים התנאים המתאימים (תנאי תזמון או תנאי SLA) מופעל במערכת תהליך הכנת ומשלוח ממשק נושא ממסרים מסוג מסוים לגוף/פים הרלוונטי/ים. התהליך מזהה את הממסרים שיש לשלוח ואת הנמענים שולף את רשומת ה – XML המקורית, מצרף אליה את בלוק נתונים מזהים של הלקוח (באם הופרד ממנה) ומרכיב את ממסר ה – XML הנדרש. כל ממסרי ה – XML המיועדים לנמען אחד נארזים יחד בממשק XML, המערכת מוסיפה להם בלוק כותרת והממשק מועבר לחדר הכספות למשלוח לנמען המתאים.

התהליך מטפל במידע אישי מזוהה ומידע אישי מזהה של חוסכים וכן בנתונים על אודות המידע הקשורים לבקשות המידע מהמערכת.

3.7 הצגת המידע למשתמש בפורטל

תהליך הצגת המידע למשתמש בפורטל האינטרנט של מערכת הסליקה כולל, בין היתר, פנייה לשירות ההזדהות VIP של חברת סימנטק במטרה לאמת את אמצעי הזיהוי החזק (OTP) שברשות המשתמש מסוג בעל רישיון, או שימוש בזיהוי OTP חד פעמי ומוגבל בזמן המופק על ידי המערכת למשתמש מסוג לקוח.

התהליך מטפל במידע אישי מזוהה ומידע אישי מזהה של חוסכים וכן בנתונים על אודות המידע הקשורים לבקשות המידע מהמערכת.

חלק ג' –
חוברת ההצעה

הגשת הצעה במכרז

1 כללים למילוי חוברת ההצעה

1.1. פרק זה מהווה את מענה המציע למכרז, אין צורך במתן מענה לכל חלק אחר במכרז, או לצרף מסמך שאינו נדרש בפרק זה.

1.2. יש לעקוב באופן מדוקדק אחר ההנחיות המופיעות בפרק זה על מנת שההצעה תוכל להיבחן ולהיות מוערכת כראוי. אין להוסיף להתנות או לשנות אף תנאי מתנאי המכרז, או את ההנחיות המופיעות להלן.

1.3. בכל מקרה של שאלות או אי-בהירות במסמכי המכרז על המציע לפנות למזמין בשאלה לצורך הבהרה, כמפורט בחלק א' למסמכי המכרז.

1.4. ניתן לצרף כל מסמך או קובץ הרלוונטי לצורך פירוט והמחשה למפורט בהצעה. יודגש כי בדיקת ההצעה, תתבסס על הפירוט שיינתן בחוברת ההצעה.

1.5. חוסר פירוט בהצעה, או פירוט מיותר שאינו עונה לדרישת המכרז, עלולים להביא לניקוד נמוך של ההצעה או פסילתה, בהתאם לשיקול דעתו הבלעדי של המזמין.

2 פרטי המציע

שם המציע	
סוג מציע (תאגיד/שותפות/עמותה/עוסק מורשה וכדו')	
תאריך הרישום במרשם (אם רלוונטי)	
מספר מזהה (לדוג' ח"פ)	

3 פרטי איש הקשר מטעם המציע

שם:
כתובת:
טלפון:
דוא"ל:

4 הוכחת עמידה בתנאי הסף של המכרז

בהתאם לאמור בפרק זה המציע יפרט את עמידתו בתנאי הסף שפורטו במכרז.

הוכחת עמידה בתנאי הסף המנהליים:

המציע מצהיר ומתחייב כי הוא עומד בתנאי הסף המנהליים המפורטים בחלק א' למכרז ובהתאם לפירוט המובא להלן:

א. מציע רשום כדין (יש לסמן ב-X את האפשרות הנכונה) –

☐ המציע רשום בישראל כדין.

☐ לא חלה על המציע חובת רישום בישראל, על פי דין. נימוק:
_____

ב. עמידה בחוק עסקאות גופים ציבוריים –

ניהול פנקסים – המציע –

☐ מנהל את פנקסי החשבונות והרשומות שעליו לנהל על פי פקודת מס הכנסה [נוסח חדש], וחוק מס ערך מוסף, התשל"ו-1975 ("**חוק מס ערך מוסף**"), או שהוא פטור מלנהלם.

☐ מדווח לפקיד השומה על הכנסותיו ומדווח למנהל על עסקאות שמוטל עליהן מס לפי חוק מס ערך מוסף.

לצורך הוכחת עמידה בתנאי סף זה על המציע לצרף אישור פקיד מורשה ולסמנו כנספח ג.2.

ג. היעדר הרשעות –

המציע ו"בעל זיקה" אליו לא הורשעו ביותר משתי עבירות לפי חוק עובדים זרים התשנ"א - 1991 (להלן: "חוק עובדים זרים") וחוק שכר מינימום, התשמ"ז-1987 (להלן: "חוק שכר מינימום") עד למועד הגשת ההצעה מטעם המציע במכרז, או שהורשעו כאמור אך כבר חלפה שנה אחת לפחות ממועד ההרשעה האחרונה ועד למועד הגשת ההצעה.

לצורך הוכחת עמידה בתנאי סף זה על המציע לצרף את התצהיר המפורט בנספח ג.3.

ד. ייצוג הולם לאנשים עם מוגבלות (יש לסמן ב- X את אחת מהאפשרויות) –

☐ הוראות סעיף 9 לחוק שוויון זכויות לאנשים עם מוגבלות, התשנ"ח-1998 (להלן: "**חוק שוויון זכויות לאנשים עם מוגבלויות**") אינן חלות על המציע.

☐ הוראות סעיף 9 לחוק שוויון זכויות לאנשים עם מוגבלות חלות על המציע והוא מקיים אותן.

במקרה שהוראות סעיף 9 לחוק שוויון זכויות לאנשים עם מוגבלות חלות על המציע, יש לפרט את אופן עמידתו בדרישות החוק (יש לסמן ב- X את אחת מהאפשרויות):

☐ המציע מעסיק פחות מ-100 עובדים.

☐ המציע מעסיק 100 עובדים או יותר.

במקרה שהמציע מעסיק 100 עובדים או יותר (יש לסמן ב- X את אחת מהאפשרויות):

☐ המציע מתחייב כי אם יזכה במכרז יפנה למנהל הכללי של משרד העבודה והרווחה והשירותים החברתיים לשם בחינת יישום חובותיו לפי סעיף 9 לחוק שוויון זכויות לאנשים עם מוגבלות, ובמקרה הצורך– לשם קבלת הנחיות בקשר ליישומן.

☐ המציע פנה בעבר למנהל הכללי של משרד העבודה והרווחה והשירותים החברתיים לשם בחינת יישום חובותיו לפי סעיף 9 לחוק שוויון זכויות לאנשים עם מוגבלות, ואם קיבל הנחיות ליישום חובותיו פעל ליישומן.

ה. המציע עומד בדרישות הרישוי והתקנים הנדרשים על פי דין לצורך ההתקשרות, אם ישנם –

☐ כן

☐ לא

המזמין יהיה רשאי לבקש אישור על עמידה בתקנים או בתקנים זרים מקבילים, אם עמידה בתקן זר מקביל אפשרית בהתאם להוראות הדין.

הוכחת העמידה בתנאי הסף המקצועיים:

עם הגשת הצעה זו, המציע מצהיר ומתחייב כי הוא עומד בתנאי הסף המקצועיים המפורטים בחלק א' למכרז.

המציע יפרט את אופן עמידתו בתנאי סף המקצועיים, בהתאם למפורט להלן:

למציע ניסיון מוכח של 3 שנים לפחות, בין השנים 2018-2024, בהקמה או בהפעלה של מערכות מידע מורכבות בתחומי הפיננסים או שוק ההון או החיסכון הפנסיוני.

שנת התחלה	שנת סיום	שם ותיאור המערכת	תחום (פיננסים או שוק ההון או החיסכון הפנסיוני)	שם לקוח ופרטי איש קשר (אם רלוונטי)

המציע העסיק בכל אחת מ- 3 השנים אחרונות (2022-2024) לפחות 30 עובדים בתחומי טכנולוגיות המידע.

שנה	מספר עובדים המועסקים אצל המציע	תחום
2024		
2023		
2022		

<u>צוות ניהול לפרויקט</u> - המציע נדרש לצרף אסמכתאות מתאימות לכל צוות ניהול הפרויקט המוצע על ידו (קו"ח, תעודות אקדמיות והכשרות נדרשות) בנספח ג.8.

ובנוסף, למלא את פרטי צוות ניהול הפרויקט המוצע על ידו, על פי הפירוט שלהלן:

<u>מנכ"ל:</u>

- **שם מלא של המועמד המוצע: _____**
- **פירוט ניסיון ניהולי:**

שם החברה/הגוף:	שנים:	התפקיד:	מספר עובדים:	פירוט אודות התפקיד:

				(ניתן להוסיף שורות)

<u>מנהל פרויקט:</u>

- **שם מלא של המועמד המוצע:** _____
- **פירוט ניסיון ניהול בפרויקטי פיתוח והפעלת מערכות מורכבות:**

שם החברה/הגוף:	שם הפרויקט:	שנים:	מספר אנשי פיתוח טכנולוגי בצוות:	פירוט אודות הפרויקט:
				(ניתן להוסיף שורות)

- **המועמד בעל ידע והיכרות מעמיקה בפרויקטים טכנולוגיים בתחום הפיננסיים וכן בעל הניסיון להלן:**

שם החברה/הגוף:	שם הפרויקט הטכנולוגי בתחום הפיננסי:	שנים:	פירוט אודות הפרויקט:
			(ניתן להוסיף שורות)

<u>ממונה אבטחת מידע:</u>

- **שם מלא של המועמד המוצע:** _____
- **המועמד הוא בעל ההסמכה הרשמית** _____ **שהוענקה לו ממוסד לימודים מוכר** _____ (יש לצרף אסמכתא מתאימה בנספח ג.8).
- **פירוט ניסיון ניהולי בתחום אבטחת המידע:**

שם החברה/הגוף:	שנים:	תפקיד:	פירוט אודות התפקיד (בדגש על פעילות בעלת מורכבות והיקפים דומים לאלו הנדרשים במכרז):
			(ניתן להוסיף שורות)

<u>מנהל פיתוח טכנולוגי:</u>

- **שם מלא של המועמד המוצע:** _____
- **המועמד בעל תואר ראשון במדעי המחשב/הנדסה תעשייה וניהול/מדעים מדויקים ממוסד לימודים מוכר** _____ (יש לצרף אסמכתא מתאימה בנספח ג.8).
- **פירוט ניסיון ניהול בפרויקטי פיתוח מערכות:**

שם החברה/הגוף:	שם הפרויקט:	שנים:	תפקיד:	מספר אנשי פיתוח טכנולוגי בצוות:	פירוט אודות הפרויקט:
					(ניתן להוסיף שורות)

ב.1. מחזור כספי - למציע מחזור כספי שנתי בהיקף שלא יפחת מ-25,000,000 ₪, בין השנים 2022-2024, עבור כל שנה:

יש לצרף חתימת רו"ח על **נספח ג.4** - אישור רו"ח מבקר אודות נתונים מהדוחות הכספיים, לצורך הוכחת עמידה בתנאי סף זה.

ב.2. הון עצמי - המציע יצרף כנספח ג.5 תצהיר התחייבות להעמדת הון עצמי עבור החברה שתוקם במידה ויוכרז כזוכה במכרז על פי הפירוט שלהלן וכל עוד לא נקבעו תקנות לעניין זה לפי סעיף 31ב(א)(3) לחוק:

- המציע יעמיד הון עצמי שלא יפחת מסך של 15 מיליון ש"ח (חמישה עשר מיליון שקלים חדשים) אשר יעמוד לאורך כל תקופת החפיפה ועד להשלמתה, כפי שמוגדרת בתכנית העבודה;
- המציע יעמיד הון עצמי שלא יפחת מסך של 10 מיליון ש"ח (עשרה מיליון שקלים חדשים) אשר יעמוד החל מהשלמת שלב החפיפה ותחילת שלב ב' - מתן השירותים, כפי שמוגדר בתכנית העבודה.
- סכומי ההון עצמי האמורים לעיל, יהיו נקיים מכל שיעבוד, עיקול וזכות צד ג' כלשהי.
- המציע יפרט את האמצעים ההוניים העומדים לרשותו, לרבות סעיף עודפים בהון העצמי.

התחייבויות ומסמכים נוספים שעל המציע להגיש במסגרת ההצעה

התחייבות להקמת חברה להפעלת מערכת סליקה פנסיונית מרכזית (נספח ג.6)

בהתאם להוראות סעיף 31ב חוק הייעוץ הפנסיוני, הממונה רשאי לתת - רישיון להפעלת מערכת סליקה פנסיונית מרכזית לחברה, כהגדרתה בחוק החברות, שעיסוקה הבלעדי הוא הפעלת מערכת סליקה פנסיונית מרכזית.

המציע יצרף להצעתו **כנספח ג.6** תצהיר התחייבות להקמת חברה להפעלת מערכת סליקה בתוך 30 ימים ממועד הזכייה, אשר תעמוד בכלל דרישות פרק ה'1 לחוק הייעוץ הפנסיוני, וזאת ככל שיוכרז כזוכה במכרז.

ההתחייבות תכלול פירוט רשימת בעלי המניות (כולל בעלי השליטה) וחברי הדירקטוריון המוצעים. בנוסף, המציע יצרף גם הסכם מייסדים הכולל התייחסות לכל הפחות לחלוקת המניות המוצעת ואופן הצבעה בדירקטוריון.

תכנית עסקית ופתרון טכנולוגי

המציע יענה לדרישות אלה במסגרת **נספח ג.9** להצעה.

איכות ההצעה

המציע ימלא, יפרט ויצרף מסמכים מתאימים על פי דרישות **נספח ג.9** - מענה מפורט לדרישות האיכות והדרישות המקצועיות.

היעדר ניגוד עניינים וכשירות להתמודדות במכרז

המציע מצהיר כי אינו מחזיק בקשרי בעלות לגוף מוסדי ו/או לבעל רישיון ו/או לתאגיד בנקאי, כהגדרתם בחוק הייעוץ הפנסיוני.

המציע יצרף **כנספח ג.7** הצהרה מחברי צוות ניהול הפרויקט המוצע על ידו, הכוללת פירוט של קשרים נוכחיים, ישירים ועקיפים, לרבות רשימת צדדים קשורים ובעלי עניין, עם גופים מוסדיים, בעלי רישיון וכן לענפי החיסכון הפנסיוני והבנקאות בכלל בישראל בלבד, אשר עולים כדי קשרי בעלות, קשרי עסקים או קשרים אחרים, העלולים ליצור מצב של ניגוד עניינים פוטנציאלי, קרבה היוצרת חשש לתלות או חשש לפגיעה אפשרית ביישום תפקידו וכן פגיעה אפשרית במטרות מערכת הסליקה.

ככל וקיים חשש יש לנמק מדוע לדעתם אין בפעילות זו משום ניגוד עניינים מהותי.

המציע מצהיר ומתחייב כי אינו מצוי בהליכי פשיטת רגל או פירוק ולא מתנהלות נגד המציע תביעות מהותיות, שעלולות לפגוע בתפקודו אם יזכה במכרז.

המציע מצהיר ומתחייב כי אין מניעה לפי כל דין להשתתפות המציע במכרז.

המציע מצהיר ומתחייב כי אין בהגשת הצעה במכרז או בביצוע ההתקשרות נושא המכרז, על ידי המציע, כדי ליצור ניגוד עניינים, בין במישרין ובין בעקיפין, בין המציע למזמין.

המציע מתחייב לעדכן בכתב את המזמין, ללא דיחוי, בכל שינוי מהותי אשר חל במידע שמסר במסגרת הצעתו המכרז.

אם המציע אינו חב במע"מ במסגרת ההתקשרות מכוח המכרז, הוא מצהיר על כך שפנה אל רשות המיסים לצורך קבלת אישור לכך, טרם הגשת הצעה במכרז.

אי תיאום הצעות מכרז

המציע מצהיר ומתחייב כי הפרטים המופיעים בהצעה זו הוחלטו על ידי המציע באופן עצמאי, ללא התייעצות, הסדר או קשר עם מציע אחר.

המציע מצהיר ומתחייב כי פרטי ההצעה לא הוצגו או יוצגו בפני כל אדם או תאגיד אשר מציע הצעות במכרז זה.

המציע מצהיר ומתחייב כי המציע לא היה מעורב בניסיון להניא מתחרה אחר מלהגיש הצעות במכרז זה, ולא היה מעורב בדרך כלשהי בהצעה שהוגשה על ידי מציע אחר.

המציע מצהיר ומתחייב כי המציע לא היה, ולא מתכוון להיות מעורב בניסיון לגרום למתחרה אחר להגיש הצעה גבוהה או נמוכה יותר מהצעתו זו.

המציע מצהיר ומתחייב כי המציע לא היה מעורב בניסיון לגרום למתחרה להגיש הצעה בלתי תחרותית מכל סוג שהוא.

המציע מצהיר ומתחייב כי הצעה זו מוגשת בתום לב.

עצמאות המציע

המציע מצהיר ומתחייב כי המציע אינו מחזיק או מוחזק על ידי מציע אחר במכרז (החזקה לעניין זה – החזקה במישרין או בעקיפין ב-25% או יותר מאמצעי שליטה, כהגדרתו בחוק ניירות ערך, התשכ"ח-1968).

המציע מצהיר ומתחייב כי גורם אחד אינו מחזיק ב-25% או יותר מאמצעי שליטה בו ובמציע נוסף במכרז.

המציע מצהיר ומתחייב כי המציע אינו קבלן משנה של מציע אחר במכרז, בקשר עם ביצוע השירותים במכרז זה.

בקשות

הגשת בקשות במסגרת ההצעה

במסגרת הצעתו רשאי המציע להגיש בקשות הנכללות בתנאי המכרז כמפורט בסעיף זה להלן וזאת כחלק בלתי נפרד מהצעתו.

הבקשות יכללו במסמכי ההצעה וינוסחו בצורה ברורה תוך הפנייה לסעיף אליו מתייחסת הבקשה.

מציע שלא יפנה למזמין בבקשה האפשרית בהתאם לכללי מכרז זה כחלק מהגשת הצעתו, יהיה מנוע מלהעלות בעתיד כל טענה, דרישה או תביעה בנושא ויראו בו כמי שוויתר על בקשתו או על הזכות הנובעת ממנה, בהתאם להקשר, אף אם הוא עומד בתנאים המהותיים המקימים את הזכאות - והכל לפני העניין והקשר הדברים.

עסק בשליטת אישה

מציע שהוא "עסק בשליטת אישה" בהתאם להוראות סעיף 2ב לחוק חובת המכרזים ומעונין שתינתן לו העדפה יצהיר על כך כלהלן (יש לסמן X במקום המתאים): .

☐ **המציע מצהיר כי הוא עסק אשר אישה מחזיקה בשליטה בו, ואשר יש לה, לבד או יחד עם נשים אחרות, היכולת לכוון את פעילותו וכי לא התקיים אף אחד מאלה:** (1) אם מכהן במציע נושא משרה שאינו אישה – הוא אינו קרוב של המחזיקה בשליטה; (2) אם שליש מהדירקטורים אינם נשים – אין הם קרובים של המחזיקה בשליטה;

לתמיכה בהצהרה זו, וכתנאי לקבלת העדפה על המציע לצרף אישור רו"ח ותצהיר כהגדרתם בחוק חובת המכרזים, המעידים על כך שהעסק הוא בשליטת אישה.

עידוד משרתי מילואים

מציע שמחזיק בשליטה בו הוא חייל מילואים כהגדרתו בחוק שירות המילואים, התשס"ח-2008, ששירת שירות מילואים 20 ימים לפחות במהלך 12 החודשים לפני המועד האחרון להגשת הצעות במכרז, ומעונין שתינתן לו העדפה בשל כך יצהיר כלהלן (יש לסמן X במקום המתאים):

☐ **המציע מצהיר כי הוא חייל מילואים כהגדרתו בחוק שירות המילואים, התשס"ח-2008, ששירת שירות מילואים 20 ימים לפחות במהלך 12 החודשים לפני המועד האחרון להגשת הצעות במכרז.**

הוא מחזיק בשליטה בעסק מגיש ההצעה. לעניין זה "מחזיק בשליטה" – משרת מילואים פעיל שהוא נושא משרה בעסק אשר מחזיק, לבד או יחד עם משרתי מילואים פעילים אחרים, במישרין או בעקיפין, ב-50% או יותר מכל סוג של אמצעי השליטה בעסק זעיר, קטן או בינוני". "אמצעי שליטה" לעניין זה – כהגדרתו בחוק הבנקאות (רישוי), התשמ"א-1981.

ההצעה אינה של חברת בת של עסק גדול. "עסק גדול" לעניין זה: "עוסק מורשה או מוסד כספי, כהגדרתם בחוק מס ערך מוסף, התשל"ו-1975, המעסיק יותר מ-100 עובדים או שמחזור העסקאות השנתי שלו עולה על 100 מיליון שקלים חדשים".

הכרה בנתונים של אישיות משפטית אחרת

במקרה בו בעברו של המציע התרחש שינוי ארגוני (לדוג' רכישת פעילות, התאגדות כחברה, רה-ארגון או איחוד של חברות בדרך אחרת), באופן בו הפעילות הרלוונטית בנושא המכרז השתלבה אצל המציע, יוכל המציע לבקש מהמזמין בכתב ובאופן מנומק לצרף לנתוניו את נתוני הגוף בו התקיימה הפעילות לפני השינוי הארגוני לשם הכרה בעמידה בתנאי סף מקצועי, אחד או יותר, או בתנאים אחרים הקבועים במכרז, או לשם קבלת ניקוד איכות והכל בכפוף לכללים הקבועים במכרז.

אם המציע מבקש שיכירו לו בנתונים של אישיות משפטית שונה לצורך עמידה בתנאי הסף מסוים או מספר תנאי סף או לשם קבלת ניקוד איכות, בהתאם לתנאים המפורטים במכרז, עליו לפרט את כלל הפרטים הרלוונטיים לצורך הכרה כאמור, ולצרף כל מסמך שיכול להוכיח על השינוי המבני, ועל השתלבות הפעילות הרלוונטית אצלו.

החלטה בדבר הכרה כאמור תהיה בכפוף לשיקול דעת המזמין.

בקשה לחיסיון

בהתאם למפורט בחלק א' למסמכי המכרז, להלן העמודים, הסעיפים או המסמכים הכלולים בהצעה אשר המציע מבקש למנוע ממציעים אחרים במכרז לעיין בהם (בטענה לחשיפת סוד מסחרי או סוד מקצועי או כל נימוק אחר המופיע בתקנה 21(ה) לתקנות חובת המכרזים):

מספר עמוד/סעיף	נושא הסעיף	נימוק למניעת החשיפה

אישור והתחייבות

בחתימתנו אנו מאשרים כי:

1. **קראנו את כל הוראות המכרז, על כל חלקיו, פרקיו, סעיפיו ונספחיו, וכן את המענה לשאלות ההבהרה שפורסם במסגרת המכרז ואת התיקונים שחלו במכרז בעקבותיו, ככל והיו, והצעתנו מוגשת בהתאם לכללי המכרז ועומדת בתנאים ובדרישות המפורטות במסמכי המכרז.**
2. **כל סעיף במכרז מובן ומקובל עלינו, והמציע יהיה מנוע ומושתק מלהעלות טענות כנגד תנאי המכרז מרגע הגשת הצעה זו.**
3. **הפרטים המופיעים בהצעה זו על נספחיה, הם אמת, וכי המציע מסוגל ומתכוון לעמוד בכל פרט מהצעתו ובהוראות המכרז.**

_____	_____	_____
תאריך	שם	חתימת מורשה החתימה
_____	_____	_____
תאריך	שם	חתימתה מורשה החתימה
_____	_____	_____
תאריך	שם	חתימת מורשה החתימה

רשימת נספחים לחלק ג' (חוברת ההצעה)

מס' נספח	שם נספח	תיאור נספח
נספח ג.1	**הצעת מחיר**	טופס הצעת מחיר מלא בהתאם להוראות המופיעות בנספח. לתשומת לב המציע – **יש להגיש טופס זה בנפרד מחוברת ההצעה**, על פי הנחיות סעיף 1.9.2.2 בפרק 1 – מנהלה.
נספח ג.2	**אישור "פקיד מורשה"**	על המציע לצרף אישור תקף מרואה חשבון או מיועץ מס על ניהול פנקסי חשבונות, ודיווח לרשויות המס כנדרש בחוק עסקאות גופים ציבוריים, או אישור על פטור מחובה זו. לצורך כך ניתן להשתמש בקישור הבא: https://www.misim.gov.il/gmishurim/frmInputMekabel.aspx?cur=0
נספח ג.3	**תצהיר עו"ד בדבר היעדר הרשעות בהתאם לחוק עסקאות גופים ציבוריים**	על המציע לצרף תצהיר עו"ד בהתאם למפורט בנספח.
נספח ג.4	**אישור רואה חשבון אודות נתונים מהדוחות הכספיים**	אישור רו"ח מבקר, בדבר היקף הפעילות של המציע, כנדרש בתנאי הסף, בהתאם לנוסח המופיע בנספח.
נספח ג.5	**תצהיר התחייבות להעמדת הון עצמי**	על המציע לצרף תצהיר עו"ד בהתאם למפורט בחוברת ההצעה.
נספח ג.6	**תצהיר התחייבות להקמת חברה להפעלת מערכת סליקה**	על המציע לצרף תצהיר עו"ד בהתאם למפורט בחוברת ההצעה.
נספח ג.7	**תצהיר מחברי צוות ניהול המוצע לעניין ניגוד עניינים**	על המציע לצרף תצהיר עו"ד בהתאם למפורט בחוברת ההצעה.
נספח ג.8	**אסמכתאות להוכחת עמידה בתנאי סף מקצועיים של הצוות הניהולי**	על המציע לצרף אסמכתאות בהתאם למפורט בחוברת ההצעה.
נספח ג.9	**מענה מפורט לדרישות האיכות והדרישות המקצועיות**	על פי המפורט בנספח.

נספח ג.1 – טופס הצעת המחיר למכרז 5/2025-מערכת סליקה פנסיונית מרכזית - הפעלה, תחזוקה ופיתוח

<u>לתשומת לב המציע - טופס זה יוגש בנפרד מחוברת ההצעה</u>

כללי

1. על המציע לעיין בכלל מסמכי המכרז טרם מילוי טופס הצעת המחיר.
2. מובהר, כי הכמויות המצוינות מטה ביחס ליחידות התמחור הן בבחינת הערכה בלבד לשם חישוב הצעה זוכה ולמזמין מסור שיקול הדעת המלא והבלעדי לקבוע את היקף השירותים שיוזמנו מהספק במסגרת ההתקשרות, וזאת לפי צרכיו בפועל של המזמין.

הצעת המחיר

1. הצעת המחיר תינתן אך ורק במספרים עגולים. ככל ומציע ינקוב במספר עשרוני, יהיה רשאי המזמין לתקן את הסכום הנקוב למספר העגול הקרוב ביותר כלפי מעלה.

אחוז ההנחה (0-30) מהמחירון שבנספח (כהגדרתו בסעיף 7.2 בפרק 7 מודל התמחור) עבור שירותי המערכת לביצוע פעולות:

__% (למילוי ע"י המציע)

חבות במע"מ – למילוי רק על ידי מציע שאינו חב במע"מ על פי דין במסגרת ההתקשרות

1. מציע שאינו חב בתשלום מע"מ במסגרת ביצוע התקשרות זו על פי דין, יצהיר על כך כלהלן (יש לסמן X במקום המתאים):

☐ המציע מצהיר כי במסגרת התקשרות לפי מכרז זה, אם יזכה, לא יהיה חייב בתשלום מע"מ וכי הוא פנה לרשות המיסים לקבלת אישור על כך.

המציע מתחייב כי:

1. לאחר שעיין במסמכי המכרז על כל נספחיו לרבות נוסח ההסכם ונספחיו, המציע מגיש בזאת הצעת מחיר למכרז.
2. מעבר למפורט בנספח זה לא יידרש על ידי המציע כל סכום נוסף אלא אם נכתב אחרת באופן מפורש במקום אחר במסמכי המכרז.
3. המציע אינו מתנה הצעה זו בשום תנאי.

---------- ----------

חותמת המציע
וחתימת מורשה חתימה של המציע

תאריך

נספח ג.3 – תצהיר בדבר היעדר הרשעות לפי חוק עסקאות גופים ציבוריים

4. אני הח"מ _____ ת"ז _____ לאחר שהוזהרתי כי עלי לומר את האמת וכי אהיה צפוי לעונשים הקבועים בחוק אם לא אעשה כן, מצהיר/ה בזה כדלקמן:

הנני נותן תצהיר זה בשם _____ שהוא המציע (להלן: "**המציע**") המבקש להתקשר עם עורך מכרז פומבי מס' ... למערכת סליקה פנסיונית מרכזית - הפעלה, תחזוקה ופיתוח. אני מצהיר/ה כי הנני מוסמך/ת לתת תצהיר זה בשם המציע.

בתצהירי זה, משמעותו של המונח "**בעל זיקה**" כהגדרתו בחוק עסקאות גופים ציבוריים התשל"ו-1976 (להלן: "**חוק עסקאות גופים ציבוריים**"). אני מאשר/ת כי הוסברה לי משמעותו של מונח זה וכי אני מבין/ה אותו.

משמעותו של המונח "**עבירה**" – עבירה לפי חוק עובדים זרים (איסור העסקה שלא כדין והבטחת תנאים הוגנים), התשנ"א-1991 או לפי חוק שכר מינימום התשמ"ז-1987, ולעניין עסקאות לקבלת שירות כהגדרתו בסעיף 2 לחוק להגברת האכיפה של דיני העבודה, התשע"ב-2011, גם עבירה על הוראות החיקוקים המנויות בתוספת השלישית לאותו חוק.

המציע הינו תאגיד הרשום בישראל. (סמן X במשבצת המתאימה):

☐ המציע ובעל זיקה אליו לא הורשעו ביותר משתי עבירות עד למועד האחרון להגשת ההצעות (להלן: "מועד להגשה") למכרז מערכת סליקה פנסיונית מרכזית - הפעלה, תחזוקה ופיתוח , מספר 5/2025.

☐ המציע או בעל זיקה אליו הורשעו בפסק דין ביותר משתי עבירות וחלפה שנה אחת לפחות ממועד ההרשעה האחרונה ועד למועד ההגשה.

☐ המציע או בעל זיקה אליו הורשעו בפסק דין ביותר משתי עבירות ולא חלפה שנה אחת לפחות ממועד ההרשעה האחרונה ועד למועד ההגשה.

זה שמי, להלן חתימתי ותוכן תצהירי דלעיל אמת.

_____	_____	_____
תאריך	שם	חתימה וחותמת

<u>אישור עורך הדין</u>

אני הח"מ _____, עו"ד מאשר/ת כי ביום _____ הופיע/ה בפני במשרדי אשר ברחוב _____ בישוב/עיר _____ מר/גב' _____ שזיהה/תה עצמו/ה על ידי ת"ז _____ /המוכר/ת לי באופן אישי, ואחרי שהזהרתיו/ה כי עליו/ה להצהיר אמת וכי יהיה/תהיה צפוי/ה לעונשים הקבועים בחוק אם לא יעשה/תעשה כן, חתם/ה בפני על התצהיר דלעיל.

_____	_____	_____
תאריך	מספר רישיון	חתימה וחותמת

נספח ג.4 – אישור רו"ח אודות נתונים מהדוחות הכספיים

תאריך: _____

לכבוד
חברת _____

הנדון: **אישור על מחזור כספי (או כל מידע אחר המופיע בדוחות הכספיים[6]) לתקופה 2022 עד 2024**

לבקשתכם וכרואי החשבון של _____ (להלן: "**המציע**") הרינו לאשר כדלקמן:

1. הננו משמשים כרואי החשבון של המציע משנת _____.
2. יש למחוק את המיותר מבין סעיפים 2.1 ו-2.2:

הדוחות הכספיים המבוקרים / סקורים [מחק את המיותר] של המציע ליום / לימים _____ בוקרו / נסקרו (בהתאמה) על ידי משרדנו. דוח רואי החשבון המבקרים נחתם ביום / בימים _____.

הדוחות הכספיים המבוקרים / סקורים [מחק את המיותר] של המציע ליום / ימים _____ בוקרו / נסקרו (בהתאמה) על ידי רואי חשבון אחרים. דוח רואי החשבון המבקרים האחרים נחתם/ו ביום / בימים _____.

3. יש למחוק את המיותר מבין סעיפים 3.1 ו-3.2:

דוח רואי החשבון המבקרים ליום _____ אינו כולל הסתייגות ו/או הפניית תשומת הלב להערת עסק חי, או כל סטייה אחרת מהנוסח האחיד.

דוח רואי החשבון המבקרים ליום _____ כולל סטייה מהנוסח האחיד, אולם אין לסטייה זו השלכה על המידע המפורט בסעיף 4 להלן.

4. בהתאם לדוחות הכספיים האמורים לעיל, המחזור הכספי של חברתכם לתקופה 2022-2024 (1) הינו בממוצע גבוה מ / שווה ל 25,000,000.

בכבוד רב,

_____
רואי חשבון

הערות:

- נוסח דיווח זה נקבע על ידי ועדה משותפת של מינהל הרכש הממשלתי ושל לשכת רואי החשבון בישראל – בדצמבר 2020.
  יודפס על נייר לוגו של משרד הרו"ח.

[6] אישור רואה חשבון וחוות דעת רואה חשבון הן אסמכתאות חלופיות. במקרים בהם מדובר בנתון חשבונאי המופיע בדוחות הכספיים המבוקרים / בדוחות כספיים סקורים בדבר מידע כספי לתקופות ביניים, תוגש אסמכתה מסוג "אישור", אחרת יוגש דוח מיוחד במתכונת של "חוות דעת". לגבי נתונים חשבונאים שלא מופיעים בדוחות הכספיים, רואה החשבון ייתן דוח מיוחד רק בנושאים שהם בתחום עיסוקו המקצועי. כמו כן, במקרה שהליך הביקורת / סקירה על הדוח הכספי טרם הסתיים, רואה החשבון יכול לתת דוח מיוחד אם נקט בנוהלי ביקורת / בנוהלי סקירה להנחת דעתו בדבר נאותותם ואימותם של הנתונים עליהם הוא נותן את הדוח. אולם, אם לדעתו של רואה החשבון השלמת הביקורת / הסקירה עלולה להביא לשינוי בנתונים שבצהרת הלקוח, עליו לציין נסיבות הימנעותו בדוח המיוחד.

נספח ג.9 – מענה המציע

להלן יוצגו דרישות מענה האיכות אשר על המציעים לפרט במסגרת הצעתם. המציעים נדרשים להציג את המענה בהתאם למספר הסעיף בנספח זה. כלל הדרישות מופיעות בחלק ב' של המכרז, ומחולקות לפי פרקים, בהתאם לפירוט שלהלן:

מענה לפרק 1 – מנהלה

1.1. המציע יצרף מענה מפורט לדרישות בסעיף 1.7.2.3 – תכנית עסקית, ויתייחס לכלל מרכיביו (דו"ח רווח והפסד, תזרים מזומנים צפוי, והערכה לגבי היקפי כוח אדם) של הסעיף. על המציע לצרף טבלה/קובץ אקסל עם התכנית העסקית בפילוח שנתי וכן הסבר לגבי הנחות העבודה המרכזיות בבסיס התכנית.

1.2. המציע יענה לדרישות סעיף 1.7.2.1 – ניסיון מקצועי של המציע והצוות הניהולי, על פי הטבלה שלהלן:

ניסיון מקצועי		
קריטריון	**רכיב**	**מענה המציע**
ניסיון המציע	**ניסיון במתן שירותי הפעלה של מערכות מידע מורכבות בתחום הפנסיוני ו\או בתחום פיננסיים\שוק ההון** (מעל 10 שנים- ניקוד מלא, 8-10 שנים - 5 נקודות, 7-4 שנים - 3 נקודות, ומטה- ציון 0)	המציע יציין את מספר שנות הניסיון בכל מערכת ויפרט אודות המערכות הרלוונטיות (שם ותיאור המערכת, טווח השנים, תפקיד המציע)
	ניסיון בהפעלת מערכת מידע המאפשרת לקיים פעולות בין גופים מוסדיים\פיננסיים (מעל 5 גופים מוסדיים/פיננסיים- ציון מלא, אחרת- ציון 0)	המציע יציין את שם ותיאור המערכת ויפרט את שמות הגופים, את סווגם (מוסדי/פיננסי) ואת תפקיד המציע *ניתן לפרט אודות יותר ממערכת אחת, אך לא יינתן ניקוד גבוה מהניקוד המקסימלי
	ניסיון ביישום תהליכים בפרוטוקולים של API (ניסיון של מעל 3 שנים- ציון מלא, ניסיון של מתחת ל-1 שנה- ציון 0, בין לבין- יחסי)	המציע יפרט את שם ותיאור המערכת, טווח השנים בו ביצע את התהליך ואת סוגי פרוטוקולים של API שיישם *ניתן לפרט אודות יותר ממערכת אחת, אך לא יינתן ניקוד גבוה מהניקוד המקסימלי
	ניסיון בהקמה ותפעול פורטלים אינטרנטיים (ניסיון של מעל 3 שנים- ציון מלא, ניסיון של מתחת ל-1 שנה- ציון 0, בין לבין- יחסי)	המציע יפרט רשימת פורטלי אינטרנט שהקים ותפעל ויפרט אודות הפורטל (שם ותיאור, טווח השנים)
	ניסיון בהפעלת מערך שירות ותמיכה (מעל 3 שנות ניסיון- ציון מלא, אחרת- ציון 0)	המציע אודות מערך שירות ותמיכה שהפעיל (שם המערכת ותיאור, טווח השנים)

ניסיון מקצועי		
קריטריון	**רכיב**	**מענה המציע**
ניסיון אנשי המקצוע	**מנכ"ל החברה המוצע:** (תנאי סף - 5 שנות ניסיון ניהולי של לפחות 20 עובדים) ניסיון כמנכ"ל ו/או בניהול יחידה עסקית בת 50 עובדים לפחות –, כל שנה מעל תנאי הסף מקנה 2.5 נקודות עד הניקוד המקסימלי	המציע יצרף רשימת חברות בהן שימש כמנכ"ל או ניהל יחידה עסקית בת 50 עובדים לפחות (שם החברה, מספר עובדים, תפקיד בחברה, טווח שנים)
	מנהל הפרויקט: (5 שנות ניסיון ניהולי של לפחות 20 עובדים ו-5 שנים ניסיון בפרויקטים טכנולוגים - תנאי סף) ניסיון מקצועי בפרויקטים טכנולוגים בתחומי הפיננסיים - מעל 10 שנים - ציון מלא, 8-10 שנים - 10 נקודות,6-8 שנים - ציון של 5 נקודות,	המציע יצרף רשימת פרויקטים טכנולוגיים של מנהל הפרויקט בתחומי הפיננסיים (שם החברה, תיאור הפרויקט, טווח שנים)
	מנהל פיתוח טכנולוגי: (תנאי סף - 5 שנות ניסיון בפיתוח) בעל ניסיון מקצועי של למעלה מ- 15 שנים - ציון מלא, 13-15 שנות ניסיון - 10 נקודות, 11-12 שנות ניסיון - 5 נקודות	המציע יצרף רשימת מקומות תעסוקה של מנהל הפיתוח (שם החברה, תפקיד בחברה, טווח שנים)
	ממונה אבטחת מידע (תנאי סף - 5 שנות ניסיון) בעל ניסיון מקצועי של למעלה מ-10 שנים - ציון מלא, 8-10 שנות ניסיון - 10 נקודות, 6-8 שנות ניסיון - 5 נקודות	מציע יצרף רשימת מקומות תעסוקה של ממונה אבטחת מידע (שם החברה, תפקיד בחברה, טווח שנים)

מענה לפרק 2 – מפרט השירותים הנדרשים

2.1. המציע יפרט אודות פורטל האינטרנט המוצע על ידו, אשר הדרישות בגינו מפורטות בהרחבה בסעיף 2.5.6 לעיל.

2.2. המציע יפרט אודות מערך השירות המוצע על ידו, אשר הדרישות בגינו מפורטות בהרחבה בסעיף 2.5.8 לעיל.

מענה לפרקים 3-4 – (טכנולוגיה, אבטחת מידע, הגנת הפרטיות, והמשכיות עסקית)

3.1. ארכיטקטורת מערכות מידע מוצעת –

3.1.1. המציע יפרט את הטכנולוגיות, מוצרי התכנה (לרבות מערכות הפעלה ושפות פיתוח) ומתודולוגית הפיתוח אשר ישמשו אותו כחלק מהפתרון המוצע על ידו בהתאם לדרישות המפורטות במכרז זה. המציע יתאר את המגבלות הטכנולוגיות הקיימות של המערכת המוצעת על ידו, במידה שישנן כאלה.

3.1.2. המציע יפרט את כל הפיתוחים הנדרשים, מעבר לתוכנה או מוצרי מדף קיימים הניתנים לשימוש ללא צורך בהתאמות כלשהן, לצורך מתן השירותים המנויים בפרק 2 למכרז זה.

3.1.3. המציע יתאר את ארכיטקטורת הפתרון המוצע עבור מערכת הסליקה ויצרף תרשים מלווה, תוך התייחסות לפרטים הבאים לפחות:

א. שכבות הפתרון בהתייחס לממשק המשתמש, לשכבת האינטגרציה והגישה לנתונים ולשכבת הנתונים, מודולריות וניידות בין סביבות;

ב. תיאור ארכיטקטורת הפתרון בהתייחס לאתר הראשי, אתר משני (DR) ועותקי מידע;

ג. מידת התמיכה ואופן התמיכה של הארכיטקטורה ביכולות גידול והרחבה של שירותי המערכת ושל זמינות השירותים. יש לציין את מגבלות הארכיטקטורה.

3.1.4. המציע יפרט את מאפייני חדר המחשב אשר ישמש את מערכת הסליקה, בהתייחס לנושאים הבאים לפחות ותוך התייחסות לאפשרויות גידול עתידיות:

א. תיאור כללי - תקן חדר המחשב (Tier) בו מתחייב המציע לעמוד, גודל החדר המתוכנן והאם קיים או שייבנה במיוחד עבור המערכת, סוג הרצפה, סטנדרט הכבילה של החשמל והתקשורת פריסת הכבילה בתמציתיות, ואופן אחסון השרתים (ארונות, מדפים וכדומה);

ב. חשמל - מקורות מתח (חברת חשמל, UPS, גנרטור) ותיאור של תצורת החשמל בתוך חדר המחשב (לרבות ארונות חשמל, שקעים וחיבורים לארונות המחשוב);

ג. אקלים - מזגנים, בקרות ומערכות גילוי וכיבוי;

ד. אבטחה - רכיבי אבטחה (כגון מצלמות ובקרי כניסה) ומידור פיזי, בהתאם לאמור בסעיף 3.4.5 בפרק 3 לעיל.

ה. המציע יענה על סעיף זה בהתאמות הנדרשות בבחירת ארכיטקטורה המשלבת ענן.

3.1.5. המציע נדרש לפרט במסגרת הצעתו את תצורת החומרה המרכזית אשר תשמש את מערכת הסליקה. יש להתייחס לכל הנושאים הבאים לפחות:

3.1.6. מציע הבוחר פתרון On-Premise:

א. שרתים - תיאור כללי של סוגי השרתים המתוכננים.

ב. אחסון הנתונים - יש לציין לגבי כל סוג מערך את הפרטים הבאים: יצרן, דגם, סוג החיבור (אופטי או נחושת), האם יחובר לרשת ייעודית רשת ה-LAN או לשרתים, ונפח האחסון;

ג. רשת LAN - יש לפרט את תצורת רשת ה-LAN ומאפיינים מינימליים של הציוד, לרבות מתגים מרכזיים ומשניים וציוד אחר נדרש, יצרן ודגם.

3.1.7. מציע הבוחר בפתרון המשלב גם ארכיטקטורה ותצורת תשתית בענן

א. משאבי מחשוב (Compute)

- סוג השירות (IaaS/PaaS/SaaS) ומיקומי האזורים (תחת המגבלות שהוגדרו במכרז) בהם תותקן המערכת.
- מאפייני משאבי העיבוד, vCPU: זיכרון, האצה ייעודית) כגון GPU או האצת הצפנה (במידת הצורך.
- מנגנוני זמינות גבוהה (High Availability) והרחבת משאבים אוטומטית (Auto Scaling).
- רמות ה־ SLA המובטחות וזמני תגובה לתקלות.

ב. אחסון נתונים

- סוגי האחסון (בלוק/אובייקטים/קבצים) ומאפייני הביצועים (IOPS/Throughput).
- הצפנה במנוחה ובתעבורה, לרבות ניהול מפתחות (KMS/HSM) .
- נפחי האחסון המתוכננים ואפשרויות ההרחבה.

ג. רשת וירטואלית

- תצורת הרשת הווירטואלית, (VPC/Virtual Network) חלוקת תתי רשתות (Subnets) והפרדת סביבות.
- רכיבי אבטחת הרשת(Security Groups, NACLs, WAF)
- חיבורים מאובטחים בין רכיבי המערכת ובין המערכת לגורמי חוץ, (VPN Private Link, Direct Connect).

3.1.8. המציע יציין את סוג בסיס הנתונים (דגם וגרסה) בו תומך הפתרון המוצע על ידו. המציע יתאר את מבנה בסיס הנתונים ואת אופן ארגון הנתונים בבסיס הנתונים, לרבות אופן התמיכה של מבנה זה בדרישות אבטחת המידע כמפורט בפרק 4. יש להתייחס לנושאים הבאים לפחות:

א. יכולות המערכת המוצעת בהתאם להערכות יצרן בסיס הנתונים וכן את יכולות הגידול של המערכת מבחינת שטחי אחסון;

ב. יכולות המערכת המוצעת באחסון שדות מידע גדולים כגון קובצי תמונות או קובצי ייפוי כוח סרוקים, ואופן הניהול והעבודה עם מידע מסוג זה;

ג. אפשרויות ההצפנה של נתונים בתוך בסיס הנתונים בחלוקה לכלל המידע, רשומות ספציפיות, שדות ספציפיים וכו'.

3.2. רשת, תקשורת, פרוטוקולים אינטגרציה וממשקים

3.2.1. המציע יפרט את תצורת תשתית התקשורת, דרך הצפנתה ורכיביה באתר המציע, לרבות אופן התמיכה בדרישות אבטחת המידע כמפורט בפרק 4. המציע יפרט את הטכנולוגיות המוצעות עבור תקשורת ציבורית ותקשורת פרטית ומאפייני כל אחד מסוגי תקשורת אלה.

3.2.2. המציע יפרט את כל ממשקי התקשורת החיצוניים הנדרשים למערכת הסליקה לרבות סוג ההצפנה, סוג הקווים ושרידותם, וכן ציוד הקצה הנדרש.

3.3. חווית משתמש

3.3.1. המציע יתאר את הממשק המוצע על ידו לרבות סקירה כללית של ממשק המשתמש (**UI**) והחוויה (**UX**) ויציג דוגמאות למסכים/ **MOCKUPS**, יציג את עקרונות העיצוב והסטנדרטים שבהם הוא משתמש, התאמה למכשירים ולסביבות עבודה ומתודולוגיה לבדיקת חווית המשתמש.

3.4. אוטומציה ניהול תפעולי והמשכיות עסקית

3.4.1. המציע יפרט בהצעתו את האמצעים שינקוט ואשר עומדים לרשותו לצורך הבטחת שרידות מערכת הסליקה ורציפות אספקת השירותים והנתונים בהתאם לאמור בסעיף 6.3.1 בפרק 6 לעיל, לרבות תיאור תמציתי של תצורת היתירות ואתר הגיבוי. המציע יתייחס לנושאים הבאים לפחות:

א. נהלי המידע והנתונים, וכן תכנית להמשכיות השירות הניתן באמצעות מערכת הסליקה במצבי חירום, לרבות לעניין סליקת כספים באמצעות מערכת זה"ב, בחלוקה לפי סוגי התקלות האפשריים;

ב. תהליכי גיבוי באתר מערכת הסליקה, לרבות גיבויים "חמים" וכן אבטחת אמינות ועקביות בגיבויים מסוג זה, וכן גיבויים תקופתיים ותדירותם. יש לפרט את שיטת הגיבוי המוצעת;

ג. תהליכי הליבה שיפעלו באתר הגיבוי המרוחק, תוך התייחסות לשירותים השונים שיסופקו על ידי מערכת הסליקה ולשלבי ההפעלה שלהם. הפירוט יכלול התייחסות לכל תהליך גיבוי השרתים (חומרה, תוכנה ונתונים) באתר המרוחק (**DRP**), לרבות תדירות הגיבוי, המרחק בין אתר הגיבוי המרוחק (**DRP**) לאתרים אחרים של המערכת, עדכניות הנתונים (**RPO**) ומהירות העלאת הנתונים במערכות (**RTO**).

ד. מציע הבוחר פתרון המשלב ארכיטקטורת ענן, יענה לסעיף זה עם השינויים הנדרשים.

3.5. אבטחת מידע, הגנת הפרטיות וניטור

3.5.1. המציע יפרט את הפתרון הטכנולוגי ליישום דרישות אבטחת מידע והגנת סייבר המתוארות כמפורט במכרז לרבות:

א. שיטות ומנגנוני אימות מתקדמים - פירוט שיטות האימות המתוכננות (למשל MFA , זיהוי ביומטרי, OTP) והאופן בו ישולבו במערכת.

ב. תהליך זיהוי מרחוק ללקוחות - תיאור הפתרון המוצע לזיהוי ואימות לקוחות מרחוק.

ג. מודל ניהול זהויות והרשאות- הצגת ארכיטקטורת מנגנוני בקרת גישה ותמיכה ב־ SSO ואינטגרציה עם מערכות קיימות.

ד. מנגנוני ניטור, איתור חריגות וניהול אירועי אבטחת מידע - הפתרון והכלים המוצעים לניטור פעולות משתמשים, זיהוי התנהגות חריגה והפעלת התראות או תגובות אוטומטיות לרבות כלי ה-SIEM ואמצעי ה-SOC המוצעים.

ה. שרידות וזמינות תהליכי הזיהוי - תיאור אמצעי ה־High Availability, מנגנוני DR ופתרונות להבטחת זמינות השירות בתרחישי אסון.

ו. ניהול מחזור חיי זהויות- פירוט תהליכי יצירה, עדכון, השעיה ומחיקה של משתמשים, כולל בקרות למניעת הרשאות עודפות.

ז. הגנה מפני הונאות והתחזות- מנגנונים טכנולוגיים ופרוצדורליים לזיהוי ניסיונות התחזות (Phishing), גניבת זהות או שימוש לא מורשה Intelligence.

3.5.2. המציע יפרט את אופן הניטור והבקרה אחר פעילות השרתים, תוך התייחסות לנושאים הבאים לפחות:

א. מתן התראות על התקרבות לבעיה ועל בעיה;

ב. מבנה ההתראות (לוגים);

ג. הגדרת המציע לעומס לא סביר על ה-CPU;

ד. הקשר בין מערך הבקרה למערכות השונות;

3.5.3. המציע יפרט את מעגלי האבטחה הפיזית המוצעים, בהתאם לאמור בסעיף 4.15 בפרק 4 לעיל.

3.6. תהליכי זיהוי, אימות וניהול משתמשים

3.6.1. המציע יפרט כיצד יבצע התאמות למערכות חומרה ותוכנה המשמשות את משתמשי מערכת הסליקה ולמערכות חומרה ותוכנה סטנדרטיות הנדרשות לצורך העברת מידע באמצעות טכנולוגיית **API** כאמור בסעיף 2.5.1.1., המציע יפרט מהן הפעולות שהמשתמשים ידרשו לבצע לשם חיבור למערכת.

3.6.2. המציע יתאר את האופן שבו הפתרון המוצע יישם את שיטות החובה לזיהוי ראשוני של לקוח כמפורט בסעיף 4.20, לרבות אופן אימות פרטי הזיהוי מול גורמים חיצוניים, ויפרט לגבי שיטות נוספות לזיהוי לקוח, ככל שהפתרון המוצע על ידו תומך בהן. יודגש כי לא יינתן ניקוד נוסף בגין שיטות נוספות כאמור.

3.6.3. המציע יפרט את ארכיטקטורת התשתית הטכנולוגית להנפקת סרטיפיקטים כמפורט בסעיף 2.5.2 ויפרט את התהליכים והדרישות ממשתמשי המערכת ותהליכי הנפקה וחידוש לצורך תפעול תשתית זו.

3.6.4. המציע יפרט את תהליך הזיהוי השוטף של לקוח, שלאחר ביצוע זיהוי ראשוני בהתאם לאמור בסעיף 4.20, וכן את תהליך לעדכון מזהים של הלקוח ו/או שחזור מזהים.

3.6.5. המציע יפרט את מגוון הפתרונות המוצעים על ידו לנושא זיהוי לקוח ומשתמש.

3.6.6. המציע יפרט את מדיניות ניהול הסיסמאות של מערכת הסליקה, ויתאר את כל כלי המדיניות שהמערכת המוצעת מאפשרת בהתייחס לכל הנושאים המפורטים בסעיף 4.18.1.8, לרבות תהליך הקצאת סיסמה חדשה למשתמש/לקוח שהושעה משימוש במערכת או שסיסמתו נחסמה.

3.7. להלן רשימת המסמכים אשר יש לצרף למענה לסעיף 3 לעיל, על המציע לסמן V לאישור צירוף כלל המסמכים על ידו:

סעיף בנספח:	מסמך נדרש:	צורף:
3.1.3	תרשים ארכיטקטורת הפתרון למערכת הסליקה (שכבות, אתר ראשי/DR/עותקי מידע, סקיילביליות ומגבלות).	
3.1.6 ג'	תרשים רשת LAN (מתגים מרכזיים/משניים, יצרן ודגם).	
3.1.7 ג'	תרשים רשת ענן (כאשר רלוונטי) – VPC/תתי-רשתות/הפרדת סביבות, רכיבי אבטחה (SG/NACL/WAF), חיבורים מאובטחים (VPN/Private Link/Direct Connect).	
3.2.1	תרשים תצורת תשתיות תקשורת ואבטחתן (ציבורית/פרטית, טכנולוגיות, התאמה לדרישות אבטחה).	
3.6.2	נוהל זיהוי ראשוני של לקוח ואימות מול גורמי חוץ (לפי 5.10.4) + פירוט שיטות נוספות (אם נתמכות).	
3.6.3	תרשים ארכיטקטורת PKI והנפקת סרטיפיקטים – תהליכי הנפקה/חידוש ודרישות ממשתמשי המערכת.	

חלק ד' –
הסכם ההתקשרות

הסכם התקשרות

נחתם ביום ___ בחודש _____ בשנת _____

ב י ן

רשות שוק ההון, ביטוח וחיסכון
(להלן: "המזמין")

<u>מצד אחד</u>

ל ב י ן

_____

מכתובת _____

(להלן: "**הספק**")

<u>מצד שני</u>

הואיל ובהתאם להוראות חוק הפיקוח על שירותים פיננסיים (ייעוץ שיווק ומערכת סליקה פנסיוניים), התשס"ה-2005, (להלן: "**חוק הייעוץ הפנסיוני**") החליט הממונה על שוק ההון, ביטוח וחיסכון (להלן: "**הממונה**") לבחור בדרך של מכרז חברה להקמתה ותפעולה של מערכת סליקה פנסיונית מרכזית (להלן: "**המערכת**" או "**מערכת הסליקה**" או "**מערכת הסליקה הפנסיונית**");

והואיל ולצורך בחירת החברה שתקים ותתפעל את מערכת הסליקה, פרסם המזמין את מכרז פומבי מס' 5/2025 למערכת סליקה פנסיונית מרכזית - הפעלה, תחזוקה ופיתוח (להלן: "**המכרז**");

והואיל והספק הגיש הצעה למכרז, כדי לספק את המוצרים והשירותים המבוקשים בהתאם לאמור במכרז, בהצעתו ובהסכם זה (להלן: "**ההסכם**");

והואיל ובכפוף לחתימתו על ההסכם וקיום הדרישות המפורטות במכרז, ועדת המכרזים של המזמין בחרה בספק כזוכה במכרז;

לפיכך הוצהר, הותנה והוסכם בין הצדדים כדלקמן:

1. כללי

1.1 להסכם זה מצורפים הנספחים המפורטים להלן:

1.1.1 **נספח א'** – המכרז על כלל נספחיו;

1.1.2 **נספח ב'** – חוברת ההצעה של הספק במכרז (חלק ג' למכרז);

1.1.3 **נספח ג'** – ערבות ביצוע;

1.1.4 **נספח ד'** – ביטוח;

1.1.5 **נספח ה'** – נספח סודיות והיעדר ניגוד עניינים;

1.1.6 **נספח ה1-** תצהיר העדר ניגוד עניינים עבור נושאי משרה במציע וביחידי המציע;

1.1.7 **נספח ו'** – נספח סייבר ואבטחת מידע;

1.2 בנוסף מסמכי המכרז והבהרות למכרז שפורסמו באתר מינהל הרכש הממשלתי (בהתאם לנוסח המעודכן ביותר המופיע שם), ייחשבו גם הם כמצורפים להסכם זה.

1.3 המבוא והנספחים להסכם מהווים חלק בלתי נפרד ממנו.

1.4 בהסכם תהיה למונחים המשמעות המופיעה במכרז. פרשנות ההסכם על נספחיו תיעשה באופן המקיים את דרישות המכרז המפורשות והמשתמעות ואת תכלית המכרז של אספקת המוצרים והשירותים למזמין באופן מיטבי.

2. תקופת ההתקשרות

2.1 תקופת ההתקשרות תארך 96 חודשים ממועד החתימה על הסכם זה **("תקופת ההתקשרות")**, כאשר למזמין הזכות להאריך את תקופת ההתקשרות בתקופות נוספות, ועד ל - 96 חודשים נוספים, על פי שיקול דעתו הבלעדי.

2.2 <u>תקופת התארגנות</u> – תקופה של עד 2 חודשים הראשונים מתוך תקופת ההתקשרות תהווה תקופת התארגנות. בתקופה זו יבצע הספק את כל הפעולות הנדרשות ממנו כהיערכות לשם התחלת מתן השירותים. המזמין רשאי להאריך את משך תקופת ההתארגנות בהתאם לשיקול דעתו הבלעדי.

2.3 <u>תקופת מעבר</u> – תקופה של 180 הימים האחרונים של ההתקשרות, תהווה תקופת מעבר. בתקופה זו יהיה רשאי המזמין להתקשר עם ספקים אחרים בנושא ההתקשרות והיקף השירותים אשר יירכשו מהספק בתקופה זו יפחת לפי צרכי המזמין. כמו כן, בתקופה זו הספק ישתף פעולה עם המזמין ועם הספק החדש שייבחר על ידי המזמין בנושא ההתקשרות, לביצוע כל הפעולות הנדרשות לשם העברת ביצוע נושא ההתקשרות לספק החדש.

2.4 כל שינוי בתקופת ההתקשרות וכן מימוש הזכות להאריך את ההתקשרות, יכנס לתוקפו רק עם חתימה של מורשיי החתימה מטעם המזמין.

3. התחייבויות והצהרות הספק

הספק מצהיר ומתחייב כי –

3.1 אין מניעה לפי כל דין להתקשרותו בהסכם.

3.2 הוא עומד בכל דרישות הדין הרלוונטיות לאספקת המוצרים והשירותים בהתאם להסכם.

3.3 ברשותו הניסיון, המיומנות, הידע, הכלים, המלאי וכוח האדם הדרושים למילוי חובותיו בהתאם לתנאי ההתקשרות.

3.4 הוא בחן היטב את הוראות המכרז ודרישות המכרז ובכלל זה הוראות הדין הרלבנטיות וכן את מבנה שוק החיסכון הפנסיוני בישראל, וכי לא תהיה לו כל תביעה או טענה כלפי המכרז או המזמין בשל אי-גילוי מספיק או בשל גילוי חסר, או בשל טעות מכל סוג שהוא.

3.5 ידוע לו כי מערכת הסליקה הפנסיונית הינה מרכיב אסטרטגי וקריטי לפעילות תקינה של שוק חיסכון פנסיוני בישראל, וכן כי העמידה בלוח הזמנים להקמת מערכת הסליקה והספקת שירותי החובה במסגרתו הינם חיוניים ליישום הוראות החוק והשגת המטרות הקבועות בו.

3.6 כל המידע שנמסר על ידו במסגרת הצעתו במכרז ובמסגרת הליכי המכרז הינו מלא, מדויק ובלתי מטעה. וידוע לו כי כל המידע שיתקבל אצלו במסגרת ביצוע הסכם זה הינו מידע סודי.

3.7 המידע והתוכנות בהם יעשה שימוש הם בבעלותו, או כי ברשותו חוזה תקף לשימוש בהם, וכי לא הפר זכויות יוצרים, פטנט, סוד מסחרי או זכות קניינית אחרת של כל צד ג', בהתאם לתנאי במכרז

3.8 הוא יספק את הנדרש ממנו על פי דרישות ההתקשרות, לשביעות רצון המזמין.

3.9 הוא ישתף פעולה עם המזמין וכל נציג מטעמו בכל הקשור למילוי התחייבויותיו על פי הסכם זה, בכלל זה הוא ישתף פעולה באופן מלא עם הוראות קב"ט המזמין.

4. סודיות

4.1 הספק מתחייב כי הוא ומי מטעמו ישמרו את המידע שהתקבל אצלם במהלך ביצוע חובותיהם על פי ההסכם והמכרז בסודיות מוחלטת, במהלך תקופת ההתקשרות ולאחריה, ולא יעשו בו כל שימוש למעט לצורך ביצוע חובותיהם בהתאם למכרז ולהסכם.

4.2 הספק מצהיר שידוע לו כי כל מידע שיימסר לו בקשר עם מתן השירותים הוא סודי, אין להעבירו לכל גורם שהוא ואין לפרסמו, אלא אם ניתן לכך אישור מראש ובכתב של המזמין.

4.3 הספק מתחייב לשמור בסוד, ולא לגלות את המידע או את הסודות המקצועיים והמסחריים שיגיעו לידיו במהלך ביצוע הסכם זה, לבד מהעברת המידע למזמין, לממונה, למקבלי השירות או לגורם אחר בהתאם להוראות הסכם זה.

4.4 הספק מתחייב שלא לעשות שימוש, לטובת עצמו או לטובת צד ג', בכל מידע שיגיע לידיו במהלך ביצוע הסכם זה, מעבר למה שהותר לו במפורש על פי ההסכם.

4.5 הספק מתחייב לפעול לאבטחת המידע שהגיע לידיו תוך קביעת נהלי גישה למידע לאיסוף, לסימון, לאימות ולעיבוד הנתונים וכמפורט גם במפרט המכרז; הספק מצהיר ומאשר כי הוא מכיר את הוראות התקנות והוראות חוק הגנת הפרטיות, התשמ"א-1981 ותקנותיו, וכי יפעל כמתחייב מחוק ותקנות אלה ומכל דין אחר הנוגע לשמירת סודיות המידע שיימצא ברשותו, לפי העניין.

4.6 הספק מתחייב לחתום ולהחתים את כל עובדיו וכל מי הפועל מטעמו, לרבות אנשי הצוות וספקי משנה, על הצהרת סודיות בנוסח המפורט בנספח להסכם זה. הספק יפסיק מידית את עבודתו של עובד שהפר את חובת השמירה על הסודיות לפי הסכם זה.

4.7 הספק מצהיר כי ידוע לו כי הפרת הוראות סעיף זה מהווה עבירה לפי סעיף 117 לחוק העונשין, התשל"ז-1979 והפרה של סעיף 31טו לחוק הייעוץ הפנסיוני, והוא יכלול בהצהרות הסודיות לפי סעיף קטן (ד) אזכור של הסעיפים האמורים.

4.8 לעניין התחייבות זו לסודיות מובהר כי הגדרת "מידע" או "מידע סודי" לא תכלול:

4.8.1 מידע שהוא נחלת הכלל או שיהפוך לנחלת הכלל שלא עקב הפרת התחייבות זו.

4.8.2 מידע שהיה בידי הספק טרם החתימה על ההסכם.

5. אבטחת מידע והגנות סייבר

5.1 הספק יהיה אחראי לאבטחת מידע של המזמין המגיע לרשותו בעת ביצוע ההסכם באמצעי אבטחה נאותים בהתאם למפורט ב**נספח ו' – נספח סייבר ואבטחת מידע**. הספק יציג למזמין, אם יידרש, את האמצעים בהם הוא נוקט לשם אבטחת המידע, ויפעל בהתאם לדרישות מאת המזמין לתיקון כל ליקוי או פרצה באבטחת המידע והגנות הסייבר.

6. ניגוד עניינים בביצוע ההסכם

6.1 הספק מתחייב כי אין בביצוע ההסכם כדי ליצור ניגוד עניינים כלשהו, בין במישרין ובין בעקיפין, בינו לבין המזמין.

6.2 בכל מקרה שיווצר חשש כלשהו לניגוד עניינים בין הספק לבין המזמין יודיע הספק על כך למזמין, ללא כל שיהוי ויפעל באופן מידי להסרת ניגוד העניינים. בנוסף, במקרה כאמור, יודיע המזמין לספק אודות אמצעים נוספים או מיוחדים הנדרשים ממנו לצורך הסרת ניגוד העניינים, והספק יבצע את הנדרש ממנו בהקדם.

6.3 הספק מתחייב להחתים כל אחד מעובדיו ומי מטעמו שיועסקו על ידו לצורך ביצוע ההסכם על הצהרת הסודיות והיעדר ניגוד עניינים בנוסח המופיע כ**נספח ה'** להסכם זה.

7. קניין רוחני וזכויות יוצרים

7.1 הספק הוא בעל הזכויות הנדרשות לצורך אספקת השירותים והשימוש בהם על-ידי המזמין ("**זכויות הקניין הרוחני**"). במקרה שהספק אינו בעל מלוא זכויות הקניין הרוחני, הוא מצהיר כי בעלי זכויות הקניין הרוחני נתנו בידיו את כל האישורים, הרשאות השימוש והרישיונות הדרושים לפי כל דין לצורך אספקת השירותים והשימוש בהם על-ידי המזמין, בהתאם לתנאי הסכם זה.

7.2 בעת ביצוע ההתקשרות, הספק לא יעשה שימוש בתוכנות מחשוב, תמונות, מסמכים וכיוצא באלה, שהוא אינו מורשה על-פי דין לעשות בהם שימוש.

7.3 תוצר שהוכן על ידי הספק במהלך תקופת ההתקשרות עבור המזמין ובכלל זאת, נתונים, מצגות, מסמכים, סיכומי פגישות, תמונות, תכנים וכיוצא בזה ("תוצרי העבודה"), הוא קניינו הבלעדי של המזמין והוא יוכל לעשות בו כל שימוש שירצה בעתיד, לרבות פרסום פומבי. הספק לא יהיה רשאי למכור, להעביר, להמחות, לפרסם, להשכיר, לרשום, או לעשות שימוש כלשהו בתוצרי העבודה, ללא אישור המזמין בכתב ומראש.

7.4 תוצרי העבודה לא יכללו תהליכי עבודה ומערכות ייעודיות של הספק, אשר לא הוכנו עבור המזמין במסגרת ביצוע ההסכם.

7.5 למען הסר ספק, תוצרי העבודה יהיו רכוש המזמין גם אם מתן השירותים ע"י הספק הופסק תוך כדי תקופת ההתקשרות.

7.6 הפרת קניין רוחני

נקבע במסגרת פסק דין חלוט של ערכאה מוסמכת כי שירות שהעמיד ספק לרשות המזמין מפר זכות קניין רוחני של צד שלישי כלשהו, הספק יפעל בהתאם למפורט להלן:

7.6.1 הספק יודיע על כך למזמין בהקדם האפשרי.

7.6.2 הספק יחדל מאספקת השירות המפר.

7.7 הספק ייעשה כל מאמץ סביר על מנת להמשיך לספק את השירות באופן שאינו פוגע בקניין רוחני של צד שלישי כלשהו, וזאת תוך עמידה בחובותיו לפי ההסכם, ומבלי לפגוע ברמת השירות.

8. קבלני משנה

8.1 בכפוף לאמור במסמכי ההתקשרות, הספק יהיה רשאי להפעיל קבלני משנה עבור שירותים שאינם מוגדרים כשירותי ליבה של המערכת.

8.2 מבלי לגרוע מהאמור, האחריות הכוללת לביצוע ההתקשרות ולעמידה בכל תנאיה תהיה של הספק ושלו בלבד.

8.3 בכל מקרה שהספק יעסיק קבלן משנה ייעודי לצורך ביצוע הוראות ההסכם ולצורך זה בלבד, המזמין יהיה רשאי לדרוש מהספק להחליף קבלן משנה זה אם הוא סבור כי הוא אינו מבצע את חובותיו כנדרש.

9. יחסים בין הצדדים

9.1 מוצהר ומוסכם בזה בין הצדדים כי:

9.1.1 היחסים ביניהם לפי ההסכם אינם יחסי עובד ומעביד והמזמין אינו המעסיק של עובדי וקבלני המשנה של הספק.

9.1.2 הספק בלבד יהיה אחראי לכל תשלום, לשיפוי בגין נזק, פיצויים או כל תשלום אחר המגיע ממנו על פי כל דין לאנשים המועסקים על ידו בין באופן ישיר בין כקבלני שירות, או לכל אדם אחר.

9.1.3 המזמין לא ישלם כל תשלום לביטוח לאומי ויתר הזכויות הסוציאליות בקשר לאנשים המועסקים על ידי הספק.

9.1.4 אם למרות האמור לעיל, ערכאה שיפוטית או מנהלית מצאה כי המזמין נושא באחריות ישירה כלפי הספק, עובדיו או קבלני משנה שלו, כאילו הוא מעסיקם, ישפה הספק את המזמין עבור כל תשלום בו הוא חויב וחורג מהתמורה המגיע לו לפי הסכם זה. בכלל זה יישא הספק בתשלומי הוצאות משפט ושכר טרחת עורך דין בהם נשא המזמין.

9.1.5 במקרה של הגשת תביעה כאמור בסעיף זה, יודיע המזמין לספק על קיומה של התביעה, ויאפשר לספק להתגונן.

10. תמורה

10.1 התמורה לספק תשולם בהתאם למפורט בהצעת המחיר, המצורפת כ**נספח ב'** להסכם, ובהתאם לכללים המפורטים להלן.

10.2 תשלום התמורה יעשה בהתאם לאחוז ההנחה הנקוב בהצעת המחיר, אשר יחושב ביחס למחירי למחירון אשר נקבע על ידי הממונה ומצ"ב למכרז (נספח ב.3 3 – מחירון למכרז) עבור שירותי מערכת הסליקה לביצוע פעולות, כפי שהם במועד ביצוע ההזמנה.

10.3 תשלום התמורה יעשה לפי ביצוע בפועל ובכפוף לתנאי ההתקשרות ולהוראות פרק 7 ("מודל התמחור") למכרז.

10.4 התמורה לספק תהיה סופית, ולא ישולם לספק סכום נוסף כלשהו בגין ביצוע הנדרש ממנו לפי הסכם זה, בכלל זה לא ישולם לספק בגין החזר הוצאות, נסיעות, תשלום עבור קבלני משנה תשלומים לצדדי ג' וכדו', אלא אם צוין אחרת במפורש במסמכי ההתקשרות.

10.5 ההצמדה למדד תהיה כמפורט בסעיף 7.3.8.15 לעיל.

10.6 במקרה שבו יחול שינוי בגובה המע"מ תעודכן בהתאם התמורה לה זכאי הספק.

10.7 במקרה בו יהיו שינויים שאינם בגובה המע"מ במיסים או בהיטלים, על מחיר השירותים או הטובין, לא יהיה בשינויים אלה כדי להשפיע על גובה התמורה, אלא בהתאם ובכפוף לקבלת אישור המזמין מראש ובכתב, ולפי שיקול דעתו הבלעדי.

10.8 בכל מקרה שבו יחולו שינויים בהוראות הדין באופן המשפיע על ביצוע ההסכם, הספק יישא בעלויות של שינויים אלו, למעט אם נכתב במפורש אחרת במסמכי ההתקשרות.

10.9 המזמין לא יידרש לכל תשלום שהוא בעד הספקת השירותים נושא מכרז זה, לרבות לעניין קבלת דוחות, דרישות לעדכון המערכת וכן קבלת המידע שבמערכת הסליקה והתיעוד של המערכת לפי הצורך. המזמין אינו ערב לתשלום מטעם המשתמשים, והאחריות על גביית סכומים אלו היא על הספק בלבד.

10.10 המזמין רשאי לדרוש מהספק להרחיב את סל השירותים, סוג המוצרים שלגביהם ניתנים השירותים וסוג הלקוחות שלהם יסופקו השירותים, במהלך תקופת ההתקשרות בהתאם להוראות הדין, במתכונת שתיקבע על ידי הממונה ובהתאם ליכולתו של ספק סביר לספק את השירותים. במידת הצורך, יקבע הממונה תעריף עבור שירות חדש, אשר יתווסף למחירון הסופי.

10.11 האחריות לגביית דמי השימוש תחול על הספק, הספק לא יהיה זכאי לכל תמורה שהיא מעבר לתמורות שיגבה עבור השירותים מן המשתמשים.

11. ערבות ביצוע

11.1 כבטחון למילוי ההתחייבויות של הספק על-פי ההסכם ימסור הספק למזמין ערבות אוטונומית בלתי מותנית, בהיקף של 10,000,000₪.

11.2 ערבות הביצוע תהיה ערבות דיגיטלית בהתאם לתקן הערבויות הדיגיטליות אשר פורסם על יד החשב הכללי, ואשר הונפקה על ידי גוף אשר הוסמך על ידי החשב הכללי להנפקת ערבות דיגיטלית בהתאם לתקן. במקרה כאמור תהיה הערבות בהתאם לנוסח המפורט כנספח ג

להסכם, ותנוהל בהתאם לתקן הערבויות הדיגיטליות ולהוראת תכ"ם 7.3.7 ערבויות דיגיטליות.

11.3 הערבות תונפק על ידי גוף המוסמך להנפיק ערבויות בהתאם להוראות המפורטות ב**הוראת תכ"ם 7.3.3 "ערבויות"**.

11.4 גוף סטטוטורי, חברה ממשלתית, חברת בת ממשלתית ומוסד להשכלה גבוהה שהמדינה משתתפת בתקציבו רשאים להגיש הוראת קיזוז במקום ערבות הגשה בהתאם לנוסח המפורט בהוראת תכ"ם 7.3.3 "ערבויות".

11.5 תוקף הערבות יהיה 90 יום לאחר תום תקופת ההתקשרות. אם המזמין יממש את האופציה להארכת תקופת ההתקשרות, יאריך הספק את תוקף הערבות בהתאמה עד ל- 90 יום לאחר תום תקופת ההתקשרות.

11.6 המזמין רשאי לדרוש להאריך את תוקף הערבות בעוד שלושה חודשים לאחר תום תקופת הערבות, במקרה בו יהיה הדבר נדרש על מנת להבטיח סיום אספקת השירותים או אחריות או לשם הבטחת עמידת הספק בהתחייבויותיו לפי ההסכם. אם הספק לא יאריך את תוקף הערבות בהתאם להוראות ההסכם, רשאי המזמין לחלט את הערבות, בהתאם לשיקול דעתו הבלעדי.

11.7 במהלך תקופת ההתקשרות רשאי המזמין, לפי שיקול דעתו הבלעדי, להפחית את סכום ערבות הביצוע, לסכום נמוך יותר, כפי שיקבע על ידו.

11.8 לאחר תום התוקף של הערבות, במקרה שהיא לא חולטה, יחזיר המזמין את הערבות לספק.

12. אחריות בנזיקין וחובת שיפוי

12.1 הספק יישא באחריות, לפי כל דין, בגין אובדן או נזק מכל סוג שהוא, שייגרם למזמין, לעובדיו וכל מי מטעמו וכן לכל גוף, אדם או צדדים שלישיים כלשהם, עקב מעשה או מחדל של הספק, עובדיו, שלוחיו, קבלני משנה שלו או כל מי שבא מכוחו או מטעמו, במסגרת ביצוע הסכם זה. הספק מתחייב לדווח למזמין על כל נזק או אובדן כאמור, באופן מידי.

12.2 המזמין, הבאים מכוחו או המועסקים על ידו לא יישאו באחריות ולא יישאו בשום תשלום, הוצאה, אובדן או נזק, בגין נזק מכל סוג שהוא שייגרם לספק, לבאים מכוחו או למועסקים על ידו . האמור לא יחול ביחס לנזק שנגרם בזדון ושהאחריות בגינו מוטלת על המזמין לפי דין.

12.3 הספק יהיה אחראי לתקן כל נזק או אובדן, אם יגרמו עקב ביצוע ההתקשרות ע"י הספק או מי מטעמו, ולהשיב את המצב לקדמותו- במועד הקרוב ביותר לאחר התרחשות הנזק או האובדן. אין באמור, כדי לגרוע מזכות המזמין לתקן את הנזק או האובדן בעצמו ולחייב את הספק בתשלום הוצאותיו. ההחלטה על אופן ביצוע התיקון, תהיה נתונה לשיקול דעתו הבלעדי של המזמין.

12.4 לא יהיה בסיומו של הסכם זה כדי לגרוע מאחריות הספק לגבי נזקים שעילת התביעה בגינם נובעת מהסכם זה או מאספקת השירותים על פיו או קשורה אליהם.

12.5 הספק מתחייב לשפות את המזמין באופן מלא, במקרה שיחויב המזמין בפסק דין חלוט של ערכאה שיפוטית מוסמכת, ולשלם כל סכום בגין חיוב שעל פי הסכם זה חב בו הספק, ובתוספת כל הוצאותיו של המזמין, לרבות הוצאות משפטיות ושכר טרחת עורך דין שיהיו

לו בקשר לתביעה בגין האמור, וכן בתוספת הפרשי הצמדה וריבית על פי דין. חובת השיפוי כאמור תחול בין אם השיפוי נובע מתביעתו של עובד של הספק או מי מטעמו של הספק (לרבות קבלני משנה) או עובד של המזמין או צד שלישי או של מבטח או מכל מקור אחר. הסכומים כאמור ישולמו למזמין מיד עם הגשת דרישתו בכתב ובה פירוט ההוצאות שנגרמו לו כאמור.

12.6 טענות צד שלישי

12.6.1 הועלתה ע"י צד שלישי, טענה שעילתה נובעת או קשורה להתקשרות זו לרבות, הפרת זכויות קניין הרוחני או נזקים שנגרמו לצד שלישי כלשהו (להלן: "**טענת הפרה**"), יפעלו הצדדים בהתאם למפורט להלן:

12.6.2 הצדדים יעדכנו אחד את השני בדבר הטענה ועילתה, בהקדם האפשרי על מנת לאפשר לכל צד להתגונן כלפי הטענה.

12.6.3 במקרה בו הוגשה תביעה בטענה כאמור, רשאי המזמין לדרוש מהספק להיכנס בנעלי המזמין לצורך ניהול ההליך.

13. ביטוח

13.1 הספק מתחייב, ולקיים את כל הביטוחים המפורטים ב**נספח ד'** על כל תנאיו, במהלך כל תקופת ההתקשרות.

13.2 בנוסף לביטוחים הנדרשים והמפורטים במכרז, על הספק לבחון את חשיפתו לאור הוראות המכרז וההסכם ולקבוע את הביטוחים הנחוצים לו, בהתאם לניהול סיכונים של הספק.

13.3 אין בכל האמור בסעיפי הביטוח כדי לפטור את הספק, מכל חובה החלה עליו על פי ההתקשרות ועל פי כל דין.

14. המחאת זכויות או חובות על פי ההסכם

14.1 חל איסור מוחלט על הספק להמחות או להסב כל זכות או חובה על פי הסכם זה או את ביצוע ההסכם, ללא אישור מראש ובכתב של המזמין, בהתאם לשיקול דעתו הבלעדי. מבלי לגרוע מהאמור, המחאת זכויות או חובות לפי הסכם זה תיעשה בכפוף לחתימה על הסכם "גב אל גב" בין הממחה לנמחה. ההסכם האמור יועבר לידי המזמין כתנאי לכניסתה לתוקף של המחאת הזכויות או החובות.

14.2 מוצהר ומוסכם בזה כי למזמין הזכות להמחות או להסב כל זכות או חובה על פי הסכם זה ללא צורך בקבלת אישור כלשהו מהספק או מצד ג' כלשהו.

15. הפסקת ההתקשרות

15.1 המזמין יהיה רשאי להודיע לספק בהודעה מוקדמת של 90 יום על הפסקת ההתקשרות מכל סיבה, בהתאם לשיקול דעתו הבלעדי של המזמין.

15.2 תוקפה של ההתקשרות מותנה בקיומו של תקציב מאושר של המזמין. במקרה שבמהלך תקופת ההתקשרות לא יהיה תקציב מאושר כאמור תופסק ההתקשרות לאלתר.

15.3 מבלי לפגוע בכלליות האמור בכל מקום בהסכם, המזמין רשאי להפסיק את ההתקשרות עם הספק, בהתראה של 30 יום, ולאחר קיום שימוע לספק, בכתב או בע"פ, בהתאם להחלטת המזמין, בהתרחש כל אחד מהמקרים הבאים:

15.3.1 אם ימונה קדם מפרק, מפרק זמני או קבוע לספק;

15.3.2 אם ימונה כונס נכסים זמני או קבוע לעסקי ו/או לרכוש הספק;

15.3.3 אם יינתן צו הקפאת הליכים לספק;

15.3.4 אם ניתן לספק צו לפתיחת הליכים לפי חוק חדלות פירעון ושיקום כלכלי, התשע"ח 2018, או צו שווה ערך במדינה אחרת;

15.3.5 אם הספק פשט את הרגל, חלה במחלה אשר מונעת ממנו את היכולת לבצע את האמור בהסכם זה, או הסתלק מביצוע ההסכם מכל סיבה אחרת;

15.4 על הספק להודיע מידית למזמין על התרחשות אחד המקרים המפורטים בסעיף זה.

16. הפרת ההסכם

הפרה יסודית של ההסכם

16.1 אלה יחשבו כהפרה יסודית של הסכם זה (להלן – "**הפרה יסודית**"):

16.1.1 הפרת סעיפי ההסכם הבאים (לפי כותרת הסעיפים): התחייבויות והצהרות הספק; סודיות; אבטחת מידע; ניגוד עניינים בביצוע ההסכם; קניין רוחני וזכויות יוצרים; קבלני משנה; ערבות ביצוע; הגבלת אחריות; ביטוח; המחאת זכויות או חובות על פי ההסכם;

16.1.2 אם הספק לקח חלק בתיאום הצעות, לצורך זכיה במכרז;

16.1.3 אספקת מוצר שלא עומד בדרישות ההתקשרות;

16.1.4 אם הספק הסתלק מביצוע ההסכם;

16.2 הפר הספק את ההסכם הפרה יסודית רשאי המזמין, לפי שיקול דעתו, לפעול בהתאם למפורט להלן:

16.2.1 לאפשר לספק לתקן את הפגם, וזאת תוך 7 ימי עבודה מעת קבלת ההודעה מאת המזמין, או תוך פרק זמן ארוך יותר שיקבע המזמין בהתאם לנסיבות העניין. בכל מקרה בו ההפרה לא תוקנה בפרק הזמן שהגודר לצורך כך, המזמין יהיה רשאי להודיע לספק בהודעה מוקדמת של 7 ימים על הפסקת ההתקשרות.

16.2.2 אם כתוצאה מההפרה היסודית המזמין או מי מטעמו צפויים להיפגע באופן מידי, רשאי המזמין להפסיק מיידית את ההתקשרות עם הספק או כל חלק ממנה ללא התראה מוקדמת ולבטל את ההסכם וזאת מבלי לגרוע מזכות המזמין לסעד או פיצוי כאמור, בהסכם או על פי כל דין.

הפרת הסכם שאינה יסודית

16.3 מבלי לגרוע מהאמור לעיל, בכל מקרה של אי עמידה של הספק בהתחייבויותיו על פי ההתקשרות, מכל סיבה שהיא, המזמין רשאי לאפשר לספק לתקן את הפגם וזאת תוך 15 ימים ממועד משלוח הודעה בכתב מאת המזמין בהתאם להוראות ההסכם, או תוך פרק זמן אחר שיקבע המזמין בהתאם לנסיבות העניין.

16.4 בכל מקרה בו ההפרה לא תוקנה בפרק הזמן שהגודר לצורך כך, יהיה רשאי המזמין לפעול בהתאם לתרופות המפורטות להלן:

ביטול ההסכם עקב הפרה או הפרה צפויה

16.5 המזמין יהיה רשאי להודיע לספק בהודעה מוקדמת של 30 יום על סיום או השהיית ההתקשרות בגין הפרת ההסכם.

16.6 נוכח הספק לדעת כי קיימת אפשרות מסתברת כי לא יוכל לעמוד בהתחייבויותיו כולן או מקצתן מכל סיבה שהיא, או כי לא יוכל לעמוד במועדי ובתנאי השירות (בסעיף זה: "**הפרה צפויה**"), יודיע על כך מיד בעל פה ובדואר אלקטרוני למזמין.

16.7 בכל מקרה של הפרה צפויה של ההסכם, רשאי המזמין לפי שיקול דעתו לאפשר לספק להכין תכנית לתיקון הליקויים ולדון בה, לסיים את ההתקשרות או להשהותה או כל חלק ממנה.

קיזוז ועכבון

16.8 מבלי לגרוע מזכויות המזמין לפי הסכם זה או על פי כל דין, למזמין תהיה זכות לקזז מסכומים שהוא חב לספק על פי ההסכם, כל חוב שהספק חייב לו, בין קצוב ובין שאינו קצוב, לרבות בין הזמנות. כן יהיו המזמין רשאי לעכב תחת ידו כל סכום שהוא חייב לספק, עד לתשלום כל חוב שיש לספק כלפי המזמין. אם אפשר, יפעל המזמין על מנת לתת אפשרות לספק להשמיע טענותיו לעניין זה.

16.9 לספק לא תהא כל זכות קיזוז או עכבון כלפי המזמין או מזמין כלשהו בגין כל סכום שלטענתו מי מהם חייב לו.

חילוט ערבות

16.10 מבלי לפגוע באמור בכל מקום אחר בהסכם, ערבות הביצוע ניתנת לחילוט על ידי המזמין עקב הפרת תנאי ההסכם על ידי הספק או בגין התנהגות שאינה מקובלת ושאינה בתום לב, או לצורך כל תשלום אחר המגיע למזמין מהספק, ובכלל זה פיצויים.

16.11 לספק תינתן הזדמנות להציג את טענותיו בכתב או בעל פה, בטרם יממש המזמין את סמכותו לפי סעיף זה.

16.12 במקרה שחילוט הערבות נעשה לצורך פיצוי המזמין, מובהר בזאת כי חילוט הערבות לא ייחשב כתשלום מלוא הפיצויים בהתאם להסכם זה, וכי המזמין יהיה זכאי לקבל מן הספק את ההפרש בין הסכום ששולם עקב חילוט הערבות, ובין סכום הפיצויים המגיעים למזמין.

16.13 לאחר חילוט הערבות, ובהתאם להנחיות המזמין ולשיקול דעתו הבלעדי, יידרש הספק להעמיד ערבות ביצוע חדשה בסכום הקבוע בהסכם זה, כתנאי להמשך ההתקשרות.

רכש מספק חלופי

16.14 מבלי לגרוע מהאמור בכל מקום אחר בהסכם ובמכרז, אם כתוצאה מהפרת הסכם או הפרה צפויה, שירות הנדרש למזמין אינו זמין מהספק לשביעות רצון המזמין, ירכוש אותו המזמין מספק חלופי, בהתאם לשיקול דעתו הבלעדי. אם אפשר, יפעל המזמין על מנת לתת אפשרות לספק להשמיע טענותיו לעניין זה.

17. תרופות מצטברות

17.1 התרופות, לרבות זכות הקיזוז, עיכבון, חילוט, פיצויים מוסכמים, וכל הפעולות שרשאי המזמין בהסכם זה לעשות בתגובה להפרת ההסכם בידי הספק, הן מצטברות, ואין בכל הוראה בהסכם זה כדי לשלול את זכותו של המזמין לכל סעד או תרופה בהתאם להסכם זה או לפי כל דין.

17.2 ויתר המזמין על זכויותיו עקב הפרת הוראה מהוראות הסכם זה על ידי הספק, לא ייחשב כוויתור על כל הפרה אחרת של אותה הוראה או הוראה אחרת.

18. פיצויים מוסכמים

18.1 על כל הפרת תנאי ההסכם רמת השירות כפי שמופיע בפרק 6.3 למסמכי המכרז יפצה הספק את המזמין כפי שנקבע במכרז ובהתאם למועדים שנקבעו במכרז.

18.2 כספי הפיצויים יועברו לקרן שתשמש למטרות שעליהן יורה הממונה. במידה שהספק לא יעביר את כספי הפיצויים המוסכמים במועד, שומר לעצמו המזמין את הזכות לחלט את הסכום שנקבע במסמכי המכרז מהערבות בכפוף לשימוע.

19. סיום התקשרות

19.1 הסתיימה או הופסקה ההתקשרות עם הספק, כולה או מקצתה, מכל סיבה שהיא, יחולו הכללים הבאים:

19.1.1 מוסכם ומוצהר כי לא תהא לספק כל תביעה או דרישה כספית או אחרת כלפי המזמין בקשר עם הפסקת פעולתו על פי הסכם זה. יובהר כי בתום סיום ההתקשרות יופעל נוהל ההיפרדות כפי שמופיע במסמכי המכרז.

19.1.2 הספק יידרש לפעול בהקדם וללא דיחוי:

19.1.2.1 להעביר למזמין או לידי מי שהמזמין יקבע באופן מסודר את כל תוצרי העבודה שהצטברו אצלו במהלך ההתקשרות.

19.1.2.2 מבלי לגרוע מהאמור לעיל, הספק יעביר למזמין או לידי מי שהמזמין יקבע תיק מערכת עדכני כולל יישומים, טבלאות, פיתוחים, ממשקים וכל תיעוד אחר שנערך בקשר למערכת.

19.1.2.3 העברת הנתונים והמידע תבוצע על ידי הספק באופן אשר יבטיח רציפות בשירות, לפי הצורך.

19.2 המזמין רשאי להתקשר בהסכם עם ספק אחר בנושא ההתקשרות.

19.3 הספק ישתף פעולה עם המזמין בהעברת האחריות בביצוע חובותיו על פי הסכם זה, למזמין או לספק אחר שנבחר על ידי המזמין. בכלל זה יעביר הספק למזמין או לספק החדש כל מידע רלוונטי, יסייע לו במענה לשאלות, ויהיה זמין לפניותיו. במקרה שהספק לא ישתף פעולה בהעברת האחריות, כמפורט לעיל, הוא יישא באחריות על כל נזק שיגרם למזמין או לספק החדש שהחל בביצוע ההסכם. לא ישולם לספק תשלום נוסף עבור שיתוף הפעולה כאמור מעבר לקבוע בהסכם זה.

20. כתובות הצדדים והודעות

20.1 כל הודעה על פי הסכם זה תימסר בדואר אלקטרוני, אלא אם הסכימו הצדדים אחרת; הודעה בדואר אלקטרוני כאמור תחשב שנתקבלה עם קבלת אישור קריאה, או לאחר 3 ימים מיום אישור משלוח ההודעה בדואר האלקטרוני, המוקדם מבניהם.

20.2 משלוח דואר אלקטרוני על פי הסכם זה יהיה לכתובת הבאות:

- כתובת דוא"ל המזמין: Pension2025@mof.gov.il או כל כתובת דוא"ל אחרת שתעודכן ע"י המזמין.
- כתובת דוא"ל הספק: _____ או כל כתובת דוא"ל אחרת שתעודכן ע"י הספק.

20.3 כל הודעה **מהותית** על פי הסכם זה (כגון הודעות בנוגע לעיכובים, חריגות בתמורה, טענות הפרה, נושאים בעלי דחיפות וכיו"ב) תימסר בדואר אלקטרוני אשר ילווה בפנייה טלפונית לצורך וידוא קבלת הדואר האלקטרוני.

20.4 אישור שליחה מתיבת הדואר האלקטרוני, ישמש ראיה למועד השליחה. אישור קריאה, ישמש ראיה לתאריך המסירה.

21. שונות

21.1 הצדדים מסכימים כי סמכות השיפוט בכל הקשור לנושאים והעניינים הנובעים או הקשורים בהסכם זה תהא אך ורק לבתי המשפט המוסמכים במחוז בו יושבת ועדת המכרזים של המזמין, ויחול עליהם החוק הישראלי.

21.2 פרטים מההסכם ומאופן מימושו יפורסמו ב[אתר חופש המידע הממשלתי](), זאת בהתאם ל[נוהל פרסום התקשרויות]() ובמקרים הרלוונטיים גם לפי [החלטת ממשלה 1116 מיום 29.12.2013](), זאת בהתאם להנחיות המפורטות בהחלטת הממשלה האמורה.

21.3 כל שינוי בהוראת הסכם זה ייעשה בהסכמת שני הצדדים, מראש ובכתב.

21.4 הסכם זה ממצה את כל אשר הוסכם בין הצדדים, ולא יהיה תוקף לכל הסכם או הסדר שנערכו עובר לחתימתו של הסכם זה בנושא ההתקשרות.

21.5 ועד החתימה על ההסכם יהיה מועד החתימה של אחרון הצדדים על ההסכם.

ולראיה באו הצדדים על החתום:

_____ **שם וחתימה** **מורשה חתימה מטעם המזמין** _____ **תאריך**	_____ **שם וחתימה** **מורשה חתימה מטעם הספק** _____ **תאריך**
_____ **שם וחתימה** **מורשה חתימה מטעם המזמין** _____ **תאריך**	_____ **שם וחתימה** **מורשה חתימה מטעם הספק** _____ **תאריך**

נספח ג'– ערבות ביצוע

תדפיס ערבות דיגיטאלית (אין למלא ידנית, למילוי על ידי מערכת)

מסמך זה הוא תדפיס של ערבות דיגיטאלית ונועד לצרכי המחשה בלבד
תדפיס זה הופק ע"י המערכת של &שם מנפיק הערבות/מקבל הערבות לפי העניין& ביום DD/MM/YYYY ב- HH:MM:SS על סמך קובץ ערבות דיגיטאלית.

נתוני הערבות

קוד הערבות הדיגיטאלית: XXXX-YYYN-NNNN-NNNN-NNCC

מנפיק הערבות:
_____ מס' סניף: ____
טלפון מנפיק הערבות: _____ פקס' מנפיק הערבות: _____
כתובת מנפיק הערבות: _____
רחוב ומספר: _____ ישוב: _____ מיקוד _____
שם מורשה החתימה 1: _____
שם מורשה החתימה 2: _____

מקבל הערבות:
_____
_____

הנערבים (להלן ביחד ו/או לחוד: "הנערב"):

מזהה נערב	שם הנערב
_____	_____

נושא הערבות:
(שם המכרז / נושא ההתקשרות)

סכומים ותאריכים
סכום הערבות _____ שקלים חדשים.
הצמדה: _____ תאריך בסיס להצמדה: _____
תאריך הנפקת הערבות: _(מילוי על ידי המנפיק)_ תאריך סיום תוקף הערבות: _____

ניסוח ההתחייבות
מנפיק הערבות, ערב בזה כלפי מקבל הערבות, בעבור הנערב, לסילוק כל סכום אשר מקבל הערבות ידרוש מאת מנפיק הערבות, בקשר עם נושא הערבות, ואשר לא יעלה על סכום גובה הערבות. מנפיק הערבות מתחייב בזאת לשלם למקבל הערבות את הסכום האמור בתוך מספר הימים לחילוט הקבועים בערבות וזאת מתאריך דרישת מקבל הערבות ומבלי שמקבל הערבות יהיה חייב לנמק את דרישתו או לדרוש תחילה את סילוק הסכום מאת הנערב.
במקרה של דרישה כאמור מנפיק הערבות לא יטען כלפי מקבל הערבות טענת הגנה כל שהיא שיכולה לעמוד לו או לנערב, ולא יתנה את התשלום בתנאי כלשהו או יעכבו מסיבה כלשהי ובכלל זה בסילוק הסכום האמור מאת הנערב.
ערבות זו אינה ניתנה להעברה או להסבה.
ערבות זו ניתנת למימוש לשיעורין, באופן שחילוטה החלקי לא יגרע מתוקפה לגבי יתרת סכום הערבות שלא חולט, ובלבד שסך כל התשלומים על פי ערבות זו לא יעלה על סכום הערבות.
על ערבות זו יחולו הוראות הדין הישראלי בלבד.
הכללים לניהול כתב ערבות זה יהיו בהתאם לתקן הערבויות הדיגיטאליות כפי שפורסם באתר הוראות התכ"ם של החשב הכללי, כנוסחו במועד הנפקת הערבות, ובכלל זה בהתאם לכללים המפורטים להלן:

- ניהול ערבות זו יעשה באופן דיגיטלי, על ידי שליחת דרישות ובקשות בין מערכות מקבל הערבות ומערכות מנפיק הערבות, בהתאם לכללים המפורטים בתקן הערבויות הדיגיטליות.
- התאריכים בערבות מתייחסים לימים קלנדריים, המסתיימים בשעה 23:59, וזאת למעט מניין הימים לתשלום בגין חילוט ערבות על ידי מנפיק הערבות. מניין הימים לתשלום בגין חילוט הערבות, יחל ביום העסקים הבנקאי בו התקבלה הדרישה לחילוט ממקבל הערבות.

במקרה שבו הדרישה התקבלה שלא במהלך יום עסקים בנקאי, מנין הימים לביצוע החילוט יחל ביום העסקים הבנקאי העוקב.

- לאחר שתאריך סיום תוקף הערבות חלף, תוקפה של הערבות פוקע ללא צורך בביצוע פעולה נוספת מטעם הנערב, מקבל הערבות או מנפיק הערבות.

<u>מספר ימים לחילוט 15</u>

<u>אסמכתאות (</u>למילוי על ידי המערכת הטכנולוגית, לא על ידי המשרד)
אסמכתא פנימית של מנפיק הערבות:
אסמכתאות פנימיות 1 של מקבל הערבות:
אסמכתאות פנימיות 2 של מקבל הערבות:
אסמכתאות פנימיות 3 של מקבל הערבות:
אסמכתאות פנימיות 4 של מקבל הערבות:

נספח ד'– דרישות ביטוח

א. הספק מתחייב לבצע ולקיים את הביטוחים המפורטים בזה לטובתו ולטובת מדינת ישראל– רשות שוק ההון ביטוח וחיסכון, כשהם כוללים את כל הכיסויים והתנאים הנדרשים להלן וכאשר גבולות האחריות לא יפחתו מהמצוין להלן:

1. <u>ביטוח חבות מעבידים</u>

(1) הספק יבטח את אחריותו החוקית על פי פקודת הנזיקין (נוסח חדש) ו/או חוק האחריות למוצרים פגומים תש"ם -1980 כלפי עובדיו בביטוח חבות המעבידים בכל תחומי מדינת ישראל והשטחים המוחזקים.

(2) גבול האחריות לא יפחת מסך 20,000,000 ₪ לעובד, למקרה ולתקופת הביטוח.

(3) הביטוח יורחב לכסות את חבותו של המבוטח כלפי קבלנים, קבלני משנה ועובדיהם היה ויחשב כמעבידם.

(4) הביטוח יורחב לשפות את מדינת ישראל- רשות שוק ההון, ביטוח וחיסכון , היה ונטען לעניין קרות תאונת עבודה/ מחלת מקצוע כלשהי כי הם נושאים בחבות מעביד כלשהם כלפי מי מעובדי הספק, קבלנים, קבלני משנה ועובדיהם שבשירותו.

2. <u>ביטוח אחריות כלפי צד שלישי</u>

(1) הספק יבטח את אחריותו החוקית על פי דיני מדינת ישראל בביטוח אחריות כלפי צד שלישי גוף ורכוש (כולל נזקי גרר), בכל תחומי מדינת ישראל והשטחים המוחזקים.

(2) גבול האחריות לא יפחת מסך 4,000,000 ₪ למקרה ולתקופת הביטוח.

(3) בפוליסה ייכלל סעיף אחריות צולבת - CROSS LIABILITY.

(4) הביטוח יורחב לכסות את חבותו של המבוטח כלפי צד שלישי בגין פעילות של קבלנים, קבלני משנה ועובדיהם.

(5) הביטוח יורחב לשפות את מדינת ישראל- רשות שוק ההון, ביטוח וחיסכון ככל שייחשבו אחראים למעשי ו/או מחדלי הספק וכל הפועלים מטעמו.

3. <u>ביטוח משולב לאחריות מקצועית וחבות המוצר</u>

COMBINED PRODUCTS LIABILITY AND PROFESSIONAL INDEMNITY POLICY FOR THE SOFTWARE AND HARDWARE INDUSTRY

או

ELECTRONIC PRODUCTS AND SERVICES ERRORS OR OMISSONS AND PRODUCTS LIABILITY INSURANCE

או

נוסח אחר לביטוח משולב לאחריות מקצועית וחבות המוצר לענף הייטק/תחום מחשוב כדלהלן:

_____(בכפוף לבחינתה ולשיקולה של ענבל).

(1) ביטוח אחריותו של הספק בגין הפעלה, תחזוקה ופיתוח של מערכת סליקה פנסיונית מרכזית בישראל המבוססת על השירותים הניתנים על ידי מערכת הסליקה הקיימת ומתן שירותים חדשים, כולל הקמה ותפעול תשתית טכנולוגית מותאמת לטכנולוגיית API לשם העברת מידע וביצוע פעולות באופן ממוכן ואחיד בשוק החיסכון הפנסיוני, הקמה ותפעול של תשתית טכנולוגית להנפקת סרטיפיקטים, הקמה ותפעול של מנגנוני אבטחת מידע, חיבור לקוחות ומשתמשים אל מערכת הסליקה, מתן שירות לבעל רישיון, תיעוד, הדרכה והכשרה לגבי השימוש במערכת, הקמה והפעלת מערך שירות ותמיכה, קיום ממשקי תקשורת עם גורמים נוספים, בהתאם למכרז והסכם עם מדינת ישראל – רשות שוק ההון, ביטוח וחיסכון, בביטוח משולב לאחריות מקצועית וחבות המוצר.

(2) הפוליסה תכסה את חבות הספק, עובדיו ובגין כל הפועלים מטעמו:

א. בקשר עם מעשה או מחדל מקצועי- כיסוי בגין הפרת חובה מקצועית, טעות השמטה, הזנחה ורשלנות.

ב. חבותו מפגם במוצר- כיסוי בגין נזקים שייגרמו בקשר עם מוצרים שיוצרו, פותחו, הורכבו, תוקנו, סופקו, נמכרו, הופצו או טופלו בכל דרך אחרת על ידי הספק או מי מטעמו.

ג. פעילות הספק, עובדיו ובגין כל הפועלים מטעמו כמפורט בסעיף (1) לעיל.

(3) גבולות האחריות למקרה ולשנה לא יפחתו מסך של 20,000,000 ₪.

(4) הפוליסה תכלול את ההרחבות הבאות:

- אובדן מסמכים לרבות אובדן השימוש ו/או העיכוב עקב מקרה ביטוח.
- מרמה ואי יושר עובדים.
- פגיעה בפרטיות.
- תקופת גילוי של לפחות 12 חודשים.
- אחריות צולבת - Cross Liability.

(5) הביטוח יורחב לשפות את מדינת ישראל– רשות שוק ההון, ביטוח וחיסכון לגבי אחריותם בגין נזק עקב פגם במוצרים אשר סופקו, הותקנו ותוחזקו על ידי הספק וכל הפועלים מטעמו ו/או ככל שייחשבו אחראים למעשי ו/או מחדלי הספק וכל הפועלים מטעמו.

4. <u>ביטוח סייבר</u>

(1) הספק יבטח את אחריותו החוקית על פי דיני מדינת ישראל בביטוח חבות סייבר, בין היתר, עקב האירועים המפורטים להלן:

- חבות בדבר הפרת פרטיות כלפי צד שלישי.
- הפרת סודיות כלפי צד שלישי.
- חבות Cyber Security כלפי צד שלישי.
- חבות Media Liability.

(2) הפוליסה תכסה אובדן או נזק סייבר לצד ראשון (הוצאות שהוצאו על ידי המבוטח לצורך שיקום הרשת של המבוטח או לנתונים השמורים ברשת של המבוטח), החלפת חומרה וכן ניהול אירועי סייבר ומשברים, תמיכה ליווי וייעוץ.

(3) גבול האחריות לא יפחת מסך 7,500,000 דולר ארה"ב למקרה ולתקופת הביטוח.

(4) הכיסוי על פי פרק החבות כלפי צד שלישי יורחב לכלול:

- סעיף אחריות צולבת, אולם הכיסוי לא יחול על תביעות הספק כנגד מדינת ישראל - רשות שוק ההון, ביטוח וחיסכון, משרדי הממשלה, יחידות הסמך וגופים נלווים.
- הרחבה לפיה הביטוח יורחב לשפות את מדינת ישראל- רשות שוק ההון, ביטוח וחיסכון, משרדי הממשלה, יחידות הסמך וגופים נלווים ככל שייחשבו אחראים למעשי ו/או מחדלי הספק והפועלים מטעמו.

(5) מדינת ישראל תיכלל המבוטחת נוספת בביטוחי הספק.

(6) הפוליסה תכלול הרחבה בדבר תקופת הגילוי של לפחות 2 חודשים.

5. <u>ביטוחים נוספים</u>:

בעלי מקצוע, יועצים בתחומים שונים, עו"ד, רו"ח, קבלנים וקבלני משנה יערכו ביטוחים מתאימים לגבי פעילותם בגבולות אחריות סבירים, כולל גם ביטוח אחריות כלפי צד שלישי, וביטוח חבות מעבידים כלפי עובדיהם, ביטוח אחריות מקצועית וביטוח חבות מוצר (ככל ורלוונטיים). כאשר הפעילות משולבת עם כלי רכב, יערכו גם ביטוחי כלי רכב הכוללים ביטוח חובה, רכוש ואחריות כלפי צד שלישי. הביטוחים יורחבו לשפות את מדינת ישראל- רשות שוק ההון, ביטוח וחיסכון ככל שיחשבו אחראים למעשיהם ו/או מחדליהם, הספק יוודא כי בכל הביטוחים שערך לפי סעיף זה, ייכלל סעיף ויתור על זכות התחלוף / השיבוב כלפי מדינת ישראל- רשות שוק ההון, ביטוח וחיסכון, ועובדיהם (ויתור כאמור לא יחול לטובת האדם שגרם את הנזק בזדון) וכן סעיף לפיו הביטוחים יהיו קודמים וראשוניים ללא זכות השתתפות ו/או חזרה.

6. <u>כללי</u>

בכל פוליסות הביטוח הנדרשות מהספק יכללו התנאים הבאים:

(1) לשם המבוטח יתווספו כמבוטחים נוספים : מדינת ישראל– רשות שוק ההון, ביטוח וחיסכון, בכפוף להרחבי השיפוי לעיל.

(2) בכל מקרה של שינוי לרעה או ביטול הביטוח ע״י אחד הצדדים לא יהיה להם כל תוקף אלא, אם ניתנה על כך הודעה מוקדמת של 60 יום לפחות במכתב לחשב רשות שוק ההון, ביטוח וחיסכון .

(3) המבטח מוותר על כל זכות תחלוף/ שיבוב, תביעה, השתתפות או חזרה כלפי מדינת ישראל- רשות שוק ההון, ביטוח וחיסכון ועובדיהם, ובלבד שהוויתור לא יחול לטובת אדם שגרם לנזק מתוך כוונת זדון.

(4) הספק אחראי בלעדית כלפי המבטח לתשלום דמי הביטוח עבור כל הפוליסות ולמילוי כל החובות המוטלות על המבוטח על פי תנאי הפוליסות.

(5) ההשתתפויות העצמיות הנקובות בכל פוליסה ופוליסה תחולנה בלעדית על הספק.

(6) כל סעיף בפוליסות הביטוח המפקיע או מקטין בדרך כלשהיא את אחריות המבטח, כאשר קיים ביטוח אחר לא יופעל כלפי מדינת ישראל, והביטוח הינו בחזקת ביטוח ראשוני המזכה במלוא הזכויות על פי הביטוח.

(7) תנאי הכיסוי של הפוליסות הנ״ל (למעט ביטוח אחריות מקצועית משולב עם ביטוח חבות מוצר וביטוח סייבר) לא יפחתו מהמקובל על פי תנאי פוליסות נוסח ״ביט״ בכפוף להרחבת הכיסויים כמפורט לעיל.

(8) חריג כוונה ו/או רשלנות רבתי יבוטל ככל שקיים.

א. הספק מתחייב בכל תקופת ההתקשרות החוזית עם מדינת ישראל- רשות שוק ההון, ביטוח וחיסכון וכל עוד אחריותו קיימת, להחזיק בתוקף את פוליסות הביטוח. הספק מתחייב כי פוליסות הביטוח תחודשנה מדי תקופת ביטוח, כל עוד ההסכם עם מדינת ישראל- משרד האוצר, בתוקף.

ב. אישור בחתימתו של המבטח על קיום הביטוחים יומצא על ידי הספק ל רשות שוק ההון, ביטוח וחיסכון, עד למועד חתימת ההסכם. הספק מתחייב להציג את האישור חתום בחתימת המבטח אודות חידוש הפוליסות למשרד האוצר, לכל המאוחר שבעה ימים לפני תום תקופת הביטוח.

מובהר בזאת כי אישורי הביטוח שיוצגו אינם באים לצמצם ו/או לגרוע מהתחייבויות הספק לערוך את הביטוחים לפי סעיפי הביטוח המפורטים לעיל, ולמען הסר ספק דרישות הביטוח המחייבות הן בהתאם לאמור לעיל. הספק נדרש ללמוד ולעמוד בדרישות אלה ובמידת הצורך להיעזר באנשי ביטוח מטעמו, על מנת לעמוד בדרישות וליישמן בביטוחיו כנדרש.

ג. מדינת ישראל – רשות שוק ההון, ביטוח וחיסכון , שומרים לעצמם את הזכות לקבל מהספק בכל עת את העתקי הפוליסות במלואן או בחלקן, במקרה של גילוי נסיבות העלולות להביא לתביעה בפוליסות ו/או על מנת שיוכלו לבחון את עמידת הספק בסעיפים אלו ו/או מכל סיבה אחרת, והספק יעביר את העתקי הפוליסות במלואן או בחלקן כאמור מיד עם קבלת הדרישה. הספק מתחייב לבצע כל שינוי או תיקון שיידרש על מנת להתאים את הפוליסות להתחייבויותיו על פי הוראות הביטוח

שלעיל. מוסכם כי הספק יהיה רשאי למחוק מפוליסות הביטוח כאמור מידע עסקי ו/או מסחרי סודי שאינו רלוונטי להתקשרות זו.

הספק מצהיר ומתחייב כי זכות מדינת ישראל - רשות שוק ההון, ביטוח וחיסכון לעריכת הבדיקה ולדרישת השינויים כמפורט לעיל אינן מטילות על מדינת ישראל- רשות שוק ההון, ביטוח וחיסכון או על מי מטעמם כל חובה וכל אחריות שהיא לגבי פוליסות הביטוח/ אישורי הביטוח כאמור, טיבם, היקפם ותוקפם, או לגבי העדרם, ואין בהן כדי לגרוע מכל חובה שהיא המוטלת על הספק לפי ההסכם, וזאת בין אם נדרשו התאמות ובין אם לאו, בין אם נבדקו ובין אם לאו.

ד. למען הסר כל ספק מוסכם בזה כי הביטוחים הנדרשים בסעיף ביטוח זה, גבולות האחריות ותנאי הכיסוי הם בבחינת דרישה מינימלית המוטלת על הספק, ואין בהם משום אישור המדינה או מי מטעמה להיקף וגודל הסיכון לביטוח ועליו לבחון את חשיפתו לסיכונים ולקבוע את הביטוחים הנחוצים לרבות היקף הכיסויים, תקופות הביטוח, וגבולות האחריות בהתאם לכך.

ה. אין בכל האמור בסעיפי הביטוח כדי לפטור את הספק מכל חובה החלה עליו על פי דין ועל פי ההסכם ואין לפרש את האמור כוויתור של מדינת ישראל- רשות שוק ההון, ביטוח וחיסכון על כל זכות או סעד המוקנים להם על פי כל דין ועל פי הסכם זה.

ו. אי עמידה בתנאי סעיפי ביטוח אלו מהווה הפרה יסודית של הסכם זה.

נספח ה' – התחייבות לסודיות והיעדר ניגוד עניינים

לכבוד

רשות שוק ההון, ביטוח וחיסכון

1. אני _____, ת"ז _____, אשר תפקידי אצל _____ *[למלא שם הספק]* (להלן - "**הספק**") הינו _____, נותן התחייבות זו בקשר למכרז מערכת סליקה פנסיונית מרכזית - הפעלה, תחזוקה ופיתוח מספר 5/2025 (להלן - "**המכרז**") .

2. בהתחייבות זו תהיה למונחים הבאים המשמעות המופיעה לצידם:

"**מידע**" - כל מידע (Information), ידע (Know-How), ידיעה, מסמך, תכתובת, תוכנית, נתון, מודל, חוות דעת, מסקנה וכל דבר אחר כיוצ"ב הקשור באספקת השירותים בין בכתב ובין בע"פ ו/או בכל צורה או דרך של שימור ידיעות בצורה חשמלית ו/או אלקטרונית ו/או אופטית ו/או מגנטית ו/או אחרת.

"**סודות מקצועיים**" - כל מידע אשר יגיע לידי בקשר לאספקת השירותים, בין אם נתקבל במהלך מתן השירותים או לאחר מכן, לרבות ומבלי לפגוע בכלליות האמור לעיל: מידע אשר יימסר על ידי מדינת ישראל ו/או כל גורם אחר ו/או מי מטעמה.

3. הנני מתחייב לשמור את המידע והסודות המקצועיים שיגיעו אלי עקב ההסכם, בסודיות מוחלטת ולעשות בהם שימוש אך ורק לצורך מילוי חובותיי על פי ההסכם.

4. מבלי לפגוע בכלליות האמור, הנני מתחייב לא לפרסם, להעביר, להודיע, למסור או להביא לידיעת כל אדם את המידע והסודות המקצועיים שהגיעו אלי עקב ההסכם, למעט מידע שהוא בנחלת הכלל או מידע שיש למסור על פי כל דין.

5. לא מתקיים כל ניגוד עניינים בין כל פעילות אחרת או התחייבות אחרת שלי לבין התחייבויות הספק על פי הסכם זה.

6. אמנע מכל פעולה שיש בה כדי ליצור ניגוד עניינים בין מילוי תפקידי על פי ההסכם לבין מילוי תפקיד או התחייבות אחרת, במישרין או בעקיפין.

7. אני מתחייב להודיע למזמין על כל חשש לקיום ניגוד עניינים בין התחייבויותיי על פי ההסכם לבין פעילות אחרת שלי.

שם: _____ חתימה: _____ תאריך: _____

נספח ה1- תצהיר העדר ניגוד עניינים עבור נושאי משרה אצל הספק וביחידי הספק

[טופס זה ימולא וייחתם רק על ידי הספק הזוכה - על ידי כל נושא משרה מוצע בחברה שתוקם על ידי הספק הזוכה, ועל ידי כל נושא משרה בכל אחד מיחידי המציע, ככל שישנם]

שם: _____, ת.ז. _____

שם המציע או החבר במציע: _____

תפקיד אצל המציע: _____

לאחר שהוזהרתי כי עלי לומר את האמת וכי אהיה צפוי לעונשים הקבועים בחוק אם לא אעשה כן, מצהיר/ה בזה כדלקמן:

1. להלן פירוט גופים מוסדיים, מפיצים וכן כל גוף אחר הקשור לענפי החיסכון הפנסיוני והבנקאות הפועלים בישראל בהם הייתי מועסק, ותאגידים הקשורים להם בין כעובד ובין כקבלן, ב-10 השנים האחרונות:

שם התאגיד	תפקידי בתאגיד	השנים בהם הייתי קשור בתאגיד	הערות וכל מידע רלבנטי אחר

2. להלן פירוט תאגידים בהם בעל תפקיד בכיר, הינו קרוב שלי. לעניין זה "קרוב" - בן-זוג, אח, הורה, סב, וצאצא או בן-זוג של כל אחד, אשר הוא קשור, באופן ישיר או עקיף, עם גוף מוסדי, מפיץ או גוף אחר הקשור לענפי החיסכון הפנסיוני והבנקאות הפועל בישראל.

התאגיד, מהות פעילותו בישראל, או שרשור הבעלות שלו לגוף מוסדי, מפיץ או גורם אחר הקשור לענפי החיסכון הפנסיוני והבנקאות הפועל בישראל (בצירוף תרשים)	שמו של קרובי, וקרבתי אליו	תפקידו בתאגיד	הערות וכל פרט מהותי אחר

3. להלן פירוט התקשרויות מהותיות עם גופים מוסדיים, מפיצים או גופים קשורים לענפי החיסכון הפנסיוני והבנקאות הפועלים בישראל, או עם תאגיד הקשור עם אחד מאלה, אשר לא פורטו בטבלה דלעיל:

_____

_____

4. איני פועל בשוק החיסכון הפנסיוני בישראל ואני עונה על כל האמור להלן:
   א. איני נושא משרה בגוף מוסדי או תאגיד בנקאי בעל רישיון בישראל;
   ב. איני סוכן ביטוח פנסיוני בעל רישיון בישראל;
   ג. איני יועץ פנסיוני בעל רישיון בישראל.

5. להלן פירוט קשרי שליטה, במישרין או בעקיפין, עם גופים מוסדיים, מפיצים וכן עם גורמים הקשורים לענפי החיסכון הפנסיוני והבנקאות בכלל בישראל.

הגוף המוסדי, המפיץ או הגורם הקשור לענפי החיסכון הפנסיוני והבנקאות בישראל	**סוג אמצעי השליטה**	**שיעור אמצעי השליטה**	**שרשור השליטה (בצירוף תרשים)**

6. להלן פירוט התקשרויות מהותיות עם גופים מוסדיים, מפיצים וכן עם גורמים הקשורים לענפי החיסכון הפנסיוני והבנקאות בכלל בישראל, או עם תאגיד הקשור עם אחד מאלה, אשר לא פורטו בטבלה דלעיל:

_____

_____

7. להלן מידע מהותי נוסף העשוי להשפיע על שיקול דעת המזמין

_____

_____

8. אני מתחייב שלא לעבוד בגוף מוסדי, מפיץ, אצל או עם גורם הקשור לענפי החיסכון הפנסיוני והבנקאות בכלל בישראל, בתקופה בה אני מועסק במערכת הסליקה הפנסיונית המרכזית ולמשך תקופה של שנה אחת מתום עבודתי כאמור.

תאריך _____ חתימה_____

תצהיר

אני החתום מטה _____, ת.ז. _____ ממלא תפקיד של _____ ב_____ (המציע או מי מיחידי המציע), מצהיר בזה כי המידע והפרטים הנזכרים לעיל משקפים מידע מלא ומדויק.

תאריך _____ חתימה _____

<u>אישור עורך הדין</u>

אני הח"מ _____, עו"ד מאשר/ת כי ביום _____ הופיע/ה בפני במשרדי אשר ברחוב _____ בישוב/עיר _____ מר/גב' _____ שזיהה/תה עצמו/ה על ידי ת.ז. _____ /המוכר/ת לי באופן אישי, ואחרי שהזהרתיו/ה כי עליו/ה להצהיר אמת וכי יהיה/תהיה צפוי/ה לעונשים הקבועים בחוק אם לא יעשה/תעשה כן, חתם/ה בפני על התצהיר דלעיל.

_____	_____	_____
תאריך	מספר רישיון	חתימה וחותמת

נספח ו' – נספח סייבר ואבטחת מידע – רמה גבוהה

הגדרות ייעודיות לטופס זה:

אירוע אבטחה – אירוע (incident) אשר עלול לפגוע בזמינות, ברציפות התפעולית, במהימנות או בסודיות המידע של המשרד, של מערכות או קוד המסופקות לו, של חומרה, תכנה, מאגרי מידע או תשתית, שבהם הספק עושה שימוש לצורך ביצוע ההסכם, ובכלל זה תקיפת סייבר.

גורם מנחה – הגורם המנחה את המזמין בהיבטי סייבר והגנות מידע כגון: היחידה להגנת הסייבר בממשלה (להלן: "יה"ב") במערך הדיגיטל הלאומי, הממונה על הביטחון במשרד הביטחון (מלמ"ב), או מערך הסייבר הלאומי. אם המזמין מנחה את עצמו, אז ייחשב המזמין כגורם המנחה לעניין זה.

גורמי שרשרת האספקה – קבלני המשנה של הספק ובכלל זה, יצרני חומרה או ספקי תוכנה או שירות, אשר הספק אינו יכול להחליפם מבלי שהדבר יפגע באספקת השירותים בהתאם לדרישות ההתקשרות.

מידע – כל מסמך, תכתובת, תכנית, נתון, עובדה, פרט תוכן, מודל, תמונה, סרט, הקלטה, תהליך עסקי, חוות דעת, קוד ולוגיקה, אשר נשמרו או תועדו על ידי הספק באמצעי טכנולוגי מכל סוג שהוא.

מידע רגיש – מידע של המזמין אשר יש בחשיפתו כדי לפגוע או לשבש בדרך כלשהי את עבודת המזמין, לפגוע בשירותים המסופקים על ידי המזמין או הממשלה, או לחשוף פרטים ומידע של המזמין אשר אינם נחלת הכלל, ובכלל זה מידע אישי של אזרחים או עובדים, תהליכי עבודה רגישים, שרטוטי מתקנים, תיאור מערכות אבטחה, קוד מקור ותוכנות של מערכות המזמין, מסמכי תכנון של מערכות המזמין או של מערכות המותאמות לשימושו, אמצעי הזדהות ואימות, מידע לגבי מזמינים מסווגים, יעדי הספקה של חומרה או מערכות וכל מידע אחר שיוגדר על ידי המזמין.

מינהל הרכש – מינהל הרכש הממשלתי באגף החשב הכללי או נציגו.

שירות חיוני – אחד מאלה:

שירותים המסופקים על ידי המזמין לאזרחי ותושבי מדינת ישראל אשר תפקודם התקין והסדור הוא קריטי לניהול חיי האזרח או לפעילות המשק.

שירות של המזמין הנדרש לתפקודו התקין של המשרד או הממשלה.

תקיפת סייבר – אירוע אבטחה אשר נוצר כתוצאה מניסיון לעבור או לעקוף את אמצעי האבטחה או הבקרה שבהם הספק או המזמין עושים שימוש, למנוע גישה לשירות או למידע, או לנצל חולשה קיימת בניסיון לגרום להרס, אובדן, דלף, שינוי, שימוש, חשיפה לא מורשית או גישה לנתוני המזמין.

1. כללי

הספק יהיה האחראי הבלעדי על אבטחת המידע שהועבר או נצבר אצלו במסגרת ההתקשרות. בנוסף, הספק יהיה אחראי על אבטחת המערכות, התוכנות והחומרה המשמשת אותו לצורך אספקת השירותים או המוצרים למזמין, על תקינותם, אמינותם (integrity) ועל תפקודם השוטף והתקין. לצורך עמידת הספק בחובות אלו יתפעל הספק ויעדכן את אמצעי האבטחה באופן שוטף,

ויוודא כי האמצעים הטכנולוגיים המשמשים לאבטחת המידע הם עדכניים ועומדים בסטנדרטים המקובלים בתחום.

מבלי לגרוע מהאמור, ולצורך עמידה בחובותיו על פי טופס זה, מסכים הספק על שיתוף פעולה עם המזמין כמפורט בטופס זה, והכל לצורך ביצוע תקין של התקשרויות עם ממשלת ישראל.

מנכ"ל הספק או בעל התפקיד הבכיר בחברה יהיה הכתובת לכל פניה באשר לחובות הספק בהתאם לטופס זה, אלא אם מינה נציג אחר מטעמו והודיע על כך בכתב למזמין.

הספק מתחייב לתקן ליקויים שנמצאו על ידי המזמין בפרק זמן סביר ועל חשבונו, וכן מסכים כי אם לא יתקן ליקויים כאמור בפרק זמן סביר, יהווה הדבר הפרה יסודית של ההסכם, ויהווה עילה להפסקת התקשרות בכפוף לשימוע.

חובות הספק לפי טופס זה יחולו כל עוד מידע רגיש של המזמין שמור במערכותיו.

2. חובת דיווח

הספק מתחייב להודיע למזמין, בהקדם האפשרי, במהלך כל שעות היממה ובכל יום בשבוע, וללא שיהוי, על כל אירוע אבטחה אשר מסכן מידע או מערכות של המזמין או עלול להשפיע על יכולתו לעמוד בהתחייבויותיו נשוא ההסכם, ובפרט יודיע למזמין על האירועים הבאים:

אירוע אבטחה או ניסיון תקיפה סייבר אשר הביא לדלף מידע הקשור למזמין או לשיבושו של מידע או קוד תוכנה.

אירוע אבטחה או ניסיון תקיפת סייבר אשר עלול להביא לפגיעה במערכות המזמין, במערכות המסופקות לו, במידע של המזמין או בקוד המשמש אותו.

אירוע אבטחה או ניסיון תקיפת סייבר אשר מטרתו לאסוף מידע על המזמין.

דיווח זה יעשה באמצעות פרטי הקשר של המזמין אשר מפורטים להלן:

_____.

הספק מתחייב להודיע על אירועים כאמור בסעיף 3.1 גם למרכז הארצי לניהול אירועי סייבר (CERT) באחד מהאמצעים הבאים:

חיוג חירום מקוצר למרכז המבצעי לניהול אירועי סייבר במספר 119.

פניה באמצעות הדואר האלקטרוני: 119@cyber.gov.il.

במקרה כאמור, **על הספק להודיע למזמין על התרחשות האירוע ועל כל פרט נוסף ביחס לאירוע זה. חובה זו תחול גם אם אין ביד הספק את כלל המידע הרלוונטי, ועליו יהיה לעדכן את דיווחיו בהתאם למידע שיצטבר אצלו ולהנחיות המזמין.** על הדיווח לכלול לפחות את הפרטים הבאים:

תיאור כללי של האירוע, אופן התרחשותו, ציר הזמן הידוע של האירוע וכולי.

אופן הטיפול באירוע, והאמצעים הננקטים באופן מידי לצורך צמצום הנזק ומזעור החשיפה בטווח הזמן המיידי.

המערכות אשר נפגעו או היו היעד לתקיפה.

המידע אשר זלג, נפגע או שהיה היעד לתקיפה.

ניתוח דרכי התקיפה, החולשות ששימשו את התקיפה וכל מידע רלוונטי אחר.

פעולות מתקנות למניעת הישנות אירועים אלו בעתיד.

כל מידע אחר, שיידרש על ידי המזמין, לצורך ניתוח האירוע.

חובת הדיווח המפורטת בסעיפים 3.1 - 3.4 לעיל תוגבל למידע הרלוונטי למערכות הספק המשמשות למתן שירותים למזמין או מחזיקות במידע רגיש, ולא נדרש גילוי מידע של לקוחות או גורמים בלתי קשורים אחרים.

באחריות הספק לקבל התחייבות מגורמי שרשרת האספקה להודיע לו בהקדם האפשרי וללא שיהוי, על כל אירוע אבטחה אשר מסכן מידע או את מערכות המזמין ואשר עלול להשפיע על יכולת הספק לעמוד בהתחייבויותיו לפי ההסכם. הודעה כאמור צריכה לאפשר לספק להודיע על האירוע לאיש הקשר של המזמין, אשר פרטיו מופיעים בסעיף 3.2 לעיל.

3. ביקורת תקופתית

המזמין יהיה רשאי לבצע, אחת לשנה לכל היותר, ביקורת תקופתית על אודות עמידת הספק בדרישות הגנת המידע, הפרטיות והסייבר החלות על אספקת השירותים למזמין. ביקורת זו תתבצע בתיאום מראש ובהתאם למפורט להלן:

בקשת דוחות ודיווחים על אופן עמידת הספק בדרישות המכרז לאבטחת מידע והגנות סייבר.

במקרה שלדעת המזמין יש צורך באימות נתונים אלו או אחרים, יפעל המזמין בדרך המפורטת להלן:

המזמין יעביר לספק רשימה מסודרת של נושאים הדורשים בדיקה או אימות.

הספק יבצע את הבדיקות הנדרשות, על חשבונו, באמצעות גוף חיצוני, בלתי תלוי בספק והמאושר על ידי המזמין, ויעביר למזמין את דוח הבדיקה המקורי והמלא, כאשר הספק יהיה רשאי להשחיר בו אך ורק נתונים על אודות לקוחות אחרים. בכל מקרה, ממצאי הבדיקה וההמלצות יוגשו במלואם.

לחלופין, הספק יהיה רשאי לבקש מהמזמין כי המזמין יבצע בדיקה זו או אחרת כחלופה לביצוע הבדיקה על ידי גוף חיצוני, ובמקרה שהמזמין יסכים לביצוע בדיקה זו, יתאם את ביצועה עם הספק תוך הקפדה על קיום הבדיקה זו בהתאם לנושאים המוגדרים בסעיף 4.1.2.1. אין בביצוע בדיקה זו על ידי עורך המכרז בכדי להפחית אי אלו ממחויבויות הספק.

במקרה שהספק סבור כי יש בהעברת המידע או באופן ביצוע הביקורת חשש לפגיעה בתהליכי העבודה שלו, או בשירותים הניתנים ללקוחות האחרים שלו או שהיא כרוכה בעלויות כספיות לא פרופורציונאלית, יפנה למזמין לצורך תיאום אופן ביצוע הביקורת.

4. ביקורת בעקבות חשש לתקיפת סייבר

המזמין יהיה רשאי לבצע ביקורת בעקבות חשש לתקיפת סייבר המשפיעה על אספקת השירותים או המוצרים למזמין, בהתאם לאחד המסלולים המפורטים להלן:

מסלול א' – ביקורת על התמודדות הספק

המזמין יהיה רשאי לדרוש כל מסמך או פירוט לגבי אופן התמודדות הספק עם תקיפת הסייבר כמפורט בסעיף 3.2 לעיל או כל מידע אחר הנדרש על מנת להעריך את היקף ההשפעה על אספקת השירותים או המוצרים למזמין.

המזמין יהיה רשאי לדרוש מהספק לבצע כל בדיקה או פעולה סבירה במערכותיו של הספק המשמשות למתן השירותים לצורך בחינת התקיפה או על מנת לבחון קיום אירוע כאמור. כל מידע שיועבר לספק לצורך בדיקה זו הוא רגיש ואין להעבירו לכל גורם אחר ללא אישור המזמין.

במקרה שהמזמין, בהתייעצות עם הגורם המנחה, מצא כי אין די באמור בסעיפים לעיל על מנת להבטיח בצורה מספקת את הגנת המערכות או המידע של המזמין, או שמדובר במידע רגיש, או באירוע שיש לו השפעה על שירותים חיוניים, יהיה המזמין רשאי לקבוע כי במקביל לעבודת הספק, המשך הטיפול באירוע יהיה כאמור במסלול ב' כמפורט בסעיף 5.1.2 להלן.

מסלול ב' – סיוע של המזמין בהתמודדות עם האירוע

פעילות במסלול זה תהיה בכפוף להחלטת המזמין ובהתאם לשיקול דעתו הבלעדי, ובכפוף להסכמה מפורשת ובכתב של הספק, למעט במקרים המפורטים בסעיף 5.1.1.3, שבהם לא תידרש הסכמה מפורשת של הספק.

המזמין יסייע לספק בביצוע הפעולות המפורטות להלן, באופן ישיר ובאמצעות כלים העומדים לרשות המזמין ועל חשבונו:

בדיקת מערכות הספק הנוגעות למתן השירותים או לאספקת המוצרים.

בדיקת הנזקים או הסיכונים שנגרמו למזמין.

סיוע בהתמודדות עם אירוע האבטחה.

אבחון אופן התקיפה, המערכות שנפגעו והשפעתה על מתן השירות.

אבחון דרכים למנוע את המשכם והישנותם של הסיכונים שנגרמו למזמין ומתן הנחיות לספק בדבר הדרכים לצמצם סיכונים אלו וכלי.

אין בסיוע על ידי המזמין בכדי להפחית אי אלו ממחויבויות הספק. במקרה שהספק חושב שהנחיה מסוימת עשויה לפגוע ברמת האבטחה או בשירותים הניתנים על ידו, עליו להתריע על כך בצורה מפורשת לנציג המזמין.

הספק ישתף פעולה כמיטב יכולתו עם דרישות המזמין ויעמיד לרשותו כל מידע נדרש לצורך אבחון והתמודדות עם אירוע האבטחה או על מנת לוודא כי אירוע כאמור לא מתקיים. מידע זה יוגבל למידע הרלוונטי למערכות המזמין או המערכות המשמשות למתן שירותים למזמין, וללא גילוי מידע של לקוחות או גורמים בלתי קשורים אחרים.

במקרה שהספק סבור כי יש בהעברת המידע או באופן ביצוע הביקורת חשש לפגיעה בתהליכי העבודה שלו או בשירותים הניתנים ללקוחות האחרים שלו, יפנה למנהל מינהל הרכש הממשלתי לצורך תיאום אופן ביצוע הביקורת.

5. נציגי המזמין

לטובת ביצוע ההתחייבויות המפורטות בטופס זה המזמין יהיה רשאי להעביר את כלל המידע שהתקבל אצלו לידי הגורם המנחה וכן לידי מינהל הרכש, וזאת לצורך הערכת סיכונים וקביעת פעולות הנדרשות מהספק.

הגורם המנחה ומינהל הרכש יהיו רשאים לבוא במקום המזמין בכל סמכות הנתונה למזמין לפי טופס זה, והספק ישתף פעולה עם הנחיות שיתקבלו מהם לפי הוראות הטופס.

הגורם המנחה ומינהל הרכש יהיו מחויבים להשתמש במידע שיתקבל מהספק אך ורק לצורכים האמורים בטופס זה תוך גילויו לגורמים הנדרשים לכך בלבד.

6. כתובת לפניות בנושא אבטחת מידע והגנת סייבר

הודעות/פניות בנושא אבטחת מידע והגנת סייבר יועברו לספק באמצעות כתובת הדואר האלקטרוני הבאה: _____@_____

חתימת הספק:

_____	_____	_____
שם	תאריך	חתימה