הנחיות אבטחת מידע למכרז אספקת שוברי תשורה דיגיטליים או מגנטיים עבור הלשכה המרכזית לסטטיסטיקה

תוכן עניינים

1. הקדמה

1.1. רקע

1.1.1. הלשכה המרכזית לסטטיסטיקה (להלן: "הלמ"ס") מעוניינת בקבלת שירות מיקור חוץ להפקה והפצה של שוברי תשורות עבור שני השירותים הבאים:

1.1.1.1. נדגמים משיבים שענו על סקרים.

1.1.1.2. עובדי הלמ"ס באירועים מיוחדים שלהם או של ילדיהם.

1.1.2. הפרויקט יתבסס על שירותים טכנולוגים לצורך אספקת שירותי מסירת התשורות ובין היתר יתבסס על שירות כספות מול הלמ"ס ושירות API, שירות ניהול המסרונים מול מקבלי התשורות, העברת מידע רגיש מהספק ללמ"ס וניהול מאגר המידע של מקבלי התשורות.

1.2. מטרות

1.2.1. מסמך זה מגדיר את הנחיות אבטחת המידע ההכרחיות מהספק לצורך ביצוע הפרויקט והוא נספח מנדטורי בלתי נפרד מהמכרז.

1.3. היקף ומגבלות

1.3.1. הנחיות אלה נכתבו על פי הנחיות מערך הסייבר הלאומי, היחידה להגנה בסייבר (יה"ב).

1.3.2. נספח פיתוח מאובטח המצורף כנספח למסמך זה מקבל משנה תוקף בכל המקרים בהם הפתרון המוצע על ידי הספק אינו מוצר מדף מוגמר וכן במקרים בהם במוצרי מדף יתבצעו תהליכי פיתוח והתאמות קוד אשר יהיו ייחודיים עבור הלמ"ס.

1.3.3. תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017, הנחית רשם מאגרי מידע מס' 2011/2 שימוש בשירותי מיקור חוץ (outsourcing לעיבוד מידע אישי) של הרשות להגנת הפרטיות והנחיות שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי .

1.3.4. מסמך זה והנחיותיו הינו חלק בלתי נפרד מהמכרז והינו מנדטורי ומחייב. על אף האמור, ראש אגף הגנת הסייבר יהיה רשאי להקל בהנחיות המסמך במקרים חריגים ובהתאם לשיקול דעתו הבלעדי. על הספק להיערך לעמידה בהנחיות כלשונן ולא תישמע טענה מצדו שלפיה סבר כי תינתן לו הקלה כלשהי.

1.3.5. יתכן כי בעת מתן השירותים יועברו לספק המבצע הנחיות נוספות. ככל שיועברו הנחיות נוספות, יידרש הספק לפעול ליישומן. הספק יישא בכל עלות הנדרשת לצורך עמידה בהנחיות אלה וכתוצאה מאי עמידה בהנחיות מסמך זה וכן בכל עלות הנובעת משינוי, שיפור, או החרגה שנערכו לבקשתו.

1.3.6. הלמ"ס אינה מתחייבת לאשר בקשות להחרגה או הקלה החורגות מנספח זה.

1.4. אחריות

1.4.1. ראש אגף הגנת סייבר בלמ"ס – קביעה ההנחיות ובקרה על אופן יישומן.

1.4.2. מנהל הפרויקט – שילוב הנחיות המסמך במכרז לאספקת השירות.

1.4.3. אגף מערכות מידע בלמ״ס – פיתוח, הקמה והתאמת תשתיות הלמ״ס לצורך שילוב הספק ומתן מענה לצרכים העסקיים.

1.4.4. הספק הזוכה – עמידה מלאה בהנחיות נספח זה לצורך מתן מענה לצרכים העסקיים.

1.5. מונחים

1.5.1. **ספק מיקור חוץ** : ספק שירות חיצוני עמו תתבצע התקשרות לצורך מתן השירותים הנדרשים לפי מכרז שוברי תשורה. . .

1.5.2. **ערוצי מידע:** ערוצי מידע ומדיה בהם יבוצע שימוש במסגרת השירות לדוגמה : אפליקציות מסרים או שירותי SMS.

2. סוגי הפתרונות באמצעותם ימומש הפרויקט

הפתרון	פירוט הפתרון	סוג המידע המוחזק אצל הספק	שיטת העברת מידע לספק ומהספק ללמ״ס	שיטת העברת מידע בין הספק לזכאים לתשורה
שירותי מיקור חוץ באמצעות ספק שירותים (אזרחים, סקרים)	הספק יספק : 1. תשתיות לצורך מסירת שוברי תשורה לאזרחים אשר השיבו על שאלוני סקרים 2. ממשק תכנותי (API) להעברת מידע על משיבי הסקרים באופן רציף 3. תשתית להעלאת קבצים ידנית עם נתוני התשורה ומעקב אחרי העברתם וקבלתם **4.** אפשרות למעקב אחרי ניצולי התשורה באופן גורף	בשיטה זו יועבר לספק מידע רגיש (טלפון המוגדר כמידע רגיש מזהה פרט). מאפייני מנה, פרטי הזכאות גובה הזכאות, פרטי זכאים , מיילים וטלפון ליצירת קשר	1. ממשק API דו-כיווני מאובטח אשר יפותח על ידי הספק ויאפשר העברת פרטי זכאים באופן שוטף מיד אחרי סיום ההשבה 2. ממשק API דו-כיווני מאובטח אשר יפותח על ידי הספק ויאפשר צפייה בניצול התשורות	שליחת הודעות סמס\ מייל \ קולי
שירותי מיקור חוץ באמצעות ספק שירותים (עובדי הלמ״ס, רווחה)	הספק יספק : 1. תשתיות לצורך מסירת שוברי תשורה דיגיטליים לעובדים באירועים מיוחדים 2. תשתית להעלאת קבצים עם נתוני התשורה ומעקב אחרי העברתם וקבלתם 3. אפשרות למעקב אחרי ניצולי התשורה	שם פרטי של העובד שם משפחה של העובד 6 ספרות אחרונות של תעודת זהות של העובד ,מספר טלפון של עובד תאריך לידה של העובד, חודש לידה של ילדי העובד	1. ממשק משתמש מאובטח אשר יפותח על ידי הספק ויאפשר קליטת קבצים ידנית ומעקב אחרי העלאתם, וצפייה בניצול התשורות	שליחת הודעות סמס\ מייל \ קולי

3. הנחיות התקשרות עם הספק

3.1. הנחיות הרשות להגנת הפרטיות

3.1.1. הספק והמענה המוצע על ידו יעמדו בהנחיות הרשות להגנת הפרטיות הבאות:

3.1.1.1. תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-1.2017 לרבות תיקון 13.

3.1.1.2. הנחית רשם מאגרי מידע מס' 2011/2 שימוש בשירותי מיקור חוץ outsourcing (לעיבוד מידע אישי) של הרשות להגנת הפרטיות.

3.1.1.3. הגדרת שירותי ענן כמיקור חוץ (Outsourcing) – תקנה 15 לתקנות הגנת הפרטיות.

3.1.1.4. טיוטת הנחיית הרשות להגנת הפרטיות בעניין תחולת הוראות חוק הגנת הפרטיות על מערכות בינה מלאכותית לכשתקבל תוקף וככל שיעשה שימוש במערכות בינה מלאכותית לעיבוד מידע רגיש המוגדר על פי התקנות.

3.2. כוח אדם מוקצה לפרויקט

3.2.1. הלמ"ס רואה בעובדי הספק וכן בקבלני המשנה של הספק ואלה יוגדרו כ"עובדי הספק" לצורך נספח הנחיות זה, כזרוע נוספת מטעם הספק. לפיכך יחולו כל החובות וההנחיות גם על עובדים הומוגניים של הספק הזוכה וגם על קבלני המשנה של הספק.

3.2.2. הספק יעביר את רשימת העובדים והספקים המורשים על ידו בביצוע השירותים לרבות עובדי תשתיות ומערכות מידע הנחשפים למידע.

3.2.3. כל העובדים בפרויקט, יחתמו על התחייבות לשמירה על סודיות ויחתים כל אחד מעובדיו המעורב בביצוע השירותים, על כתב סודיות זה.

3.2.4. הספק יעדכן את הלמ"ס בכל שינוי בהוספת עובדים או ספקים חדשים אשר עלולים להיות או חשופים למידע של הלמ"ס.

3.2.5. הספק יוודא הסרת הרשאות גישה לעובדים וספקים שאינם נדרשים בגישה למידע.

3.2.6. הספק יעביר תצהירים לנושא היעדר רישום פלילי עבור כלל העובדים אשר יפעלו מטעמו במסגרת הסקרים וכן מסמכים נוספים שידרשו על ידי קב"ט הלמ"ס.

3.2.7. כל העובדים והספקים בפרויקט או עובדים שיהיו חשופים למידע יאושרו על ידי קב"ט הלמ"ס וראש אגף הגנת הסייבר. קב"ט הלמ"ס או ראש אגף הגנת הסייבר בלמ"ס יהיו רשאים לסרב לתת את הסכמתם להעסקת עובד פלוני של הספק הזוכה ו/או מי מטעמו מכל טעם שימצא לנכון, ומבלי שיהא עליו לנמקו.

3.2.8. לא תתקיים גישה למידע של הלמ"ס בגישה של ספקים צד ג' ללא אישור הלמ"ס.

3.2.9. לא יועבר מידע ו/או יאוחסן מידע אצל ספקים צד ג' ללא אישור הלמ"ס.

3.3. רפרנטים לנושאי אבטחת מידע והגנה בסייבר

[1] https://www.nevo.co.il/law_html/law00/14 4811.htm#Seif15

3.3.1. על מסמך הנחיות אבטחת המידע יחתום בנוסף, **ממונה אבטחת המידע ו/או ממונה אגף הגנת הסייבר מטעם המציע בעל כתב מינוי בתוקף (יש לצרף את כתב המינוי בתשובה להצעה)**. הוא יחתום כי הוא נושא באחריות לעמידה בהנחיות נספח זה וכי הוא מתחייב לפעול ליישום כלל הנחיות אבטחת המידע והגנת הסייבר המפורטות במסמך זה.

שם: _____ משפחה: _____ תפקיד: _____

ת.ז: _____ חתימה: _____ תאריך: _____

4. ניהול סיכונים בשרשרת האספקה

4.1.1. על פי הנחית יה"ב [2] (יחידת ההגנה בסייבר) לניהול ספקים בשרשרת האספקה של משרדי הממשלה ויחידות הסמך -מס' 5.19 מיום 14.11.2019 **הספק וקבלני משנה מהותיים** (כגון: ספקים מהותיים כגון ספקי תשתיות מחשוב, פיתוח, ספקים המחזיקים או ניגשים למידע תפעולי, ספקים הנגישים למידע של הלמ"ס) **המעורבים או עלולים להיות מעורבים בפרויקט**, נדרשים בביצוע סקר ספק הסייבר להתעדה ברמה ב' (B) [3] לפי מערכת "יוב"ל" של מערך הסייבר הלאומי. הספק יוכל לבחור האם לבצע את השאלון באמצעות בודק מאושר מטעם מערך הסייבר הלאומי [4] או באמצעות מילוי עצמי וזאת על פי שיקול דעתו. הסקר יעשה למול שאלון מערך הסייבר העדכני ביותר במערכת יעדים ובקרות לארגון (יוב"ל): https://www.gov.il/he/departments/news/querysupply.

4.1.2. ספק אשר מופיע ברשימת הספקים המאושרים של מערך הסייבר או ביצע תהליך התעדה בתקופה של עד שנה מיום זכית הספק במכרז, יוכל להציג את האישור וכך לפטור עצמו מביצוע סקר נוסף. ובתנאי שהאישור בתוקף לרמת ההתעדה הדרושה על פי נספח זה (רמה B או A) ונעשתה על ידי בודק מאושר מטעם מערך הסייבר.

---

[2] https://www.gov.il/he/departments/guides/supply_chain_guide?chapterIndex=7

[3] https://www.gov.il/he/departments/general/expsupplychain - ראה קבצי הרחבה להורדה בנושא הגנת סייבר בשרשרת האספקה – דגשים עבור צד לקוח – הרחבה מקצועית.

[4] https://www.gov.il/he/departments/guides/supply_chain_guide?chapterIndex=4

4.1.3. ככל שהספק (או הספקים) לא ביצע תהליך התעדה ואינו מופיע ברשימת הספקים המאושרים לרמה B או A, אזי לאחר הזכייה במכרז, מתחייב הספק לבצע סקר בשלות סייבר על בסיס שאלון יוב"ל (יעדים ובקרות לארגון) של מערך הסייבר הלאומי ו**<u>להשלים את התהליך עד מועד אספקת השירות בפועל על פי המכרז</u>**. חריגה מלוחות הזמנים להשלמת תהליך ההתעדה תתבצע בתיאום עם הגורם המזמין בלמ"ס ואגף הגנת הסייבר. יחד עם זאת, מובהר לספק כי הלמ"ס אינה מתחייבת לחרוג מלוחות הזמנים שהוגדרו ליעדי הפרויקט.

4.1.4. הספק יעביר את תוצאות הסקר (או הסקרים) והאסמכתאות שצורפו לסקר, לראש אגף הגנת הסייבר בלמ"ס ולמנהל הפרויקט מטעם הלמ"ס.

4.1.5. **<u>נדגיש:</u>** לא תאושר פעילות מול הספק ולא יימסר מידע לספק – עד להשלמת השאלון והפערים שיתגלו במסגרתו – אלא במקרים חריגים בלבד ובאישור ראש אגף הגנת הסייבר בלמ"ס. כמו כן הלמ"ס לא תוכל להסתפק בהצהרות בדבר עמידה בתקני אבטחה ISO.

4.2. סקרי בטיחות לעמידה בתקנות הגנת הפרטיות

4.2.1. עמידה בחוק הגנת הפרטיות ותקנותיו:

4.2.1.1. הספק יחזיק/ינהל מידע רגיש ומחויב לעמידה בתקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017. במסגרת זו על הספק לבצע סקר סיכונים לעמידה בתקנות הגנת הפרטיות במלואן עבור כל אחד מהשירותים המוצעים המנוהלים על ידו.

4.2.1.2. הספק יידרש להצהיר (לפני הזכייה במכרז) כי הוא עומד בחוק הגנת הפרטיות ובתקנותיו במלואם בטרם אספקת השירות ללמ"ס.

4.2.1.3. סקר בטיחות (סיכונים) טכנולוגי:

4.2.1.4. מערכות הספק יידרשו לעמוד בסקר סיכונים ו/או בדיקת חדירות לשירותי התשתית והאפליקציה.

4.2.1.5. במסגרת הסקרים ייבחנו פערים ביישום הטכנולוגיות וההנחיות למול הנחיות מסמך זה. הסקרים ותחולתם יעשו באחד מהאופנים הבאים:

4.2.1.6. סקר מקיף - לפני הפעלת השירות וכן בכל עלייה לייצור של כל סביבה ו/או שירות (בדגש על שירותים מהותיים).

4.2.1.7. במידה ויעשה **שינוי מהותי (נתון לשיקול ראש אגף הגנת הסייבר בלמ"ס)** או במידה והפעילות תורחב לתקופה של מעל 18 חודשים, יבוצע סקר מחזורי לאחר 18 חודשים מיום ביצוע הסקר הראשון.

4.2.1.8. סקר חלקי - במקרה בו הספק יבצע שינוי במבנה הרשת ו/או עדכון תוכנה/אפליקציה (למשל עדכון גרסה) ו/או שינוי בקוד, טכנולוגיה חדשה וכיו"ב. כמו כן הספק מתחייב לעדכן את הלמ"ס בכל שינוי כזה.

4.2.1.9. סקר ממוקד סיכון - במקרים בהם פורסמה ו/או הועברה על ידי אגף הגנת הסייבר בלמ"ס ידיעה על הימצאות חולשה או סיכון מהותי אשר עלול להשפיע על הגנת הסייבר בפרויקט, יבוצע סקר חלקי על האזורים ו/או הטכנולוגיות שעלולות להיות מושפעות מהחשיפה.

4.2.1.10. הסקרים יעשו באופן ידני, וכן באופן ממוכן באמצעות כלי סריקה וניתוח ממצאים. לצורך בדיקות קוד יבצע הספק בדיקות (Code Review) באופן אפקטיבי (ידני או ממוכן).

4.2.2. ככל שיתגלו סיכונים, תידרש הלמ"ס לבצע הערכת סיכונים, לבחון ולהגדיר את אופן הטיפול בהם בטרם הפעלת השירות.

4.3. סקר חצרות ספקים שיבוצע ע"י הלמ"ס

4.3.1. הספק מאשר ומסכים כי הלמ"ס או מי מטעמה, תבצע הערכת סיכון וסקר בחצרותיו ובחצרות ספקים וקבלני משנה ונותני שירות צד ג' אשר יגישו מועמדות לשירות, בהתאם לשיקול דעתה הבלעדי של הלמ"ס.

4.3.2. סקר חצרות ספקים אשר יבוצע על ידי הלמ"ס ו/או מי מטעמה, יכלול בדיקות אבטחה פיזית, לוגית, הקשחת מערכות, ארכיטקטורה, ניהול משתמשים והרשאות, בדיקות אפליקטיביות, אחסון מידע וכדומה. הספק מחויב לתיקון ממצאים שיתגלו במסגרת סקר הספקים ובפרט ממצאים אשר עלולים לפגוע בלמ"ס או במידע שלה בהיבטי סודיות, זמינות ואמינות.

4.3.3. הספק מסכים ומאשר כי ידוע לו כי יתכן שסקרים נוספים יוכלו להתבצע גם על ידי מערך הסייבר הלאומי ו/או מי מטעמו שהוסמך לכך. הספק ישתף פעולה עם סקרי בטיחות שיתקיימו באופן מחזורי ע"י אגף הגנת הסייבר של הלמ"ס ויעמוד בלוחות הזמנים שייקבעו לתיקון הליקויים שימצאו בסקרי הבטיחות כאמור.

4.4. מענה לליקויי אבטחה וסייבר

4.4.1. הספק מסכים, כי ככל שיעלו ממצאים במסגרת הערכת הסיכונים או סקר חצרות הספק ו/או על פי מסקנות דוח מערכת יוב"ל ו/או סקר מערך הסייבר הלאומי, הן בחצרותיו והן אצל קבלני משנה שלו, יתחייב הספק לפעול לתקנם מידית בחצרותיו (ובחצרות ספקים, קבלנים ונותני שירות צד ג').
לגבי אופן הטיפול, יידרש הספק לספק אסמכתאות וכתב התחייבות החתום ע"י מורשה חתימה המפרט את אופן הטיפול בממצאים, וכן התחייבות כי ממצאי הסקר טופלו במלואם. ממצאים חריגים או חריגה מאופן טיפול הליקויים יובאו לאישור ראש אגף הגנת הסייבר בלמ"ס ויהיו נתונים לשיקולו הבלעדי.

4.4.2. הספק וקבלני המשנה, מודעים לכך כי עיכוב בתיקון הליקויים שיתגלו במסגרת תהליך הערכת הסיכון ו/או סקר חצרות ספקים, או מתן מענה חלקי לסיכונים שיתגלו, עלול למנוע ממנו מלספק או להמשיך לספק שירות ללמ"ס וכן בפיצוי הלמ"ס.

4.4.3. ממצאים הנובעים מפערים בשאלון יוב״ל וממצאים בסיכון גבוה יטופלו עד 3 חודשים ובטרם אספקת השירות.

4.4.4. הספק וקבלני המשנה יסכימו כי הלמ״ס או מי מטעמה תהא רשאית בכל עת, לבצע ביקורות, לרבות ביקורות פתע.

4.4.5. הלמ״ס (או מי מטעמה) תהא רשאית לבצע סקרים חוזרים בחצרות הספק במועדים משתנים לרבות ביקורות פתע.

4.4.6. בהסכם השירות עם הספק יצוין כתנאי מתלה – כי במידה וספק השירות ו/או קבלן המשנה, אינו פעל לתיקון הליקויים המהותיים / ממצאי יוב״ל, מיום תחילת אספקת השירות, יפסק הסכם השירות עם הספק ו/או קבלן המשנה באופן מיידי. חריגים יאושרו על ידי ראש אגף הגנת הסייבר בלמ״ס.

4.4.7. בהסכם השירות יצוין תנאי יסודי מפסיק, כי אם במהלך אספקת השירות, יתגלה סיכון גבוה נוסף, רשאית הלמ״ס להפסיק את השירות מול הספק ו/או קבלן המשנה, עד לתיקון מלא של הליקוי שהתגלה.

4.4.8. הספק מאשר כי במקרים בהם הסיכונים והממצאים לא קיבלו מענה המניח את הדעת של אגף הגנת הסייבר בלמ״ס, רשאי ראש אגף הגנת הסייבר בלמ״ס למנוע פעילות מול הספק.

4.4.9. הספק מאשר ומסכים כי הלמ״ס או מי מטעמה יוכלו, בכל שלב, לבצע סקר סיכונים טכנולוגי בכל נושא שימצא על ידה כרלוונטי לניהול הסיכונים שלה ובין יתר: תשתית, אפליקציה, מערכות תקשורת, מערכות אבטחת מידע, אבטחה פיזית ורשת בטחון פיזי (בקרת כניסה, מצלמות, אזעקה וכיו״ב).

4.5. הערכה וניהול סיכונים לספקים אשר לספק אין שליטה ישירה עליהם

4.5.1. במקרים בהם לא ניתן לבצע סקר סיכונים בחצרות הספק על בסיס הנחיות יוב״ל (לדוגמה ספקי חו״ל, ענן בחו״ל, ערוצי מידע חיצוניים/מסרים), יקיים הספק סקר מתודולוגי להערכת סיכונים בשימוש עם ספקים, על בסיס שאלון יוב״ל, ויוודא קיום של בקרות מפצות חוזיות אפקטיבית להתמודדות עם הסיכונים שיתגלו במסגרת סקרים אלה.

4.5.2. הבקרות והסכמי ההתקשרות עם ספקי צד ג׳ (לחילופין יועבר מסמך נוחות חתום על ידי רו״ח מבקר) יועברו לבחינת המחלקה המשפטית בלמ״ס לצורך בקרה לעמידה בתקנות הגנת הפרטיות של מדינת ישראל והנחיות נספח זה. **נדגיש כי הצהרות בדבר עמידה בתקני אבטחה ISO, אינן מספקות מענה שלם והלמ״ס לא תוכל להסתמך רק על תקנים אלה.**

4.5.3. ככל שיתגלו פערים מול ספקי צד ג׳, הפערים יועברו לידי המחלקה המשפטית ואגף הגנת הסייבר בלמ״ס לצורך מסירת הנחיות נוספות. הלמ״ס אינה מתחייבת לאשר פעילות עם ספקים שלא יעמדו בהנחיות.

4.6. סקרי בטיחות שיעשו על ידי הלמ״ס

4.6.1. בטרם אישור הפעלת השירות הלשכה המרכזית לסטטיסטיקה תהיה רשאית לבצע בדיקות אבטחת מידע של הלמ"ס ובדיקות אבטחת המידע לשירות.

4.6.2. הבדיקות תעשנה לאחר הקמה מלאה של השירות ולאחר בדיקות QA (ובטרם מסירת מידע רגיש לספק). הספק יעדכן את הארכיטקטורה והמסמכים הדרושים וכן ירכוש פתרונות אבטחה בהתאם לממצאי הבדיקות.

4.6.3. הלמ"ס רשאית, בכל עת, לבקר את מערכות המידע של הספק הזוכה בהן נמצא מידע שהתקבל מהלמ"ס או נוצר במהלך ההתקשרות, בהתאם לשיקול דעתה הבלעדי של הלמ"ס. על הספק הזוכה להעמיד לרשותה ולעיונה של הלמ"ס ו/או נציג מטעמה את כל החומר והמידע שידרשו ע"י הלמ"ס ו/או נציגיה, עפ"י שיקול דעתה הבלעדי של הלמ"ס ו/או נציגיה.

4.6.4. ביצוע הסקרים מטעם הלמ"ס לא ישחרר את הספק הזוכה מהתחייבויותיו ואחריותו כלפי הלמ"ס למילוי ההנחיות וההוראות בנושא אבטחת המידע בהתאם לתנאי מכרז זה.

4.6.5. הספק יתחייב לתקן ממצאים שהתגלו לפני הפעלת השירות ודורגו בסיכון גבוה לפני הפעלת השירות.

4.6.6. כמו כן במידה ויאותרו סיכונים בסיכון גבוה במהלך ההתקשרות עם הספק, מתחייב הספק לתקנם באופן מידי. חריגים יאושרו על ידי ראש אגף הגנת הסייבר בלמ"ס.

4.6.7. הספק מאשר כי במקרים בהם הסיכונים והממצאים לא קיבלו מענה המניח את הדעת של אגף הגנת הסייבר בלמ"ס, רשאי ראש אגף הגנת הסייבר בלמ"ס למנוע פעילות מול הספק.

5. הגנה על המידע והגנת הפרטיות

5.1. נהלים ומדיניות

5.1.1. הספק יקיים נהלים ומדיניות להגנה מפני הפרות אבטחת מידע ויציג אותם ללמ"ס על פי דרישתה מעת לעת.

5.1.2. הספק יקיים מדיניות לפיה ייעשה שימוש במידע של הלמ"ס רק לצורך המטרה שהוגדרה בסעיף 1.1.1, בהתאם לעקרון צמידות המטרה בחוק הגנת הפרטיות.

5.2. איסור הצלבה והעשרת מידע

5.2.1. הספק לא יצליב, יקשר, יאחד או יעשיר את המידע שהתקבל מהלמ"ס באמצעות מידע ממקורות אחרים, אלא אם הדבר נדרש במפורש לביצוע השירותים ואושר מראש ובכתב על ידי הלמ"ס.

5.2.2. הספק לא ינסה לזהות מחדש אדם שמידע לגביו הותמם, הוצפן, קודד או הוסרו ממנו פרטים מזהים.

5.3. צמצום מידע ואיסור איסוף מידע עודף

5.3.1. הספק יאסוף, יקבל, יעבד וישמור רק את המידע המינימלי הנדרש לצורך ביצוע השירותים.

5.3.2. הספק לא יאסוף, יעתיק, ישמור או יעבד מידע שאינו נחוץ למטרה שהוגדרה בהסכם.

5.3.3. ככל שהתקבל אצל הספק מידע עודף, מידע שגוי, מידע שלא היה אמור להימסר לו או מידע שאינו נדרש עוד לביצוע השירותים, הספק יודיע על כך ללמ״ס ללא דיחוי ויפעל בהתאם להנחיותיו.

5.4. מסירה וקבלת מידע מהספק

5.4.1. הלמ״ס תעביר לספק ותקבל ממנו מידע רגיש. המידע שיועבר לספק יכלול את סוגי המידע הבאים:

5.4.1.1. מידע על אזרחים / נדגמים: מידע זה יכלול שם, שם פרטי, מספר טלפון, כתובת מייל ואת שם הסקר בו ענו של אזרחים אשר יסיימו את תהליך מילוי שאלוני השבה.

5.4.1.2. מידע על עובדי הלמ״ס ובני משפחותיהם: מידע זה יכלול שם פרטי ושם משפחה של עובד, 6 ספרות אחרונות של תעודת הזהות של העובד, תאריכי לידה של העובד וחודש לידה של ילדיו, מספר טלפון של העובד. אין להעביר לספק כתובת מייל אישית או אירגונית של עובד. שליחת שוברים לרגל אירועים מיוחדים של ילדי העובדים ייעשו בצירוף נוסח גנרי שלא חושף פרטים אישיים על ילדי העובדים.

5.4.2. העלאת ידנית של מידע, צפייה או חיפוש של מידע, ומעקב אחר קבלה יתבצעו דרך הממשק המאובטח. הספק יספק משתמשים עם סוגי הרשאות שונות:

5.4.2.1. **הרשאה למחלקת רווחה** מנהלן רוחה, הרשאות צפיה, הרשאות טעינה - לצורך טיפול בתשורה של אוכלוסיית העובדים: העלאת קבצים ידנית ומעקב.

5.4.2.2. **הרשאת לחטיבת האיסוף** מנהלן איסוף, הרשאות צפיה, הרשאות טעינה – לצורך טיפול בתשורה של אוכלוסיית המשיבים – העלאת קבצים ידנית ומעקב אחר מידע שהגיע מקבצים וממשקים

5.4.2.3. **הרשאת מנהלן** – לטיפול בתשורה כללי ולמעקב אחר אוכלוסיות משיבים ועובדים (מקבצים וממשקים).

5.4.3. הספק יעביר ללמ״ס היזון חוזר בעת ניצול שוברים (או כשל במימוש). כל התקשורת בין הלמ״ס לספק תתבצע באמצעות ממשק API מאובטח להעברת המידע על תנועת וסטטוס השוברים.

5.4.3.1. העברת המידע תתבצע באופן שלא ניתן לעריכה כדי למנוע התערבות לא רצונית בתכנים שימסרו על ידי הספק (שיבוש מידע, זיוף או הסתרת פעולות, הכחשת שימוש בשוברים).

5.4.3.2. סוג המידע שיועבר מהספק אל הלמ״ס בנוגע לניצולים יהיה בהתאם לשדות המידע שהוגדרו בנספח הטכנולוגי של המכרז, ואין להעביר מידע פרטי נוסף על זכאים ללא בקשה מפורשת של הלמ״ס

5.4.3.3. יש לתכנן רמות גישה שונות ומתאימות לצפייה בנתוני הניצולים לפי סוג השובר. לדוגמא – משתמש מאגף רווחה יקבל הרשאות למשוך נתוני ניצול על שוברים שניתנו לעובדי הלמ"ס בלבד)

5.5. העברת מידע מחוץ לגבולות מדינת ישראל

5.5.1. הספק יפעל על פי תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס"א-2001, (להלן- 'התקנות') ויוודא שלא מועבר מידע ממאגרי מידע במדינה אל מחוץ לגבולותיה אלא בתנאים המפורטים בתקנות הגנות ובאישור בכתב מהמחלקה המשפטית וממונה הגנת הפרטיות, בלמ"ס.

5.5.2. ככל שיינתן אישור לכך אזי העברת המידע תתבצע בהתאם למפורט בסעיף 8.3 "מיקום גיאוגרפי ותחומי שיפוט" כאמור במסמך הנחיות ראש רשות התקשוב הממשלתי הנחיות היחידה להגנת הסייבר בממשלה – יה"ב (מספר הנחיה 5.5) ומודגש כי רק ממדינות מאושרות (לפי הנחיות של הרשות להגנת הפרטיות). הלמ"ס אינה מתחייבת לתת אישור להוצאת מידע מחוץ לגבולות מדינת ישראל.

5.6. שירותי Hosting וענן.

5.6.1. הספק יוכל לעשות שימוש בשירותי ענן ו/או Hosting לצורך מתן השירותים או באמצעות מערכות פנימיות של הספק המותקנות בחצרותיו (On-Premise).

5.6.2. בכל השירותים (ענן, Hosting, On-Premise) יידרש הספק בהגנה **משולבת** על המידע באמצעות הקשחת המערכות, הצפנה אפליקטיבית והצפנת תשתית (דוגמת TDE במערכות SQL).

5.6.3. בנוסף יפריד הספק את שרתי ה- SQL / Database יהיו בנפרד משרתי האפליקציה.

5.7. שימוש בשירותי ענן

5.7.1. הספק מסכים ומצהיר כי כל שירותי הענן ושירותי הגיבויים אשר יסופקו על ידו (לרבות שירות תמיכה צד ג' ושימוש בקבלני משנה) וכן מידע אישי, לרבות מספרי תעודת זהות ותאריכי לידה, כלל הנתונים, לרבות גיבויים, שכפולים ועיבודים יעשו במדינת ישראל בלבד או בסביבת נימבוס או בכפוף לאישור להעברת מידע מחוץ לגבולות מדינת ישראל ובהתאם למפורט בסעיף 8.3 "מיקום גיאוגרפי ותחומי שיפוט".

5.7.2. ובכל מקרה לא יאושר שימוש בשירותי ענן המאוחסנים או מנוהלים ממדיניות העוינות לישראל או ממדינות אשר לישראל אין קשרים דיפלומטיים עימן.

5.7.3. כל שימוש בשירותי ענן ו/או Hosting יאושר באופן פרטני על ידי ראש אגף הגנת הסייבר בלמ"ס.

5.7.4. כל שירות ענן יצריך עמידה מלאה בתקנות ISO270017, ISO270018 ו- GDPR. ע"מ לוודא עמידה בהנחיה זו, מתחייב הספק להעביר אסמכתא או תצהיר לעמידה מלאה בהנחיות אלה (וללא פערים מהותיים).

5.8. מסירת מידע לספק

5.8.1. העברת מידע רגיש (עסקי או תפעולי וכן מידע לגבי זכאים לתשורות והיזון חוזר (מעקב אחר ניצול תשורות וכדומה) בין הספק ללמ"ס ולהיפך, תעשה באמצעות ממשק מאובטח כמו ממשקי API או כספות.

5.8.2. כל תכתובת המכילה מידע מסווג (עסקי או תפעולי) תתבצע בערוץ תקשורת מאובטח.

5.8.3. על הספק להעמיד אמצעי הגנה וניטור אפקטיביים בכל תהליך העברת מידע בתנועה.

5.9. אחסון מידע בחצרות הספק

5.9.1. הספק רשאי לעשות שימוש בתשתיות פיזיות משותפות כגון תשתיות: אחסון, גיבוי, עיבוד וניהול מידע של הלמ"ס. יחד עם זאת, על הספק ליישם אמצעי הפרדה והגנה אפקטיביים אשר ימזערו ככל הניתן סיכוני סייבר בעלי השפעה על המידע או השירות הניתן ללמ"ס ובין היתר: מניעת חשיפת מידע לגורם לא מורשה ולקוחות אחרים של הספק, בין היתר באמצעות הצפנה ייעודית, ניהול הרשאות גישה קפדניות, מידור תקשורתי, אבטחת מערכות הרשת, המחשוב והאפליקציות, סיווג ומניעת דלף מידע ופעילות פרו-אקטיבית אפקטיבית איתור סיכוני סייבר.

5.9.2. הספק יקיים הפרדה בין סביבות חיצוניות, סביבות נמוכות (פיתוח, בדיקות) לבין סביבות הייצור בהן קיים מידע של הלמ"ס.

5.9.3. הספק יפריד באופן אפקטיבי, בין שירותים הניתנים ללמ"ס (ובין היתר מידע של נדגמים משיבים ועובדי הלמ"ס ובני משפחותיהם) למידע של ארגונים ולקוחות אחרים של הספק.

5.9.4. הספק לא יבצע כל פרסום של מידע הקשור ללמ"ס אלא אם ניתן אישור מכך על ידי הלמ"ס במסגרת הסכם ההתקשרות או מידע שהועבר על ידי אגף הגנת הסייבר ו/או נקבע אחרת בהסכם ההתקשרות.

5.10. שמירה על מידע ומניעת דלף

5.10.1. הספק יגן על מידע של הלמ"ס בעת שינוע המידע ובעת אחסון המידע.

5.10.2. בכל המקרים בהם יועבר מידע רגיש לספק ובין היתר מזהים אישיים כגון: מספר תעודת זהות, טלפון, כתובת דואר, כתובת דוא"ל, תפקיד (עבור עובדי הלמ"ס). מזהים אלה ידרשו להיות מוצפנים או מגובבים (Hashed) במערכות הספק והן בתנועה של המידע, לדוגמה:

5.10.2.1. הספק ישמור את מספרי תעודות הזהות במנגנון Hash חד-כיווני (עם Salt) אלא אם נדרש שימוש תפעולי המחייב הצפנה הפיכה.

5.10.2.2. הספק ישמור את מספרי הטלפון, כתובות דוא"ל, מזהים אישיים שמצריכים פענוח לצורך יישום התהליך העסקי, באופן מוצפן במשך כל תקופת האחסון.

5.10.2.3. חל איסור לשמור מזהים אישיים ב- clear text (ללא הצפנה או גיבוב).

5.10.2.4. על הספק לעשות שימוש במנגנון מתקדם, בניהול הספק, לניהול מפתחות ההצפנה / הגיבוב.

5.10.3. על הספק להגן מפני דלף מידע מזהה פרט באמצעות כלים מתקדמים לאיתור וסיווג מידע רגיש (Data Classification) ומניעת דלף מידע רגיש (Data Leakage Prevention).

5.10.4. על הספק להימנע ככל הניתן משמירת מידע עודף ולפעול להסרתו בהתאם להנחיות הלמ"ס.

5.11. אי מסירת מידע לצד ג' (שאינו הספק)

5.11.1. הספק לא ימסור את המידע לצד ג' (שאינם צד הרכש/השובר) ללא אישור בכתב מאגף הסייבר והמחלקה המשפטית של הלמ"ס.

5.12. שירותי בינה מלאכותית

5.12.1. הספק לא יזין מידע רגיש של הלמ"ס או מזוהה עם הלמ"ס והשירות הניתן, למערכת בינה מלאכותית, למודל שפה, למערכת למידת מכונה, לכלי פיתוח מבוסס בינה מלאכותית או לשירות מקוון חיצוני, אלא אם השימוש אושר מראש ובכתב על ידי הלמ"ס.

5.12.2. הספק לא ישתמש במידע לצורך אימון, טיוב, הערכה או בדיקה של מודלים או אלגוריתמים שאינם מיועדים באופן בלעדי לביצוע השירותים עבור הלמ"ס.

5.12.3. האיסור יחול גם על מידע מותמם, מדוגם, חלקי או מסווג, אלא אם הלמ"ס אישר במפורש את סוג המידע ואת אופן השימוש בו.

5.12.4. הספק יערך ליישום הנחיית הרשות להגנת הפרטיות בעניין תחולת הוראות חוק הגנת הפרטיות על מערכות בינה מלאכותית.

5.13. מדיה פיזית

5.13.1. הספק לא יאחסן מידע של הלמ"ס באמצעי מדיה נתיקה או דפוס.

5.13.2. הספק יקיים נהלים להשמדה של מדיה מגנטית ואופטית לרבות כוננים קשיחים, אמצעי אחסון ניידים או נתיקים, מצעי גיבוי וכן מידע דפוס בסיום ההתקשרות עם הלמ"ס ויציג אותם ללמ"ס על פי דרישתה על פי צורך.

5.14. הלבנת מידע

5.14.1. כל קובץ (בין אם מהלמ"ס או מצד ג') אשר יועבר לסביבת המחשוב ולמערכת ניהול השוברים, מחוייב לעבור תהליך הלבנה ו- CDR של הספק.

5.15. השבת מידע בעת סיום התקשרות עם ספקים

5.15.1. בעת סיום התקשרות עם הספק ועל פי דרישה בכתב של הלמ"ס, באחריות הספק הזוכה ו/או המפעיל את השירות לחסום ולהסיר את הרשאות הגישה אשר נפתחו לספק ולעובדיו במערכות המחזיקות מידע של הלמ"ס.

5.15.2. באחריות הספק להשיב כל מידע שנמסר להם לרבות מידע לוגי, פיזי וכיו"ב וכן מידע נלווה / תוצרים שהופקו במהלך תהליך ההתקשרות.

5.15.3. הספק יצהיר בתצהיר – כי הוא מחק, גרס, גרט ו/או השיב ללמ"ס כל מידע אשר נמסר לו במסגרת מילוי תפקידו. בין אם מדובר במידע פיזי או לוגי לרבות מידע ממערכות מחשוב וגיבוי.

6. המשכיות עסקית

6.1. נהלים ומדיניות

6.1.1. הספק יקיים נהלים ומדיניות המשכיות עסקית ושמירה על זמינות השירותים הניתנים ללמ״ס במסגרת פרויקט זה על הקריטריונים שהוגדרו במכרז.

6.2. שרידות והמשכיות עסקית

6.2.1. כלל המערכות בסביבת הפתרון יוגדרו כתשתית המחייבת שרידות ויתירות מלאה בתצורת High-Availability או Active-Active . הזמינות תוגדר כ- 99.99%.

6.2.2. הספק יקיים תהליכי גיבוי, שחזור ובדיקות תקינות לגיבוי ושחזור, באופן אפקטיבי ותדיר (תדירות גבוהה) אשר יאפשרו אחזור המידע בנקודות זמן שונות ומרובות בהתאם לצרכי הלמ״ס.

6.2.3. יעשה שימוש בכלים להבטחת זמינות הנתונים של מידע שהוגדר כחיוני בתהליך הערכת הסיכונים למערכות המידע המסופקות בשירות זה.

6.2.4. מערכות תשתית ליבה, רכיבי תשתית סיסטם ורכיבי אבטחת מידע יותקנו בתצורת Active-Active. ניתן להשתמש ברכיבים וירטואליים בתצורת Active Standby.

6.3. גיבויים

6.3.1. כל מערכות התשתית ואבטחת המידע לרבות חומרה, תוכנה והנתונים השמורים במערכות המחשוב, יגובו לאמצעים נפרדים מהציוד בו הם נמצאים באופן מסודר.

6.3.2. תדירות הגיבויים תקבע על סמך סיווג הנתונים ורגישות המערכת.

6.3.3. כל מידע הרלוונטי לשירות המסופק ללמ״ס בדגש על מידע מזהה יגובה באופן מוצפן.

6.3.4. לכל מערכת מחשוב ומערכת תקשורת נתונים יוגדרו נהלים מפורטים לגיבוי תוכנה ונתונים וכן לשחזור תוכנה ונתונים מאמצעי הגיבוי.

6.3.5. הספק יבצע גיבוי תפעולי בכל שינוי מהותי במערכות הרשת והמחשוב.

6.3.6. יעשו גיבויים סדירים לכלל המערכות באופן ממוכן תוך שמירת מספר רב של גרסאות אחורנית.

6.4. אחסון הגיבוי

6.4.1. מתוך הנחה שיגובה מידע רגיש (תפעולי או אישי) הספק מחוייב להגן על המידע באופן מקסימלי בתנועה ובמנוחה. ויבצע:

6.4.1.1. ניהול בקרת גישה לוגית למידע.

6.4.1.2. הצפנת נתונים.

6.4.1.3. אחסון בסביבה מוגנת מפני גישה לא מורשית ונזקי טבע.

6.4.1.4. אבטחה פיזית אפקטיבית בהתאם לבקרות אבטחה פיזית המפורטות בהמשך.

6.5. שחזור ובדיקת תקינות הגיבויים

6.5.1. הספק יקיים שיחזור תקופתי/חלקי של הגדרות רגישות במערכת, לבדיקת אמינות הגיבוי.

6.5.2. הספק יבצע שחזור מדגמי למערכות נבחרות לבדיקת איכות הגיבוי ויכולת השחזור.

7. אבטחה פיזית

7.1. נהלים ומדיניות

7.1.1. הספק יקיים בכל עת נהלים ומדיניות להגנה ואבטחה פיזית של המידע ויציג אותם ללמ״ס על פי דרישתה.

7.1.2. הספק ימנה גורם מוסמך אחראי על היבטי אבטחה פיזית ובטחון.

7.1.3. הנהלים יועברו לקב״ט הלמ״ס במידת הצורך.

7.2. בקרה גישה פיזית

7.2.1. הספק יפעל למידור גישה פיזית למידע של הלמ״ס (על בסיס הצורך למידע) ובין היתר:

7.2.1.1. יפעל למידור פיזי בין מתחמי הספק למתחמים בהם מוחזק, מועבר או מעובד מידע של הלמ״ס. לדוגמה: חדר מחשב, ריכוז תקשורת, סביבת עבודה של עובדי הספק הניגשים למספרי הטלפון של אזרחים וכן כל סביבה אשר תוגדר בחצרות הספק כרגישה על ידי קב״ט הלמ״ס וראש אגף הגנת הסייבר בלמ״ס.

7.2.1.2. יפעיל אמצעי בקרת כניסה לזיהוי חד ערכי של עובדים ומבקרים במתחמים בהם מוחזק או יוחזק מידע של הלמ״ס (למשל באמצעות מנגנון RFID אישי, נציין כי לא יאושר שימוש בקודן בכניסה למתחמים דוגמת אלה המפורטים בסעיף זה).

7.2.2. הספק יאחסן חומר פיזי (דפוס, קלטות גיבוי, מצעי מדיה) באזורים מאובטחים וממודרים.

7.3. ניטור ובקרה

7.3.1. הספק יקשר את מערכות הביטחון למוקד אבטחה 7-24 למשך כל תקופת ההתקשרות.

7.3.2. הספק יוודא דריכה אוטומטית של מערכות האזעקה מעבר לשעות פעילות החברה.

7.3.3. הספק יאפשר יכולת תחקור לוגים ממערכות הביטחון לתקופה של שנתיים.

7.3.4. הספק ישמור תיעוד / רישום מבקרים בסביבות המחזיקות מידע רגיש לתקופה של שנתיים.

7.4. אירועי בטחון וסייבר

7.4.1. אירועי בטחון וסייבר בסביבת הספק (או ספקי משנה רלוונטיים לפעילות), אשר יחולו בסביבה המיועדת לפעילות הספק במסגרת הסכם התקשרות זה, ידווחו גם לחמ״ל הסייבר בלמ״ס בטלפון 02-6593124 ולקב״ט הלמ״ס.

8. אבטחת מידע וסייבר

8.1. נהלים ומדיניות

8.1.1. הספק יקיים בכל עת נהלים ומדיניות להגנת הסייבר ויציג אותם ללמ"ס על פי דרישתה.

8.1.2. הספק ימנה מנהל אבטחת מידע ו/או ממונה הגנת הסייבר בעל כישורים ותעודות מתאימות וכן ניסיון מקצועי טכנולוגי של לפחות 5 שנים בניהול הגנת הסייבר. **גורם זה יאשר את הפתרון המוצע על ידי הספק ויחתום על נספח זה בטרם הגשתו כמענה למכרז\ וישמש נאמן אבטחת המידע והגנה בסייבר במשך תקופת ההתקשרות.**

8.2. טיפול באירועי אבטחת מידע וסייבר

8.2.1. על הספק להציג ללמ"ס מוכנות לטיפול באירועי אבטחת מידע, בין השאר בקיומם של מסמכי מדיניות ונהלים לטיפול באירועי סייבר, אבטחה פיזית, שיבוש מידע, דלף מידע ופגיעה בזמינות השירותים.

8.2.2. הספק ימנה נציג שיהיה אחראי על טיפול באירועי אבטחת מידע (ניתן למנות נציג שיהיה בקשר עם חברה שלישית הנותנת שירותי אבטחה בעת הצורך), ופרטי הנציג והחברה השלישית יועברו ללמ"ס מראש ובכתב.

8.2.3. הספק נדרש לדווח באופן מיידי ללמ"ס במקרה של אירוע או חשש לאירוע אבטחת המידע מכל סוג, לרבות דליפת מידע או שימוש חורג מההרשאה שניתנה לספק. הדיווח יעשה בכתב ובטלפון עד 24 שעות מרגע זיהוי האירוע. הדיווח יתבצע ל לחמ"ל הסייבר בלמ"ס בטלפון 02-6593124.

8.2.4. הספק ידווח ללמ"ס באופן מיידי על כל אירוע, חשש או חשד הנוגעים להפרת פרטיות, לרבות שימוש במידע למטרה שלא אושרה, איסוף מידע עודף, העברת מידע לגורם בלתי מורשה.

8.2.5. הספק נדרש לדווח באופן מיידי ללמ"ס על כל אירוע או חשש לאירוע אבטחת מידע אשר ידוע לו כי הוא מתרחש גם אצל ספקי צד ג' וקבלני משנה החשופים למערכות ולמידע של הלמ"ס. הדיווח יעשה בכתב ובטלפון עד 24 שעות מרגע זיהוי האירוע.

8.2.6. במקרה של אירוע אבטחת מידע, על הספק ו/או קבלן המשנה לפעול למניעת דליפת המידע ולמניעת כל נזק כתוצאה מהתקלה.

8.2.7. הספק ייצר, יגן ויתחזק היסטוריה של לוגים ממערכות המחשוב שלו, תוך שמירה על יכולות ניטור (Monitoring), לנתח ולבצע תחקור על אירועי אבטחת מידע.

8.2.8. הספק יפעל לניטור כל פעילות המשתמשים מטעמו, באופן שיאפשר לאתר את המשתמש שגרם ו/או שמעשה ו/או מחדל שלו גרמו ו/או אפשרו את האירוע.

8.2.9. במקרים בהם אגף הגנת הסייבר בלמ"ס או מי מטעמו יעבירו לספק מידע בנושא איומי סייבר, יפעל הספק לקיום בקרות מפצות ויעדכן את הלמ"ס בגין הבקרות אותן הוא מבצע.

8.3. ניטור אירועי אבטחת מידע וסייבר

8.3.1. הספק יפעל לקיומו של מערך ניטור אירועי אבטחת מידע עם יכולת תגובה מהירה במקרה של אירוע אבטחה.

9. פניות ציבור

9.1. נהלי עבודה ואחריות משותפת

9.1.1. הספק יגדיר ביחד עם הלמ"ס, נהלים והנחיות להסדרת אופן הטיפול בפניות ציבור ועובדי הלמ"ס בין היתר בנושאי ניהול השוברים, מסירת מידע פרט, חופש המידע וזכות עיון וכן בכל המקרים בהם יתבקש מידע המזוהה עם הלמ"ס והשירות הניתן לה.

9.1.2. הנהלים אלה יאושרו בין היתר, גם על ידי המחלקה המשפטית, אגף הגנת הסייבר והממונה לנושא הגנת הפרטיות.

9.1.3. כל פנייה לעיון, תיקון, בירור, מחיקה או מימוש זכות אחרת ביחס למידע תועבר הלמ"ס ללא דיחוי. הספק לא ישיב באופן עצמאי לפנייה של אדם הנוגעת למידע פרט המוחזק או המעובד עבור הלמ"ס, אלא אם יוגדר אחרת בנהלים.

9.1.4. הספק יסייע ללמ"ס באיתור המידע הרלוונטי בהתאם לכללים שיוגדרו בנהלים.

10. הנחיות ארכיטקטורה

10.1. מסמכי תכנון

10.1.1. הספק יציג ללמ"ס מסמכי תכנון ואפיון הבאים: גאנט, מסמך התכנון , רשימת מערכות וטכנולוגיות, מיפוי תהליכים וניהול סיכונים.

10.1.2. **הצגת הפתרון ואופן המימוש (High Level Design) -** יציג את עקרונות הפרויקט ואופן קישור המערכת לסביבות הלמ"ס השונות וכן לשירותי ערוצי התקשורת השונים. **התכנון יוגש במסגרת המענה להצעה וישמש לניקוד איכות ההצעה בהיבטי הגנה בסייבר.**

10.1.3. לאחר זכיית הספק, נדרש הספק למסור מסמך תכנון מפורט (Low Level Design) המפרט בהרחבה את עקרונות הפרויקט ואופן קישור המערכת לסביבות הלמ"ס השונות וכן לשירותי ערוצי התקשורת השונים. **ללא קבלת מסמך זה באופן העונה על הנחיות נספח אבטחת המידע, לא תאושר פעילות הספק.**

10.1.4. מסמכים אלה יועברו לראש אגף הגנת הסייבר בלמ"ס, אגף מערכות מידע בלמ"ס ונציגי המחלקה העסקית. המסמכים יבחנו להתאמת הפתרון לצרכים העסקיים התפעוליים וכן עמידה בהנחיות אבטחת המידע.

10.1.5. הספק מתחייב לפעול לתיקון ליקויים שיתגלו במערכות או במסמכי האפיון ולהתאים את הפתרון לצרכים התפעוליים וצרכי אבטחת המידע של הפרויקט.

10.1.6. עלויות הנובעות משינויים במסמכי הארכיטקטורה שאינם במסגרת התכנון המקורי שאושר במסגרת מסמך התכנון יחולו במלואן על הספק.

10.2. מערכות הגנה בתקשורת

10.2.1. הספק יבצע שימוש ברכיבים הבאים: Firewall, IPS, Anti-Spoofing, Anti-bot, Antivirus, Antimalware, EDR.

10.2.2. הספק יפעיל מנגנוני ניטור כגון: IPS, Network Antivirus ו- Content Inspection על כל תעבורה נכנסת ויוצאת בין הסביבות.

10.3. אבטחת גישה לממשקי ניהול

10.3.1. תיושם הפרדה, הקשחה של ממשקי ניהול מממשקי השירות והאפליקציה על בסיס תפיסות הגנה מקובלות של היצרנים ותקנים מובילים.

10.3.2. ממשקי הניהול והתקשורת באמצעותה יתבצע הניהול, יהיו מוצפנים, מוגנים ומאפשרים אימות זיהוי חד ערכי על בסיס ניהול משתמשים וקבוצות משתמשים על פי קבוצות הרשאה (קריאה בלבד, עריכה חלקית, עריכה מלאה). במקרים בהם יהא צורך בפענוח הפרוטוקולים לצורך ניטור תעבורה מוצפנת, תתאפשר יכולת ניטור במערכות הניטור ואבטחת המידע של הספק (לדוגמה במקרה של שימוש ב- SSL, תתאפשר יכולת לבצע SSL Inspection).

10.3.3. הגישה לממשק הניהול תתאפשר רק מרשתות ניהול שאושרו לכך.

10.3.4. אימות משתמשי הניהול יעשה מול מערכת ניהול משתמשים (דוגמת: Active Directory, Radius, IAM/IDM וכדומה)

10.3.5. אין לאפשר ניהול מקומי של משמשים וסיסמאות.

10.3.6. כל פעולות הניהול יתועדו במלואן.

11. יישום מערכות הגנה

הערה: הנחיות אלה תיושמנה ברשת הספק בכל אחת מהסביבות המחזיקות או מעבדות מידע של הלמ"ס.

11.1. מערכות הגנה וניטור

11.1.1. הספק יישם אמצעי הגנה, ניטור, זיהוי וחסימה בהתאם לארכיטקטורה, רגישות המידע והערכת הסיכונים. היישום יכלול, לפי הצורך, הגנה על תעבורת רשת, שירותים החשופים לאינטרנט, יישומים, ממשקי API ובסיסי נתונים, לדוגמה: Firewall, IPS/IDS, WAF, API Security, Database Monitoring או פתרון מקביל ופתרונות לאיתור אנומליה והטעיה (Deception).

11.1.2. מנגנוני ההגנה יאפשרו זיהוי וחסימה של תקיפות מוכרות, פעילות חריגה, גישה בלתי מורשית וניסיונות ניצול חולשות.

11.1.3. הפתרונות יאפשרו בקרה גם על תעבורה מוצפנת, ככל הניתן.

11.1.4. מנגנוני ההגנה, החתימות והחוקים יעודכנו באופן שוטף ובהתאם להנחיות היצרן.

11.1.5. אירועי אבטחה משמעותיים יתועדו ויועברו למערך הניטור המרכזי/SOC של הספק.

11.1.6. הספק יבטיח שרידות וניטור תקינות של מערכות ההגנה, לרבות התרעה במקרה של כשל או ירידה ברמת ההגנה.

11.1.7. הספק רשאי לממש את הדרישות באמצעות פתרון ייעודי, יכולות מובנות בתשתית או שילוב פתרונות, ובלבד שיוכיח עמידה בדרישות האבטחה.

11.2. הגנה על בסיסי נתונים

11.2.1. הספק יישם פתרון Database Firewall להגנה על בסיס נתונים.

11.2.2. גישה לבסיסי נתונים תבוצע באמצעות חיבור מוצפן, חשבונות בעלי הרשאות מינימליות ושיטות גישה מאובטחות. סודות, סיסמאות ופרטי חיבור לא יישמרו באופן גלוי בקוד או בקובצי תצורה.

11.2.3. פתרון ה- Database Firewall ידע לנטר פעילות של משתמשים אלה.

11.2.4. פניות לבסיסי נתונים יבוצעו באופן המונע הזרקת קוד, לדוגמה באמצעות Parameterized Queries, Stored Procedures או מנגנון מקביל.

12. הגנה מפני מניעת שירות מקומית (DOS) או מבוזרת (DDOS)

12.1. הגנה על ממשקי אינטרנט

12.1.1. כל ממשקי האינטרנט החשופים לאינטרנט או לרשתות זרות ימוגנו באמצעות מערכות הגנה: DDOS Protection, WAF ו- IPS. המערכות תדענה לזהות התנהגות חריגה על בסיס חתימות והתנהגות סטטיסטית (אנומליה).

12.1.2. הספק יקצה כתובת IP ייעודית לכל ממשק חיצוני הפונה לאינטרנט.

12.1.3. הספק יפריד בין סביבות Front End ל- Back End באמצעות חוקה ייעודית ב-FW.

12.1.4. הספק יפעיל מנגנוני ניטור לאבטחת מידע בין הסביבות בהתאם לסוגי האיומים הקיימים: למשל WAF להגנה על שרתי אינטרנט, DB Firewall על שרתי DB, מערכות IPS, איתור אנומליה והטעיה.

13. הקשחת מערכות

13.1. הקשחת עמדות קצה, שרתים, מערכות תקשורת ואבטחת מידע

13.1.1. הספק יקשיח את כלל רכיבי התשתית, התקשורת, השרתים, תחנות הקצה ובסיסי הנתונים בהתאם להמלצות היצרן, Best Practices מקובלים והערכת הסיכונים.

13.1.2. ההקשחה תכלול, בהתאם לרכיב ולשימוש:

13.1.2.1. ביטול חשבונות, שירותים, פרוטוקולים ותוכנות שאינם נדרשים.

13.1.2.2. שינוי או ביטול הגדרות וחשבונות ברירת מחדל.

13.1.2.3. הגבלת ממשקי ניהול לרשתות וגורמים מורשים בלבד.

13.1.2.4. שימוש בפרוטוקולי ניהול ותקשורת מאובטחים.

13.1.2.5. יישום הרשאות מינימליות והפרדה בין חשבונות משתמש, שירות וניהול.

13.1.2.6. הפעלת EDR/Anti-Malware ו־Host Firewall לפי הצורך.

13.1.2.7. מניעת חיבור אמצעי אחסון והתקנים בלתי מורשים.

13.1.2.8. הצפנת מידע המאוחסן בתחנות ובשרתים.

13.1.2.9. תיעוד פעולות ואירועי אבטחה והעברתם למערכת ניטור מרכזית.

13.1.2.10. סביבות ומערכות המשמשות לעיבוד מידע של הלמ״ס יופרדו באופן לוגי או פיזי ממערכות שאינן נדרשות לצורך השירות.

13.1.3. תחנות קצה המשמשות לעבודה עם מידע של הלמ״ס ינוהלו באופן מרכזי, יוגבלו למשתמשים מורשים בלבד, ולא יאפשרו שמירה, העתקה, הדפסה או העברת מידע לערוצים או התקנים בלתי מאושרים.

13.1.4. לא תתאפשר הדפסת מידע של הלמ״ס אלא אם אושרה במפורש ובהתאם לצורך עסקי.

14. עדכוני חומרה ותוכנה

14.1. עדכוני חומרה, תוכנה ואבטחת מידע

14.1.1. הספק יפעיל תהליך מרכזי ,מחזורי ומבוקר לניהול עדכוני אבטחה עבור מערכות הפעלה, תחנות קצה, שרתים, רכיבי תקשורת, מוצרי אבטחה ותוכנות צד שלישי לרבות תלויות (Dependencies) וחבילות (Packages).

14.1.2. עדכוני אבטחה וגרסאות קריטיות ייבחנו ויותקנו בהתאם לרמת הסיכון, חומרת הפגיעות והנחיות היצרן, ובמסגרת זמני הטיפול שיוגדרו במכרז.

14.1.3. הספק יפיץ עדכונים קריטיים בסמוך למועד פרסומם או גילויים.

14.1.4. הספק יוודא כי מערכות אינן פועלות בגרסאות שאינן נתמכות על ידי היצרן, אלא באישור חריג ובכפוף לבקרות מפצות אפקטיביות. הספק לא יעשה שימוש במערכות שלא ניתן להחיל עליהן עדכוני אבטחה (דוגמת מערכות שהוגדרו End of life , end of support).

14.1.5. הורדת עדכונים תבוצע באמצעות תשתית או שירות עדכון מאושר ומבוקר, ללא מתן גישה בלתי מבוקרת לאינטרנט ממערכות רגישות.

14.1.6. הפצת העדכונים תתבצע בתהליך מוסדר, לאחר בדיקות, למניעת פגיעה במערכות.

15. ניהול משתמשים וסיסמאות

15.1. ניהול משתמשים והרשאות

15.1.1. הספק ינהל את כלל המשתמשים, חשבונות השירות והחשבונות הניהוליים באופן מרכזי ומבוקר, תוך שימוש בחשבונות אישיים.

15.1.2. אין לעשות שימוש בחשבונות משותפים או גנריים ללא בקרה אפקטיבית המאפשרת זיהוי הגורם המבצע שימוש בחשבונות אלה בפועל (דוגמת כספת סיסמאות).

15.1.3. הרשאות יינתנו בהתאם לעקרונות הצורך לדעת והרשאה מינימלית, תוך הפרדה בין חשבון משתמש רגיל לחשבון ניהולי וביצוע סקירות הרשאה תקופתיות.

15.1.4. גישה למערכות ולממשקי ניהול רגישים תחייב אימות רב־שלבי (MFA), בהתאם לרמת הסיכון.

15.1.5. לכל קבוצת משתמשים תוגדר גישה רק למידע ולפעולות הנדרשים לצורך תפקידה. מגבלות ההרשאה יחולו גם על צפייה, שינוי, הורדה וייצוא מידע.

15.1.6. יצירה, שינוי, השבתה והסרת משתמשים והרשאות ינוהלו בתהליך מבוקר, לרבות הסרה מיידית של הרשאות שאינן נדרשות עוד.

15.1.7. פעולות הזדהות, ניסיונות גישה ופעילות של משתמשים בעלי הרשאות גבוהות יתועדו ויהיו זמינים לניטור ולתחקור.

15.2. סיסמאות ואמצעי הזדהות

15.2.1. סיסמאות, סודות (Secrets) ונתוני הזדהות יישמרו ויועברו באופן מאובטח ולא יישמרו באופן גלוי.

15.2.2. אין להעביר סיסמאות באמצעים או פרוטוקולים גלויים.

15.2.3. מדיניות הסיסמאות תיקבע בהתאם להנחיות אבטחה מקובלות, ותכלול אורך מספק, מניעת שימוש בסיסמאות חלשות או פרוצות והגנה מפני ניסיונות ניחוש.

15.2.4. החלפת סיסמה תידרש במקרה של חשד לחשיפה, פגיעה בחשבון או בהתאם להערכת הסיכון, ולא רק על בסיס מחזור זמן קבוע.

15.2.5. עבור חשבונות שירות ומערכות, הספק יעדיף מנגנוני הזדהות מאובטחים שאינם מבוססי סיסמה, ככל שהטכנולוגיה מאפשרת.

16. שירותי הפצת מידע ב- SMS ו/או אפליקציית מסרים

16.1.1. שימוש בשירותי SMS או אפליקציות מסרים של צד ג׳ יבוצע באמצעות שירות עסקי מאושר, בכפוף להתקשרות חוזית הכוללת דרישות אבטחת מידע, פרטיות, זמינות ודיווח על אירועים ושינויים מהותיים.

16.1.2. ככל שהספק עושה שימוש בספק צד ג׳ למסירת ההודעות, ספק צד ג׳ חייב לעמוד בהנחיות נספח זה. אין בהוראה זו מלהסיר אחריות של הספק הזוכה.

16.1.3. שילוב שירות המסרים במערכת יבוצע באמצעות ממשקים מאובטחים ובהתאם להנחיות אבטחת ה־API והפיתוח המאובטח של הלמ״ס.

16.1.4. ערוץ המסרים ישמש להעברת מידע תפעולי נדרש בלבד. אין להעביר באמצעותו מידע אישי או רגיש שאינו נדרש לצורך השירות.

16.1.5. ככל שנשלחים קישורים, ייעשה שימוש בקישורים מזוהים תחת דומיין מאושר. אין להשתמש בשירותי קיצור כתובות ציבוריים.

16.1.6. ככל שהצורך העסקי הוא בהפצת הודעות בלבד, הערוץ יוגדר כחד-כיווני ולא יאפשר קליטת מידע חוזר מהמשתמשים.

16.1.7. הספק יישם בקרות למניעת דלף מידע בערוץ המסרים, באמצעות מנגנון DLP או בקרה מקבילה המתאימה לארכיטקטורה ולשירות.

16.1.8. פיתוח ייעודי של מנגנון המסרים יבוצע בהתאם לדרישות הפיתוח המאובטח המפורטות במסמכי המכרז.

17. הנחיות להגברת מודעות אבטחת מידע בהודעות התשורה

17.1. מודעות עובדים

17.1.1. הספק יקיים הדרכות מודעות אבטחת מידע לעובדים הנגישים למידע או למערכות הלמ"ס, ויציג אסמכתאות לביצוען לפי דרישה.

17.1.2. הודעות הנשלחות למקבלי השוברים יהיו במבנה אחיד ומזוהה, מתוך נוסחים מאושרים מראש על ידי הלמ"ס.

17.1.3. ההודעה תכלול זיהוי ברור של הגורם השולח ומטרת ההודעה, באופן שיסייע למקבל להבחין בין הודעה לגיטימית לבין ניסיון התחזות או פישינג.

17.1.4. ככל שההודעה כוללת קישור למימוש השובר, הקישור יהיה תחת דומיין מאושר ומזוהה ולא באמצעות שירות קיצור כתובות ציבורי.

17.1.5. ההודעה תכלול פרטי קשר או ערוץ מאושר לבירור, אימות ההודעה ודיווח על חשד להתחזות או פישינג.

17.1.6. אין לכלול בהודעה מידע אישי או רגיש מעבר לנדרש לצורך מסירת ומימוש השובר.

18. תיעוד, לוגים וניטור

18.1. מערכת איסוף מרכזית

18.1.1. הספק יוודא כי כלל המערכות הרלוונטיות לשירות יפיקו לוגים ויעבירו אותם למערכת איסוף וניטור מרכזית, כגון SIEM, Collector או פתרון מקביל.

18.1.2. הלוגים יתעדו, בהתאם לסוג המערכת והפעילות:

18.1.2.1. מזהה משתמש, מערכת או שירות.

18.1.2.2. מועד הפעולה.

18.1.2.3. מקור ויעד הפעילות.

18.1.2.4. סוג הפעולה ותוצאתה.

18.1.2.5. פעולות ניהול ושינויי הרשאות או תצורה.

18.1.2.6. גישה, שינוי או מחיקה של מידע.

18.1.2.7. אירועי הזדהות מוצלחים וכושלים.

18.1.2.8. פעילות חריגה ושימוש בחשבונות בעלי הרשאות גבוהות.

18.1.3. עבור שינויים מהותיים, יתועדו ככל שניתן פרטי השינוי, לרבות הערך לפני ואחרי השינוי והגורם שביצע אותו.

18.1.4. אין לתעד בלוגים סיסמאות, סודות, פרטי הזדהות או מידע רגיש שאינו נדרש לצורך ניטור ותחקור.

18.1.5. הלוגים יישמרו לתקופה שתוגדר על ידי הלמ"ס, תוך הבטחת זמינותם, שלמותם והגנה מפני שינוי או מחיקה בלתי מורשים.

18.1.6. הגישה ללוגים תוגבל לגורמים מורשים בלבד וכל גישה או שינוי במערכות התיעוד יתועדו.

18.1.7. הספק יגדיר מנגנוני זיהוי והתראה לפעילות חריגה, ובכלל זה:

18.1.7.1. גישה או שליפה חריגה של מידע.

18.1.7.2. מחיקת מידע

18.1.7.3. שינויי הרשאות או הגדרות אבטחה.

18.1.7.4. פעילות חריגה של משתמשי ניהול או Service Accounts.

18.1.7.5. כשל או הפסקת פעילות של רכיבי אבטחה וניטור.

18.1.8. אירועי אבטחה משמעותיים והתראות רלוונטיות יועברו ל-SOC או לגורמים המוסמכים, בהתאם למדיניות ולחומרת האירוע.

18.1.9. הספק יאפשר הפקת דוחות לצורך בקרה ותחקור של אירועי אבטחה, פעולות ניהול, חריגות ומגמות.

18.1.10. הספק יגבה את נתוני התיעוד בהתאם למדיניות הגיבוי ויוודא מעת לעת את יכולת השחזור.

18.1.11. ככל שנדרש בהתאם להערכת הסיכונים, הספק יפעיל שירות מודיעין סייבר לצורך איתור חשיפות של פרטי גישה, מידע רגיש או מידע השייך ללמ״ס במקורות חיצוניים.

18.2. מודיעין סייבר

18.2.1. הספק יפעיל שירות מודיעין סייבר לצורך איתור חשיפות, דלף מידע ואיומים הנוגעים ללמ״ס במקורות חיצוניים, לרבות Clear Web, Deep Web ו-Dark Web.

18.2.2. השירות יכלול התרעה על חשיפת מידע רגיש, פרטי גישה, נתונים מזהים או מידע ארגוני, וכן העברת ממצאים מהותיים לגורמים המוסמכים בלמ״ס לצורך טיפול.

19. פיתוח מאובטח

19.1. מודיעין סייבר

19.1.1. בכל המקרים בהם הספק יבצע תהליכי פיתוח או שימוש במערכת אשר מבוצע בה פיתוח ואינה מוצר מדף מוגמר וכן בפתרונות Open Source ומערכות AI. הוא מחוייב לעמוד בהנחיות הפיתוח המאובטח של הלמ״ס.

19.1.2. במקרה כזה הספק מחוייב לפנות ללמ״ס לקבלת נספח הפיתוח המאובטח ולפעול בהתאם להנחיות המפורטות בו במלואן.

התחייבות המציע

הריני מתחייב לעמוד בכל הדרישות המפורטות בנספח זה (נספח ז׳), במידה ואזכה במכרז לאספקת שוברי תשורה דיגיטליים/מגנטיים עבור הלמ״ס, ידוע לי כי קיום התנאים האמורים הם תנאי יסודי להסכם ההתקשרות בין הלמ״ס לספק הזוכה.

_____	_____	_____
תאריך	שם	חתימה וחותמת