# נספח ב' - מערכת ניהול תקציבי הסעדה – אגף תקשוב ואגף ארגון ומינהל - משרד החוץ - אפיון, מפרט טכני וריכוז דרישות

**להלן מפרט טכני מוצע בהתאם לאפיון מערכת שהוכן על ידי משרד החוץ, המשיבים מתבקשים להעביר התייחסותם לאפיון שלהלן, בהתאם לאמור בפנייה לקבלת מידע המצ"ב**

## 1. רקע

משרד החוץ מפעיל שני מזנונים במתחם המשרד המופעלים ע"י זכיין במסגרת מכרז פומבי:

1. מזנון בשרי - ארוחת צהריים בלבד.
2. מזנון חלבי - עבור ארוחת צהריים ובנוסף קפיטריה לממכר מוצרים נוספים במהלך כל שעות העבודה. המזנון משמש גם לצורך אספקת כיבודים למשרדים וכן אירוח לפי הצורך.

המזנונים מנוהלים ע"י ספק אחד אולם המכרז מאפשר הפעלה ע"י ספקים נפרדים.
המשרד כולל כ-1200 עובדים/נותני שירותים ובנוסף כ-150 מבקרים/אורחים ביום.
המשרד עושה שימוש רב גם בכיבודים לצורך אירוח אישים/משלחות ואירועים גדולים.
מספר הסועדים כיום כ-450-550 סועדים ליום.

## 2. מהות המערכת – מצב קיים

**מערכת קפיטריה - ניהול ארנק אלקטרוני של העובד וניהול ומעקב של רכישות מסובסדות.**
מערכת שפותחה במשרד החוץ. המערכת מנהלת פריטים ומחירונים לאוכלוסיות שונות לפי רמת זכאות שנקבעה מראש.
כל עובד זכאי להפקיד כסף אשר מנוהל במערכת וביכולתו לרכוש מוצרים על חשבון היתרה העומדת לזכותו.
ישנן אוכלוסיות שמקבלות פעם ביום או יותר זכאות לרכישת ארוחה מסובסדת מלאה או מסובסדת חלקית (השתתפות המשרד).

**מערכת מזנון – ניהול מערך אספקת הכיבוד במשרד**
מערכת שפותחה במשרד החוץ. המערכת מנהלת הזמנת כיבוד עבור ישיבות בהשתתפות גורמים חיצוניים ו/או אירוח מיוחד ו/או הזמנת מוצרים ספציפיים ליחידות לפי צורך
ההזמנות עוברות תהליך אישור ומועברות לביצוע של ספק ההסעדה ולאישור סופי של קבלת השרות ע"י היחידה.
לכל יחידה מוקצב סכום שנתי שאיתו אפשר לרכוש את השרות, כאשר קיימת בקרה עוצרת במידה ונרשמת חריגה מהתקציב.

**ניהול נוסף :**
ניהול אספקת חלב ליחידות ע"פ הקצאה שנקבעת מראש
ניהול שוברים – עבור אורחים בסבסוד מלא או חלקי
ניהול שוברים – עבור עובדים ששכחו כרטיס

## 3. מטרה

שרות/מוצר שיהווה פתרון לניהול כל למערך ההסעדה של משרד החוץ – רכישות עובדים וכיבודים

בחשיבות גבוהה פתרון לניהול הרכישות המסובסדות של עובדי המשרד כפי שיפורט בהמשך

המוצר ייתן פתרון לדרישות הכלליות שיפורטו ויורכב משני מודולים מרכזיים :
1. מודול רכישות עובדים (קפיטריה)
2. מודול ניהול כיבוד ואירוח (מזנון – כיבודים)

*פרוט הדרישות בהמשך

### 4. משתמשי המערכת

- אחראים של מערך ההסעדה ומנהלי המערכת
- ספק ההסעדה ועובדיו
- אגף כספים
- עובדי המשרד
- יחידות המשרד

### 5. פירוט הפתרון

**<u>שינוי תפיסה – השרות ושיטת הרכישה החדשה לעובדים</u>**

- המשרד יירכוש מוצר/שרות ואשר עונה לדרישות עם אפשרות להתאמה והרחבה לפי דרישה
- **בעקרון העובד <u>לא</u> יטען כסף מראש**
  *במידה ויידרש תהיה אופציה לכרטיס נטען שהספק מנהל ומספק לעובדים
- הרכישה תתבצע במזנונים ספציפיים בתחום המשרד
  העובד יוכל לבצע רכישה בשני המזנונים בסכום התקציב היומי הניתן ע"י המשרד.
  מעבר לסכום הסבסוד היומי העובד ישלם **מכספו** האישי.
- יישום מדיניות סבסוד בהתאם לתקציב יומי לעובד עפ"י מדיניות משרד החוץ.
- במידה ולא נוצל התקציב היומי לא יתאפשר לנצל אותו ביום אחר.
- הסכום הראשוני שינוקה יהיה מתוך התקציב שניתן לעובד ע"ח המעסיק.
- יתרת_סכום ההקצבה היומית אינה נצברת למועד אחר ולא עוברת לעובד בשום דרך
- כל עובד יגדיר במערכת מראש כרטיס אשראי ממנו ינוכה התשלום הנוסף , המערכת תאפשר לעובד לעדכן את כרטיס האשראי במידת הצורך.
- כל סכום שנדרש לשלם מעבר לתקציב היומי ינוכה מכרטיס האשראי של העובד ו/או במזומן
- עובד שלא הזין מראש את פרטי כרטיס האשראי יוכל לשלם את היתרה במעמד הרכישה בכרטיס אשראי או במזומן.

- עבור זיהוי העובד והתקציב היומי שלו - המשרד יעביר לחברה את נתוני העובדים לפי אוכלוסיות עם התקציב המותאם. הנתונים יעברו בקובץ או בממשק בדרך שתהיה מוסכמת על שני הצדדים אחת ליום (או בתדירות אחרת שתקבע) ובאישור א. מידע.

### 6. להלן הדרישות העיקריות :

כללי

**<u>ניהול פריטים (מוצרים) ומחירים (דרישות סף –חובה)</u>**

יש לנהל פריטים עבור סוגי רכישות שונות :

- פריטים בסבסוד המשרד עבור רכישות עובדים
- פריטים עבור הזמנת כיבוד לאורחים ואירוח
- פריטים עבור הקצאה יומית/תקופתית ליחידה (לדוגמא חלב)

הפריטים והמחירים המנוהלים לסוגי הרכישות הנ"ל בחלקם משותפים/זהים ובחלקם לא המחירים של הפריטים מבוססים על מחירי מכרז של המשרד מול הספק
מומלץ להשתמש בפלטפורמה אחת לעדכון שמות , מחירי הפריטים והמאפיינים שלהם

ניהול והזנת פריט -
יש לאפשר הזנה של פריטים (שם מוצר) כאשר לכל פריט יש מזהה חד-ערכי במערכת
לצורך זיהוי הפריט בעת רכישה יתאפשר זיהוי המק"ט של הפריט באמצעות הקלדה ובאמצעות ברקוד

יש צורך בניהול מאפיינים לפריטים עבור הצרכים השונים (יש אפשרות ליותר ממאפיין אחד לפריט ):

- ניהול שיוך פריט לפי סוג הרכישה (רכישה במזנון , הזמנת כיבוד וכו')
- ניהול קטגוריות לפריטים (ארוחות , שתיה , סנדוויצים וכו)
- ניהול פריטים לרכישה לפי סוג מזנון (בשרי, חלבי)
- ניהול מחירים – עדכוני מחיר , כולל עדכון מחיר בתאריכי תוקף עתידיים ועדכוני רטרו.
- עדכון גורף ונקודתי של מחירי הפריטים בעת שינויי מדדים ומע"מ
- ניהול סוגי מחירונים לפי סוגי סבסוד שונים
- ניהול אוכלוסיות וקישור למחירון מתאים
- ניהול זמני רכישה – למוצרים ספציפיים לפי שעות.
- הגבלת מוצרים לרכישה בתקצוב המשרד
- דוחות עם יכולות הדפסה של רשימות הפריטים בחתכים שונים כולל היסטוריה של עדכונים

**היסטוריה -**
נדרש לשמור היסטוריה של הפריט ומאפייניו בעת עדכונים וכן אין למחוק פריט לחלוטין אלא להפוך אותו לפריט לא פעיל בעת הצורך על מנת לשמר מידע היסטורי (עבור דוחות , בקרה וכו').
למזמין תהיה גישה לכלל המידע, לרבות ההיסטוריה. בהתאם למורשי הגישה (הרשאות).

**קפיטריה – רכישות עובדים**

השרות ישמש את עובדי המשרד מול ספק ההסעדה במזנונים השונים של המשרד
*כיום פעיל ספק הסעדה אחד , ייתכן שיתאפשר יותר מספק הסעדה אחד

- זיהוי עובד:
  קריאת כרטיס עובד לשם זיהוי –- כרטיס חכם המסופק למשרד ע"י ממשל זמין, קריאה ע"י קורא קרבה או פתרון אחר ישים שיאושר ע"י המשרד.
- אפשרות לחסימות כרטיסים בודדים (מתן אפשרות לחסימת רכישות במזנון לעובד ספציפי, מכל סיבה שהיא)
- אימות סבסוד לעובד – בדיקת זכאות הקצבה יומית.
- ניהול תנועות – רכישה , זיכוי
- אזור אישי לעובד: ניהול מעקב לעובד – כולל פתרון לעובדים שאין להם שם משתמש ברשת הארגונית.
  פרוט כל התנועות של העובד
  אפשרות לביצוע פעולות שונות מהאזור האישי
- זיכוי - זיכוי לפי נהלים שיקבעו - יתבצע מידית הן ברמת החברה והן ברמת החיוב כולל ביטול ניצול הסבסוד במידת הצורך.

- פתרונות לתקלות בהם אין תקשורת (כדוגמת הפסקת חשמל/ אין אינטרנט):
  - מתן אפשרות לביצוע חיוב של תקציב יומי מיום שעבר לאפשר לתקן מקרים בהם לא ניתן היה לבצע את החיוב בפועל במעמד הרכישה עקב תקלה
  - הגדרת נוהל/ דרך פעולה לאופן ביצוע רכישות בזמן שהמערכת אינה עובדת מסיבה כלשהי.
- חיפוש מהיר של זיהוי המוצרים במערכת לטובת עבודה שוטפת ומהירה של הספק
  אפשרות לזיהוי מוצרים לפי ברקוד
  אפשרות לזיהוי ע"י הקלדת מק"ט
  אפשרות חיפוש גם ע"י הקלדת שם המוצר
  (*אופציה – אפשרות למסך מגע לעובדי המזנון)
- עבודה ממספר עמדות במקביל
- מסך צפייה לבקרת העובד בזמן הרכישה
- אפשרות להזמנת רכישה לפני הגעה פיסית למזנון (יתרון)
- ממשק קל ואינטואיטיבי לרכישה, ממשק מתחלף לפי הגדרות (מוצרים לפי שעות קנייה, מועדפים ועוד).
- שמירת נתוני היסטוריה לכל הישויות, התנועות והפעולות במערכת
- דוחות לצורך התחשבנות, מעקב ושאילתות פרטניות. דוחות קבועים ודוחות דינאמיים לפי דרישה.
- מנגנוני בידוק ובקרה, לוגים .
- אפשרות להדפסת דו"חות.

**<u>הקצאת חלב או כל מוצר נוסף ליחידה על בסיס יומי/תקופתי</u>**

הקצאת פריט/ים ע"ב יומי ליחידה –עדיפות להקצאה לפי פריט מוגדר מראש.

- מורשים מטעם היחידה* יוכלו לקבל את הפריט/ים לפי ההקצאה (הקצאה על בסיס יומי או כל תקופה שתוגדר)
- לא יתאפשר לקחת מוצר אחר שלא הוגדר
- התחשבנות חודשית של המשרד מול הספק לפי סיכום תמחור הפריטים של כל היחידות שנלקחו.

*אפשרות לנהל מורשים ויחידות באופן עצמאי ללא תלות במבנה הארגוני של המשרד במידה ולא יאושר להעבירו

**<u>הקצאת שוברים (בסבסוד מלא או חלקי)</u>**

הקצאת כרטיסי אורח לבעלי תפקידים מאושרים הכולל תקצוב (מלא / חלקי) , בהתאם להחלטת המשרד:

- הקצאת סכום בהתאם לתדירות הגעת אורח- ניתן לתקצב יומית או חודשית.
- אפשרות לחידוש אוטומטי של הסכום לניצול
- תקציב/סכום רכישה על כרטיס/שובר חד פעמי – לשימוש אחד בלבד.
- תקציב/סכום רכישה על כרטיס/שובר רב פעמי – למספר שימושים.
- אפשרות להכנת הכרטיסים/שוברים מראש
- אפשרות להכנת שוברים לקבוצה
- אפשרות לניצול ביום ספציפי
- אפשרות לניצול פריטים ספציפיים
- אפשרות לניצול רטרו או עתידי במידת הצורך באישור בלבד

**ניהול כיבודים**

השרות ישמש את יחידות המשרד להזמנת כיבוד עבור ישיבות ועבור ארוח מיוחד לפי נוהלי המשרד

- ניהול פריטים ומחירים *לפי הסעיף הנ"ל
- ניהול סוגי הזמנות (כיבוד רגיל , כיבוד משודרג , ארוח משודרג לאישים/משלחת ועוד.)
- ניהול ושיוך פריטים מותאמים לכל סוג הזמנה
- אפשרות להגביל כמות רכישה מכל מוצר
- אפשרות להגביל כמות רכישה מכל מוצר גם לפי כללים מסויימים בהזמנה (כגון לפי כמות משתתפים)
- ניהול יחידות המשרד הזכאיות להזמנת כיבוד
- ניהול אולמות ואזורים במשרד בהם יוגשו הכיבודים*
- הקצאת תקציב לפי סכום , שנתי (או כל תקופה שתבחר) עבור כל יחידה*
- הקצאת תקציב לפי נושא/משימה
- זיהוי היחידה המזמינה (יחידה של העובד המזמין) *
- **בקרה עוצרת** – חסימת אפשרות הזמנה ליחידה כאשר יש חריגה מהתקציב
- התראות – לגבי ניצול תקציב
- טופס הזמנה (תאריך , שעה , שם מזמין/יחידה מזמינה , הערות , מיקום , פריטים להזמנה , כמות משתתפים וכו' )
- **WorkFlow – ניהול העברת ההזמנה לגורמים שונים (אחד או יותר), מאשרים ומבצעים בסטטוסים שונים, כולל הוספת הערות**

- הזמנה תועבר מהמזמין לאישור ע"י גורם מהמשרד (במידת הצורך תועבר לעוד גורם במקביל או לגורם עוקב מאשר נוסף)
- תועבר לביצוע במזנון
- תוחזר למזמין לאישור

יש צורך בדשבורד ניהולי נוח עבור מאשרי ומבצעי ההזמנה כולל אפשרות חיפוש והדפסה לקשיח

- אפשרות לעדכון , ביטול , החזרה של הזמנה , דיווח על הזמנה שלא הגיעה וזיכוי
- דוחות ושאילתות חיפוש לכל הגורמים

**פירוט הנתונים שיועברו למזמין עבור תפעול המוצר/שרות :**

- פרטי עובדי המשרד הזכאים לרכישה במסגרת השרות - **חובה**

**אופציונלי** (לפי דרישה ובאישור אבט"מ) :
- פרטי עובדי המשרד הזכאים להזמנת כיבוד – כולל היחידה התקציבית שלהם
- רשימת אולמות ומיקום
- רשימת יחידות לתקצוב

<u>פרטי עובדים</u>

נדרש להעביר ת.ז ו/או מספר עובד - עדיפות למספר עובד, ופרטים נוספים כגון שם העובד.

נדרשת התחייבות לעמידה בתקנות הגנת הפרטיות, כולל יכולת מובנית להסתרה של פרטי השם מגורם לא מורשה.

ניהול מיקום/אולמות
נדרש להעביר את רשימת האולמות/אזורים בהם יוגשו הכיבודים כולל המיקום שלהם
מאושר להעביר רק מספר חדר בשלב הזה.
תוספת תאור/שם אולם תחייב מענה הצפנה לשדות הללו

ניהול יחידות מתוקצבות
נדרש להעביר רשימה של יחידות* המשרד על מנת לתקצב את הרכישות בהתאם

יש לזהות את היחידה אליה משוייך העובד על מנת לנצל את התקציב המתאים
ייתכן והיחידה הישירה של העובד לא מתוקצבת ויש לבדוק מה יחידת האב המתוקצבת (עד שתי רמות מעל)
פתרון חלופי -
לשייך ולנהל בהרשאות פנימיות את העובדים המורשים להזמין ליחידה המתוקצבת

* כרגע מאושר להעביר את המבנה הארגוני שפורסם ע"י המשרד פומבית/חיצונית וכולל רק אגפים וחטיבות (אין יחידות). לכן בשתי האפשרויות אפשר להתייחס ולהתבסס כרגע על המבנה הארגוני הנ"ל
כלומר יחידות יהיו אגף או חטיבה

ניתן לספק את הרשימות/הנתונים בקובץ מאובטח לחברה בתדירות ובפורמט שיקבע ויתואם מולה
אם יידרשו ממשקים בהמשך הם יאופיינו בנפרד

**ממשקים נוספים**
**אפשרות להעברת מידע אל מערכת השכר המשרדית (תשלומים של כל עובד בנפרד לפי תקופה וכו' לפי דרישה) לפי אפיון שייקבע בהמשך**

**פרסומים (אופציונלי)**
פרסום מידע אינפורמטיבי לעובד:
בשלב זה המידע יפורסם בפלטפורמה של השרות/מוצר והמידע לא יישתל/יועבר למערכות המשרד.

- פרסום דוח ביקורת מזנונים + אפשרות לצפייה בדוחות קודמים.(*לא חובה)
- פרסום תפריטים יומיים לעובדים.
- פרסום מנת היום.
- פרסום הודעות מיוחדות בנושא.

**תמיכה נדרשת**

SLA רלוונטי, היקף תמיכה מבוקש

**עבור מערכת הרכישות נדרש שרות לקוחות זמין מיידי-** מענה מיידי לעובדים לכל בעיה/תקלה בעת רכישה

בהתקנה On-Prem:

| דרגת חומרה | סוג תקלה | אופן הטיפול | פיצוי מוסכם |
|---|---|---|---|
| 1 | תקלה קריטית – תקלה הגורמת להשבתה של כלל המערכת. | טיפול מיידי רצוף עד למתן הפתרון. | א. 300 ₪ לכל 30 דקות שבהן הספק עיכב את תחילת הטיפול למתן הפתרון. יחושב לכל 30 דקות החל מ 30 דקות ראשונות ממועד קרות התקלה.<br>ב. בנוסף, 600 ₪ לכל שעה במידה והתקלה לא תוקנה בתוך 60 דקות ממועד קרות התקלה. |
| 2 | תקלה דחופה – תקלה הפוגעת בצורה משמעותית בפעילות המערכת. | התחלת טיפול מיידי במהלך שעות העבודה הרגילות, ועבודה רצופה עד למתן הפתרון. | א. 300 ₪ לכל 30 דקות שבהן הספק עיכב את תחילת הטיפול למתן הפתרון. יחושב לכל 30 דקות החל מ 30 דקות ראשונות ממועד קרות התקלה.<br>ב. בנוסף, 600 ₪ לכל שעה במידה והתקלה לא תוקנה עד 07:00 ביום העבודה העוקב פיצוי זה יחושב החל מהשעה 07:00 העוקב. |
| 3 | תקלה רגילה – תקלה שאינה קריטית ואינה דחופה. | התחלת טיפול עד תום יום העבודה העוקב את יום דיווח התקלה. | א. 600 ₪ לכל יום שבו הספק עיכב את תחילת הטיפול למתן הפתרון. יחושב לכל יום החל מהיום העוקב השני לאחר קרות התקלה.<br>ב. בנוסף, 600 ₪ לכל יום במידה והתקלה לא תוקנה עד 07:00 ביום העבודה העוקב הרביעי החל מקרות התקלה. |

בהתקנה עננית:

| דרגת חומרה | סוג פעילות | אופן הטיפול | |
|---|---|---|---|
| 1 | פגיעה בפעילות קריטית – השבתה בפעילות עיקרית במערכת, כדוגמת רכישה או הזמנת כיבוד. | טיפול מיידי רצוף עד למתן הפתרון. | א. 300 ₪ לכל 30 דקות שבהן הספק עיכב את תחילת הטיפול למתן הפתרון. יחושב לכל 30 דקות החל מ 30 דקות ראשונות ממועד קרות התקלה.<br>ב. בנוסף, 600 ₪ לכל שעה במידה והתקלה לא תוקנה בתוך 60 דקות ממועד קרות התקלה. |
| 2 | פגיעה בפעילות שאינה קריטית (רגילה) – כדוגמת דוחות, הזנת פריטים בקטלוג. | טיפול מיידי רצוף עד למתן הפתרון. | א. 600 ₪ לכל יום שבו הספק עיכב את תחילת הטיפול למתן הפתרון. יחושב לכל יום החל מהיום העוקב השני לאחר קרות התקלה.<br>ב. בנוסף, 600 ₪ לכל יום במידה והתקלה לא תוקנה עד 07:00 ביום העבודה העוקב הרביעי החל מקרות התקלה. |

- **יש להכניס סעיף לגבי קנסות במידה והמערכת לא עבדה X זמן עם/בלי פתרון חלופי**

**דגשים נוספים**

מדיניות ניהול אשראי

1. **ניהול אשראי – עבור רכישות עובדים**

- בהתאם למדיניות המשרד ניתן לקבוע את אופן השימוש בחיוב באשראי - לדוגמה, במידה וניתן סבסוד של X ש"ח לכל ארוחה, כל שקל מעל X ₪ יהיה מחשבון האשראי הפרטי של העובד.
- השימוש בכרטיס העובד נעשה לצורך זיהוי סבסוד עבור רכישת ארוחות
- העובד צריך להכניס את פרטי כרטיס האשראי לאתר בעת ההרשמה לשרות
- עבור השלמת הרכישה מכספו של העובד יהיה שימוש בכרטיס האשראי המשוייך לעובד בשרות
- ניתן לבצע עסקאות נוספות באשראי בהתאם להגדרת המשרד.

- כל סכום שמעבר לסכום שהוקצה לעובד ינוקה אוטו' מאשראי העובד
- הגבלת עסקאות באשראי – ניתן לבצע הגבלה יומית /חודשית בעסקאות אשראי.
- בכל רכישה אחרת ניתן גם לרכוש בכרטיס האשראי הרשום של העובד
- ניתן לחייב את חשבון העובד באופן מידי או חודשי (עדיפות לחיוב חודשי שהינו פשוט, זול ונוח יותר).
- במידה ועובד לא מעוניין או אין באפשרותו להזין את פרטי האשראי למערכת מראש יתאפשר לו לשלם את החלק שלו באשראי במעמד הרכישה או במזומן לבחירתו.
  *אופציה לכרטיס נטען מראש שהספק מספק לעובדים ומנהל
- סליקה מידית - חברת הסליקה מבצעת בדיקת מסגרת, מאשרת וסולקת באותו יום.
- סליקה חודשית - חיוב נעשה אחת לחודש (חיוב בהתאם למועדי חברת האשראי, העובד רואה במעמד החיוב).

זיכוי עובד

- ניתן לבצע זיכוי לעובד לפי נהלי החברה - דרך שירות הלקוחות / דרך רפרנט מול תיק לקוח. הזיכוי מתבצע מיידית הן ברמת החברה והן ברמת האשראי ו/או בהתאם לסוג התשלום שבוצע.

**<u>דוחות והתחשבנות סוף חודש (במידה ומשרד החוץ יבקש לשלם ישירות לספק ההסעדה שלא דרך הספק הזוכה בניהול מערכת ההסעדה)</u>**

- נגישות לדוחות באתר בכל רגע נתון ויקבל פרוט דוחות במייל אחת לחודש.
- לספק ההסעדה של משרד החוץ אין עמלות סליקה או כל עלות אחרת.
- פעם בחודש יוצאת חשבונית מסודרת לספק ההסעדה, התשלום יועבר לספק ההסעדה בכפוף לתשלום של משרד החוץ

<u>דוחות – דוגמאות לדוחות שיש צורך בהם</u>

* אפשרת להנפקת הדוחות לפי תיחום תאריכים (בד"כ יונפקו פעם בחודש)

<u>דוחות התחשבנות</u>:

דוח מוצרים שהמשרד משתתף במימון(סבסוד שלהם) :
- רשימת המוצרים + כמות שנמכרה + הסכום המצטבר שהמשרד צריך לשלם
- סיכום מוצרים - סה"כ הסכום המצטבר שהמשרד צריך לשלם עבור כל המוצרים

<u>דוחות שוברים לפי סוג</u> :
- פרוט שוברים והסכום לתשלום עבור כל שובר
- סיכום כמות שוברים שהונפקו וסכום לתשלום

<u>דוחות נוספים</u> :
- דוח מחירון מוצרים לפי תקופה
- דוח כמויות מוצרים שנרכשו לפי תקופה
- דוח השתתפות משרד עבור כל מוצר לפי אוכלוסיה (לכל אוכלוסיה סכום השתתפות שונה – עובד משרד , בני שרות וכו')
- דוח כמויות מוצרים שנרכשו לפי תקופה עבור כל אוכלוסיה

- דוח סכום השתתפות משרד עבור כל מוצר לאוכלוסיה
- דוח רכישה לפי עובד (בנוסף אמור ליהיות משוקף לעובד כל התנועות שביצע מול המערכת)
- דוחות בקרה (תשלומים , זיכויים ...)

**נתונים טכניים נוספים**

---

- השרות/מוצר צריך לעבוד בכל הדפדפנים המובילים היום בשוק Chrome, Edge וכו' ולהתעדכן בהתאם לעדכונים של הדפדפנים.
- לשרות/מוצר יהיה גם אתר המותאם לתצוגה במכשירי טלפון ניידים – יתרון
- לשרות/מוצר תיהיה אפליקציה ייעודית – יתרון
- הממשק צריך ליהיות נוח ואינטואיטיבי לכל סוגי המשתמשים , בדגש על עובדי המשרד המקבלים את השרות ועובדי מערך ההסעדה המספקים שרות.
- יתרון לשרותי api לממשקים מול מערכות המשרד

**<u>הדרכה והטמעה – באחריות הספק הזוכה</u>**

- ליווי הגדרות המוצר/שרות עד ההטמעה בשטח.
- תועבר הדרכה ייעודית עבור אחראי המערכת וכל הגורמים הרלוונטיים במשרד החוץ.
- ליווי וקשר שוטף של מנהל המוצר מטעם החברה מול רפרנט עסקי/רפרנט תקשוב במשרד החוץ ככל שיידרש.
- חומרי הדרכה ותכני עזרה עבור כלל העובדים שישתמשו במוצר/שרות.
- מטלות ההדרכה ה וההטמעה הנ"ל הן באחריות הספק הזוכה כלול בהצעת המחיר, ללא תוספת תשלום.

## <u>נספח ג' – דרישות אבטחת מידע והגנת הסייבר</u>

### 1. כללי

1.1 נספח זה מפרט את דרישות אבטחת המידע והגנת הסייבר של המזמין לפרויקט זה.

1.2 הספק אחראי לכלל היבטי אבטחת המידע והגנת הסייבר לאורך כל מחזור החיים של הפתרון המוצע, לרבות למידע של המזמין במועד סיום ההתקשרות, כמפורט בהנחיות נספח זה.

1.3 למען הסר ספק, בכל מקום בו צויין "ספק" או "מציע", הכוונה לכלל שרשרת האספקה של הספק - הספק עצמו, כל ספק משנה, יועץ או גורם צד שלישי המעורב בפתרון או באספקת השירותים במסגרת ההתקשרות.

### 2. נאמן הגנת סייבר ואבטחת מידע

2.1 הספק ימנה נאמן הגנת סייבר ואבטחת מידע (להלן "הנאמן") מצוות אבטחת המידע של הספק ובעל הכשרה מתאימה, האחראי על הגנת סייבר ואבטחת המידע הנכלל במאגרי המידע של המזמין, המאוחסנים במערכות ובשרתי הספק כנדרש על פי כל דין.

2.2 הנאמן יעמוד בקשר שוטף עם מנהל הגנת הסייבר של המזמין (להלן "מנהל הגנת הסייבר"), ויהיה אחראי על יישום הנחיותיו.

2.3 הנאמן יהיה בעל נסיון, ידע והסמכות מתאימות וישמש כבעל מקצוע מרכזי לעבודה שוטפת מול מנהל הגנת הסייבר (POC), לרבות בשלבי התכנון, האפיון, ההקמה, ההטמעה, התפעול השוטף, התחזוקה, טיפול באירועי אבטחת מידע וסייבר ושיפור מתמיד של מנגנוני אבטחת המידע והגנת הסייבר.

2.4 בעת ביקור נציגי המזמין במתקני הספק, ייפגש הנאמן עם מנהל הגנת הסייבר של המזמין.

## 3. עמידה בחוקים, תקנות, הוראות אסדרה (רגולציה), מדיניות ותקני אבטחת מידע

3.1 הספק נדרש לעמוד בהוראות החוק החלות במדינת ישראל ובכל מדינה אחרת בה יסופק השירות ובכלל זה החוקים הבאים והתקנות המלוות להן:

3.1.1 חוק להסדרת הביטחון.

3.1.2 חוק המחשבים.

3.1.3 חוק הספאם.

3.1.4 חוק הפרטיות.

3.1.5 חוק הביומטריה.

3.2 הספק נדרש לעמוד בדרישות האסדרה (רגולציה) החלות במדינת ישראל ובכל מדינה אחרת בה יסופק השירות, ובכלל זה:

3.2.1 תוה"ג 2.0, בדגש על אספקת שירותי "ענן".

3.2.2 הנחיות מערך הסייבר הלאומי ו/או תקשוב ממשלתי/ יה"ב ל"נימבוס".

3.2.3 הגנות ב"שרשרת האספקה".

3.2.4 הנחיות פיתוח מאובטח.

3.2.5 הנחיות רלוונטיות בתו"ל "רימון".

3.3 ספק השירות והיצרן נדרשים לעמוד בכל התקנים הבאים:

3.3.1 CSA STAR

3.3.2 ISO/IEC 27001

3.3.3 ISO/IEC 27017

3.3.4 ISO/IEC 27018

3.3.5 ISO 22301

3.3.6 ISO/IEC 27701

3.3.7 ISO/IEC 28000

3.3.8 AICPA SOC 1-3

3.3.9 PCi-DSS

3.3.10 HIPAA

3.3.11 NIST SP800-171

3.3.12 NIST CSF 1.1

3.3.13 GDPR

3.3.14 NIST 800-53 (Rev. 4) או מקביל

3.3.15 תקן בינלאומי מוכר לניהול מהימנות עובדים

3.4 הספק נדרש לעמוד בבדיקות קבלה אבטחתיות לארכיטקטורה שנקבעה, סקרי סיכונים ומבדקי חדירה (Penetration Tests) עיתיים, אשר יאושרו על ידי מנהל הגנת הסייבר ומערך הסייבר הלאומי.

## 4. ארכיטקטורה וגבולות

4.1 בשלב הכנת ההצעה, יעביר המציע למזמין מסמך המתאר את הארכיטקטורה המלאה של המערכת המתוכננת לספק את השירותים הנדרשים ואת הצעתו להגדרת גבולות האחריות בין הספק למזמין.

4.2 בשלב תכנון המערכת, יועברו לספק הנחיות לאבטחת המידע והגנת הסייבר מטעם מנהל הגנת הסייבר ומערך הסייבר הלאומי.

4.3 ההנחיות יכללו דרישות טכניות ואו"שיות (ארגון ושיטות) ליישום במערכת (לדוגמה: הזדהות חזקה, מימוש מנגנוני הצפנה מלאים, שילוב רכיבי חומת אש, סינון פוגענים ואנומליות, יכולות ניטור ביטחוני עמוקות, קבלת הכשרה מקצועית של החברה בנושא היבטי סייבר של היישום, ניהול אירועי אבטחת מידע וסייבר, כתיבת נהלים רלוונטיים, מתן תדרוך ביטחוני למשתמשי המערכת השונים, סקרי סיכונים ומבדקי חדירה תקופתיים).

4.4 ההנחיות יידונו במשותף והספק יגיש למשרד מסמך תכנון על (HLD) ותכנון מפורט (LLD) לאישור.

4.5 במהלך הקמת המערכת, הספק יממש את התכנון בליווי ופיקוח של המזמין, בהתאם למסמכי התכנון.

## 5. הנחיות לתכנון אבטחת מידע

5.1 בשלב תכנון המערכת, יועברו לספק הנחיות לאבטחת המידע והגנת הסייבר מטעם המזמין ומערך הסייבר הלאומי.

5.2 ההנחיות יכללו דרישות טכניות ונוהליות ליישום במערכת, לרבות:

5.2.1 הנחיות לפיתוח ועידכוני תוכנה מאובטחים.

5.2.2 דרישות אינטגרציה בהיבטי אבטחת מידע.

5.2.3 הפרדת סביבות - פיתוח, בדיקות, ייצור.

5.2.4 הזדהות חזקה לרבות אמצעים פיזיים וכן התממשקות לתשתיות הזדהות חיצוניים.

5.2.5 ממשקים לתשתיות ארגוניות כגון Active Directory, שרתי Exchange.

5.2.6 מימוש מנגנוני הצפנה מלאים.

5.2.7 הגנה תשתיות תקשורת, תשתיות עיבוד ומחשוב ותשתיות אפליקטיביות.

5.2.8 ניהול זהויות והרשאות.

5.2.9 שילוב רכיבי חומת אש.

5.2.10 סינון פוגענים ואנומליות.

5.2.11 יכולות ניטור אבטחתי עמוקות.

5.2.12 קישור ממוכן למערכות הניטור האבטחתי המרכזיות של המזמין.

5.2.13 זיהוי ומניעת דלף מידע.

5.2.14 אחסון, גיבוי ושרידות.

5.2.15 הגבלות על המיקום הגאוגרפי של מאגרי המידע.

5.3 ההנחיות יידונו במשותף והספק יגיש למשרד מסמך תכנון על (HLD) ותכנון מפורט (LLD) לאישור.

5.4 במהלך הקמת המערכת, הספק יממש את התכנון בליווי ופיקוח של המזמין, בהתאם למסמכי התכנון.

5.5 הספק יספק מערכת בקרות למזמין המאפשרת למזמין לבצע ניטור מהיכן בוצע חיבור למערכת.

5.6 הספק יערוך מבדקי חדירה וסקרי סיכונים לפחות אחת לשנה. תוצאות הסקרים והמבדקים יוצגו למזמין ולממונה הגנת הסייבר של המזמין בפגישה השנתית. על הספק להציג תכונית לתיקון הממצאים במידה ויש. במקרה של ליקויים מהותיים המשפיעים ישירות על מערכות המזמין משרד החוץ יש לידע באופן מידי את ממונה הגנת הסייבר של המזמין על המצאות הליקוי.

## 6. ניהול משתמשים והרשאות

6.1 הספק נדרש לנהל את הגישה לשירותי הענן לפי סוג ההתקן (מחשבים נייחים/ניידים, טלפונים חכמים וכו') ומיקומו הגיאוגרפי.

6.2 תשתית המערכת המוצעת תכלול מערך ניהול זהויות והרשאות המאפשר את הגדרת יכולות הצפייה, העדכון, השליטה והבקרה של כל משתמש ובכל אובייקט.

6.3 יש להגדיר הרשאות גישה למידע באופן פרטני תוך הענקת הרשאות גישה רק לגורמים אשר גישתם למידע הכרחית לצורך מילוי תפקידם (לדוגמה ע"י מנגנון IAM).

6.4 הספק יאפשר שימוש במערכת ניהול המשתמשים של המזמין או במערכת לניהול זהויות והרשאות משתמשים, עפ"י החלטת המזמין.

6.5 הפתרון יתמוך בתהליכי ניהול משתמשים של המזמין, כגון קליטה ועזיבה של עובד, מעבר תפקיד, הוספת תפקידים ופרופילים וכדומה.

6.6 מנגנון ניהול המשתמשים וההרשאות, לרבות הקישור בין מערכות המשרד לבין הענן, יאופיין ע"י הספק בהתאם להנחיות מנהל הגנת הסייבר ומערך הסייבר הלאומי, בשלבי התכנון של הפרויקט.

## 7. בקרת גישה

7.1 על הספק לתמוך בהזדהות בשיטת MFA ע"י לפחות שניים מרכיבי ההזדהות הבאים:

7.1.1 Something you have: כרטיס חכם תמו"ז **כברירת מחדל**, RSA Token, OTP, קוד הנשלח באמצעות SMS או מופק דרך טלפון/התקן חכם אחר.

7.1.2 Something you know: סיסמה מורכבת וארוכה.

7.1.3 Something you are: אמצעי ביומטרי כגון טביעת אצבע, רשתית עין, זיהוי פנים וכדומה.

7.2 מדיניות הסיסמאות תקבע ע"י מנהל הגנת הסייבר של המזמין, בהתאם לתפקיד/פרופיל משתמשים, ותכלול הגדרה של מורכבות הסיסמאות, תוקף, הגבלות על שימוש בסיסמאות היסטוריות, נעילת חשבון אחרי מספר ניסיונות הזדהות שגויים, פרק זמן לניתוק תקשורת (Session Time Out) המחייב זיהוי מחדש של המשתמש, ועוד.

## 8. אבטחת מידע בתנועה

8.1 הספק נדרש להעביר מידע אשר נמצא בתנועה כגון מידע העובר בין המזמין לבין הענן, בין ספקי ענן שונים או בין רכיבים שונים בתוך הענן, על-גבי תווך תקשורת מוצפן לפחות אחד בתקן/שיטה מקובלים, אשר יאושרו ע"י מנהל הגנת הסייבר (כגון SSL, IPSEC, VPN, SSH וכו').

8.2 על הספק לתמוך בפרוטוקול המאפשר גישה למאגרי מידע פנימיים ליצירת שאילתות וביצוע עדכונים ללא צורך בשמירת המידע בענן (כדוגמת OData). הגישה למאגרי המידע תאובטח על-ידי פרוטוקול הזדהות כדוגמת OAuth 2.0, User Managed Access (UMA) או XACML.

8.3 הספק יידרש לאבטח את המערכת בענן באמצעים להגנה מפני מתקפות זמינות מסוג DDOS תשתיתי ואפליקטיבי.

8.4 הצעת הספק תכלול פתרון הגנת סייבר ואבטחת מידע בעל יכולות מתקדמות של ניטור ובקרה, מניעת פעילות זדונית בזמן הזיהוי, הצפנה במנוחה/תנועה, יכולות תיעוד ומעקב אחר פעולות ושינויים ויכולות אבטחה נוספות הנכללות בפלטפורמה זו.

## 9. אבטחת נתונים נייחים

9.1 הספק מתחייב לאחסן את נתוני המידע של המזמין בשיטה המאפשרת לפצל את המידע המאוחסן בשרתי הספק בין מספר שרתי אחסון שונים (כדוגמת מנגנון IDA), במטרה להקשות על תוקף או עובד הספק, בהשגת המידע בשלמותו.

9.2 הספק יאפשר למזמין להצפין את כל המידע, ובדגש על מידע רגיש המאוחסן בענן תוך שימוש באלגוריתם הצפנה סטנדרטי ומוכר.
מידע רגיש הינו מידע המוגדר כרגיש על פי הוראת כל דין, או שהוגדר כך על-ידי קב"ט המזמין, או על-ידי ממונה הגנת הסייבר של המזמין.

9.3 הספק יאפשר למזמין להתמים (MASKING) מידע בענן על-פי דרישת המזמין כברירת מחדל.

9.4 הספק יתמוך באפשרות ששדה מהותי אחד לפחות (שדה מזהה המאפשר זיהוי חד ערכי) יאוחסן ברשת המזמין ולא ברשת הספק.

9.5 הספק יתמוך בהצפנה תוך שימוש במערכת HSM כך שיאפשר למזמין לשמור מפתחות הצפנה אשר יהיו בשליטה בלעדית של המזמין (חילול והחלפת מפתחות).
לספק לא תהיה גישה למערכת ה- HSM, למעט לצורכי הצפנת מידע.

9.6 על הספק להציג בפני מנהל הגנת הסייבר את ארכיטקטורת אחסון הנתונים בענן, כדי לאפשר למזמין לזהות סיכונים אבטחתיים ולקבוע בקרות זמינות להתמודדות עם סיכונים אלו, אשר הספק יהיה מחוייב ליישם.

## 10. תקשורת והתקני קצה

10.1 הספק יתמוך בקישור למערכות המזמין בשתי החלופות הבאות:

10.1.1 דרך האינטרנט בתווך מוצפן.

10.1.2 באמצעות תשתית ייעודית מוצפנת בין הספק למזמין אשר תאפשר רציפות עבודה במידה והגישה לספק דרך רשת האינטרנט לא תתאפשר.

10.2 הספק יאפשר ניתוב (Routing) בין תקשורת האינטרנט לבין התשתית הייעודית.

10.3 הספק יספק אפשרות כניסה לענן מבוסס מיקום וכתובות IP.

10.4 הספק יאפשר למזמין להגדיר מדיניות לזיהוי משתמשים והתקני קצה, לרבות הגבלת מיקום גיאוגרפי, סוג התקן ושייכותו הארגונית, ויאכוף מדיניות זו כחלק אינטגרלי מהשירותים אותם יספק.

10.5 כלל הגישה לשירות, מכל מתקני המזמין, תתבסס על שילוביות ל- CASB של המזמין.

## 11. ניהול מפתחות הצפנה

11.1 הספק יאפשר למזמין לנהל את מפתחות ההצפנה באופן עצמאי במתקני המזמין או על-ידי גורם צד שלישי המתמחה בניהול מפתחות הצפנה, עפ"י החלטת מנהל הגנת הסייבר.

11.2 אם יוחלט כי ניהול מפתחות ההצפנה יבוצע בענן, על הספק לספק רכיב ייעודי לאחסון וניהול מפתחות הצפנה באופן מאובטח, בהתאם לדרישות מנהל הגנת הסייבר.

11.3 הספק יעמוד בתקני אבטחה מחמירים כגון FIPS 14-2, Common Criteria EAL4+ וכדומה, ויתמוך בפרוטוקולי הצפנה סטנדרטים ומוכרים.

## 12. שמירת המידע

12.1 הספק יהיה מחויב לשמירת פרטיות הנתונים, בהתאם להנחיות המחייבות במדינה בה ממוקם מתקן המחשב ממנו מסופק השירות.

12.2 המזמין יהיה רשאי להורות כי נתונים שדות רגישים לא ישמרו במערכות הענן אלא במערכות המזמין.

12.3 האתרים בהם ישמור היצרן את המידע ימוקמו במדינת ישראל או במדינות הנכללות בהנחיות מנהל הגנת הסייבר.

12.4 היצרן יתחייב כי הנתונים שינוהלו ביישומים שיופעלו בעבור המזמין יוותרו בתחומי המדינות הנ"ל, ולא יועברו למדינות אחרות, בכלל זה לא יאגרו ע"י ספקי אינטרנט, סלולר וכו'.

12.5 היצרן מתחייב שלא להעביר המידע של המזמין לצד שלישי או לכל גורם אחר ללא הרשאה בכתב של המזמין.

12.6 היצרן יפעיל לכל הפחות שני אתרים, הממוקמים במרחק של מעל ל-100 קילומטר אחד מהשני, כאשר שני האתרים פועלים בגיבוי הדדי, וכל אחד מהם יכול לספק מענה מלא לכל צורכי המזמין, בכפוף להגדרת המדינות המאושרות לעיל.

12.7 היצרן מתחייב לאפשר למזמין לבצע בקרה על המידע השמור באתריו הפיזיים.

12.8 היצרן מתחייב למחוק את כלל המידע הקשור למזמין במסגרת הסכם זה עם תום ההתקשרות או בהתאם להנחיה של המזמין, ללא יכולת אחזור.

## 13. אחסון וגיבוי

13.1 מנהל הגנת הסייבר יקבע היכן יישמרו מאגרי המידע של המזמין לרבות אתר הגיבוי, לאחר המלצה של הספק ובהתאם לאמור בנספח זה.

13.2 הספק יפעיל גיבויים אוטומטיים בזמן אמת של מידע של המזמין בכל אתר בו הוא מאוחסן.

13.3 הספק ישמור גיבוי Offsite באתר שיאושר מראש ע"י מנהל הגנת הסייבר.

13.4 שיחזור מידע והעלאת נתונים מגיבוי הינם באחריות ניהול ותפעול של הספק.

13.5 הספק מחוייב לדווח למנהל הגנת הסייבר על כל פעולה של שיחזור מידע מגיבוי.

13.6 לעניין תקנות הגנת הפרטיות – הספק הזוכה יחשב לספק מחזיק במידע בעניינו פרטיות ברמת אבטחה גבוהה.

## 14. אירועי אבטחת מידע (לרבות היבטי פרטיות) וסייבר

14.1 אירוע אבטחת מידע וסייבר מוגדר כאירוע בו קיים חשש להתרחשות נזק למזמין או לפגיעה בסודיותם, שלמותם וזמינותם של נכסי מידע של המזמין או לפגיעה בפרטיות כהגדרתה בחוק, ברגולציות או בתקנים המחייבים במסגרת ההתקשרות עם הספק.

14.2 הספק מחוייב לדווח בזמן אמת למנהל הגנת הסייבר על כל חשד לאירוע אבטחת מידע או סייבר או אירוע חריג במתקניו העלול להצביע על חשד כזה.

14.3 האחריות לטיפול באירועי אבטחת מידע וסייבר הינה של הספק, בהתאם למתודולוגיות מוכרות, למחויבויות הספק במסגרת ההתקשרות, לתקני אבטחת המידע אליהם הוסמך הספק ובכפוף להנחיות פרטניות מטעם מנהל הגנת הסייבר של המזמין, ככל שיינתנו.

14.4 הספק יעביר בסוף כל חודש דוח מפורט, מאושר מטעם הספק ע"י נאמן אבטחת המידע, על אירוע אבטחת מידע וסייבר שזוהו וטופלו על ידו במהלך החודש החולף, ניתוח האירוע, הממצאים, המסקנות, הלקחים והצעדים שננקטו בעקבות האירוע.

14.5 בהיבט אירועי כשל עפ"י תקנות הפרטיות לספק מחזיק – יש לפעול עפ"י מדיניות המזמין ובכפוף לתקנות שבתוקף ומתעדכנות מעת לעת.

## 15. רישוי וגרסאות תוכנה

15.1 הספק מתחייב להעמיד לרשות המזמין בזמן אמת את כלל יכולות ותכונות אבטחת המידע והסייבר בגרסאותיהם המלאות והעדכניות כחלק אינטגרלי מהפתרון.

15.2 כל מוצרי התוכנה בהם יעשה שימוש או בהם נדרש לעשות שימוש כחלק מהפתרון (כגון דפדפנים), נדרשים לתמוך בגרסאותיהם העדכניות ביותר.

## 16. בדיקות אבטחת מידע והגנת סייבר

16.1 בדיקות הקבלה של המערכת יכללו בדיקות אבטחת מידע והגנת סייבר, לרבות מבדקי חדירה (Penetration Tests).

16.2 במהלך תקופת הבדק תחול על הספק אחריות בלעדית לתיקון/השלמת כל ליקויי אבטחת המידע שיתגלו, במועד הקצר ביותר האפשרי ובלוח זמנים שיוצג ע"י ספק למזמין ויאושר ע"י מנהל הגנת הסייבר.

16.3 סביבות הפיתוח, הבדיקות והייצור יהיו זהות בהיבטי יכולות אבטחת המידע והגנת סייבר, לרבות עמידה בתקני אבטחת מידע והגנת סייבר מחייבים.

## 17. קורסים והכשרות

17.1 הספק נדרש לקיים הכשרות בתחומי הסייבר ואבטחת המידע לעובדי המזמין הרלוונטיים, בדגש על מיצוי יכולות הפתרון להשגת הגנה אופטימלית.

## 18. נגישות למידע על-ידי עובדי הספק

18.1 הספק נדרש לעמוד בהנחיות מנהל הגנת הסייבר, מערך הסייבר הלאומי והתקשוב הממשלתי באשר להגבלת הנגישות של עובדיו למידע של המזמין.

18.2 אין לאפשר לעובד יחיד של הספק את היכולת לשלוף את כלל המידע של המזמין; כל פעולה כזו מחייבת אישור פרטני של מנהל הגנת הסייבר, אשר יכלול זיהוי חזק שלו מול המזמין ואישור אקטיבי של הפעולה כתנאי לביצועה.

18.3 כלל הפעילויות מול בסיס הנתונים המרכזי ינוטרו ויתועדו ברמה פרטנית ובאופן חד ערכי.

## 19. פניית מגורם אכיפה לקבלת מידע

19.1 הספק מחוייב לעדכן על כל פניית גורם אכיפה מקומי או בינלאומי לקבלת נתונים של המזמין (עם או בלי צו בית משפט), טרם מסירת מידע כלשהו, וימנע ממסירת מידע של המזמין ללא אישור בכתב ומראש ע"י המזמין.

## 20. מניעת Lockdown

20.1 הספק יאפשר למזמין לשמור עותק מקומי של כלל המידע של המזמין בחצרות המזמין ו/או בכל אתר אחר שיקבע מנהל הגנת הסייבר וזאת על מנת למנוע מצב של Lockdown.

## 21. מעקב, ניטור ובקרה

21.1 הספק השירות יידרש לספק דוחות כגון SSAE 16 SOC2 או ISAE 3402 Type 2 report, אודות בקרות המיושמות בשטחו על-ידי גופים חיצוניים אמינים הסוקרים נושאים הקשורים לאבטחת המידע, זמינותו, שלמותו וחשאיותו, לרבות בקרות הקשורות להגנת סייבר וההגנה על הפרטיות עפ"י כל דין.

21.2 בהתאם למודל השירות הנבחר ולסוג המערכת או המידע הנשמרים בענן, על הספק להבטיח את אמינות נתוני הרישום של אירועים במערכות או ברכיבים שיוגדרו על-ידי מנהל הגנת הסייבר כבעלי רגישות גבוהה לתפקוד המערכת.

21.3 לצורך ניטור והתראה על אירועי אבטחה המתרחשים בענן, רישומי המערכת ייאספו על-ידי מערכת SIEM או Syslog ייעודית בענן ו/או ישלחו למערכת ה-SIEM של המזמין, בהתאם להחלטת מנהל הגנת הסייבר.

21.4 הספק יאפשר למזמין לאסוף את רישומי המערכת בזמן אמת/באופן מתוזמן.

21.5 לוגים יועברו בפורמט UTC או בפורמט שיקבע עם הקבלן הזוכה בשלב ה- HLD.

21.6 הספק מתחייב לשמור היסטוריה של רישומי מערכת לתקופה המשתנה בהתאם לרגישות המערכת ולדרישות רגולטוריות התקפות למערכת, כפי שיקבע ע"י מנהל הגנת הסייבר.

21.7 על הספק לוודא כי רישומי המערכת נשמרים בשרת מרכזי המנוהל על-ידי צוות עובדים נפרד מהצוות המפעיל את המערכת.

21.8 אם הספק יבקש לשנות את מערכת הלוגים, עליו לעדכן את מנהל הגנת הסייבר 60 יום מראש, על מנת שיוכל להיערך.

21.9 הספק נדרש לבצע ניטור לשירותים ולמערכות בענן ברבדים הבאים:

- ניטור סיכונים מתפתחים – הערכת סיכונים דינאמית לכלל התהליך העיסקי, אשר מבוטא באמצעים טכנולוגיים, אשר בטיפול הקבלן.
- ניטור לוגים – איתור בזמן אמת או בדיעבד של בעיות טכניות או אירועי אבטחת מידע המתרחשים.

- ניטור ביצועים – מעקב אחר עומסים במשאבי המחשוב בענן.
- ניטור ומעקב אחר פעילויות חריגות/עוויינות (ניסיונות הזדהות כושלים, גישה לא מורשית, ניסיונות כניסה כפולים ועוד).

21.10 הספק יספק מידע אודות תוצאות מבדקי חדירה המתבצעים במתקניו באופן תדיר לפי סטנדרטים מקובלים על פי תקני אבטחת מידע.

## 22. ביקורת – עמידה בהסכם בין הספק למזמין

22.1 הספק יאפשר למנהל הגנת הסייבר ונציגים נוספים של המזמין, לקיים בכל עת סיור במתקניו הרלוונטיים לצורך ביקורת אבטחת מידע ועמידה בהסכמים ו/או חוזים אשר יחתמו בין הספק למזמין. לכל סיור יצוותו הנציגים הרלוונטיים מטעם הספק על-פי דרישת המזמין, לרבות הנאמן.

22.2 אחת לשנה לפחות ייערך ביקור של נציגי המזמין במתקני הספק, בהתאם להחלטת המזמין.

22.3 הספק יאפשר למזמין להיפגש עם בעלי תפקידים רלוונטיים בתיאום מראש.

22.4 במקרה של קבלן המונחה ע"י גורם אחר (מס"ל, 770, מלמ"ב) – יש להציג אישור עדכני ומפורט של עמידה בתקנות "שרשרת האספקה" לקבלן מהותי.

## 23. סיום ההתקשרות עם הספק

23.1 עם סיום ההתקשרות עם הספק, על הספק מוטלת האחריות לבצע את הנחיות מנהל הגנת הסייבר, מערך הסייבר הלאומי והתקשוב הממשלתי/ יה"ב, לרבות הפעולות הבאות:

23.1.1 מחיקה חד חד ערכית ולא ניתנת לשחזור של כל הנתונים והמידע השמורים בשירות הענן ונמצאים תחת שליטת המזמין.

23.1.2 השמדת עותקים של הנתונים והמידע בהם נעשה שימוש במסגרת פעילות הספק עבור המזמין.

23.1.3 דרישה מהספק להעביר התחייבות משפטית ולהציג הוכחות לכך שהמידע הושמד (רישומים ודוחות רלוונטיים).

23.1.4 במקרים אחרים קבלה פיזית של רכיבי האחסון של המידע.

23.1.5 במידה והמידע הוצפן – ביטול (Revoke) מפתחות ההצפנה ומחיקתם.