הנחיות אבטחת מידע להקמה ותפעול של הליך איסוף הנתונים בסקר הוצאות משקי הבית - "פאנל צרכנים"

אין להעתיק או להשתמש במסמך זה או חלקים ממנו ללא אישור בכתב מראש תחום אבטחת המידע בלמ"ס. מסמך זה הינו לשימוש עובדי מחלקת אבטחת מידע וגורמים מורשים מטעמם בלבד. כל המוצא מסמך זה מתבקש להחזירו לידי הלשכה המרכזית לסטטיסטיקה, רחוב כנפי נשרים 66, גבעת שאול – ירושלים.

תוכן עניינים

1.	**הקדמה**	**3**
2.	**תיאור תהליך האיסוף**	**5**
3.	**הנחיות התקשרות עם הספק**	**5**
4.	**תכנון ארכיטקטורה, רכש ואישור טכנולוגיות**	**12**
5.	**הגנה על המידע**	**13**
6.	**שימוש בשירותי בינה מלאכותית**	**15**
7.	**מחשוב ענן**	**17**
8.	**תשתית סוקרי שטח**	**18**
9.	**סביבת המחשוב והתקשורת של הפרויקט (סביבת הספק וה-** call Center**)**	**19**
10.	**אבטחת מערכות המחשוב של הספק**	**20**
11.	**אבטחת תשתיות טלפוניה**	**25**
12.	**אבטחת מערכות הקלטת שיחות**	**27**
13.	**רציפות תפעולית**	**28**
14.	**ממשקים אלחוטיים**	**29**
15.	**גישה מרחוק**	**29**
16.	**ניהול משתמשים במערכות הספק**	**30**
17.	**הגנה על מידע פיזי**	**32**
18.	**ניטור**	**33**
19.	**פניות ציבור**	**36**
20.	**מודעות אבטחת מידע לעובדי הספק**	**36**
21.	**הנחיות פיתוח מאובטח לספק**	**40**

1. הקדמה

1.1. רקע

1.1.1. הלמ"ס פונה לספקים לצורך הקמה ותפעול של הליך איסוף הנתונים בסקר הוצאות משקי הבית - "פאנל צרכנים" כאמור בפרק ג' במרכז (פירוט השירותים ותוכן ההתקשרות עם הספק הזוכה).

1.1.2. מטרת הפרויקט הינה הקמת פאנל בתשתית אנ"ס בלמ"ס, בו ייאסף באמצעים שונים מידע בשיטות שונות ובין היתר: גישה ישירה לנתונים פיננסיים, ניתוח נתוני האשראי, גישה לנתוני המסלקה הפנסיונית, הוצאות רכישת מוצרי בני קיימא, מידע נוסף יתבסס על פענוח של חשבוניות קניה (דיגיטליות או נייר) שיספקו משתתפי הפאנל.

1.1.3. המענה יעשה בשיטות איסוף בכלים שונים: קבלת נתונים באמצעות מערכת הבנקאות הפתוחה, השבה עצמית באינטרנט (CAWI), השבה באמצעות ראיון טלפוני (CATI) ובסקר המרכזי גם השבה באמצעות ראיון פנים אל פנים בשטח (CAPI).

1.1.4. איסוף באמצעות סוקרי שטח יתבצע באמצעות פתרון משולב המבוסס על מחשבים מוקשחים ומערכת Mobile Device Management (MDM) / EMM (End Point של **<u>הלמ"ס</u>**.

1.1.5. בסביבת הפאנל בתשתית אנ"ס של הלמ"ס יוחזק גם מידע רגיש שייחשף לספק ויאפשר לו לבצע את האסוף. ובין היתר: מדגם אוכלוסייה, פרוטוקולי פנייה לנדגמים, נוסחי שאלונים, פרטי התקשרות וכדומה.

1.2. מטרות

1.2.1. מטרת מסמך זה להגדיר את הסיכונים האפשריים בקיומו של תהליך השבה באמצעות סוקרי מיקור חוץ (סיכונים בשרשרת האספקה), והתווית הדרכים להפחתת הסיכונים באמצעות הנחיות אבטחת מידע לנושאי תשתיות המחשוב והאפליקציה בלמ"ס, בחצרות ספקי ה- Call Center והגנה על אמצעי מחשוב של הספק.

1.2.2. הנחיות אלה נכתבו לשלב הפיילוט ולשלב הפרויקט המלא לאחר הפיילוט. לאור ייתכנות של פערי זמנים , שינויים טכנולוגיים וסיכונים בין של הפיילוט לשלב יישום הפרויקט, יתכן כי יועברו הנחיות נוספות.

1.2.3. מסמך זה מגדיר את הנחיות אבטחת המידע לספק, קבלני משנה מטעמו ועובדיהם במהלך ההתקשרות ואספקת השירות ללמ"ס.

1.3. היקף ומגבלות

1.3.1. הלמ"ס הינה ארגון תמ"ק (תשתית מידע קריטית) ולפיכך נדרשת היא וספקי השירות הפועלים עבורה (או בשמה) לעמוד בהנחיות מערך הסייבר הלאומי כפי שכן מובאות במסמך זה.

1.3.2. תשתית אנ"ס היא תשתית מהותית של הלמ"ס בתהליכי איסוף.

1.3.3. הנחת המוצא כי הספק הזוכה יכול להפעיל גם קבלני משנה ועצמאים בחלק מהפעילות והנחיות אלה יחולו גם עליהם.

1.3.4. המסמך מכיל הנחיות אבטחת מידע לנושאים רבים הרלוונטיים לפרויקט ובינם: הנחיות למתן מענה לסיכונים טכנולוגיים הן בסביבות ובמערכות המיושמות בחצרות הלמ"ס ובתשתיות הענן שלה והן בסביבות ובמערכות המיושמות בחצרות הספק וסביבות הפיתוח של הספק: בהיבטי תשתית, אפליקציה ופיתוח מאובטח, אבטחה פיזית, סיכונים בשרשרת האספקה בשימוש בשירותי מיקור חוץ ועוד.

1.3.5. חלקם של עובדים אלה יעשה שימוש באמצעי מחשוב חיצוניים או אישיים. מסמך זה נועד להגדיר את אחריות הספק בהעסקת ספקים ועובדים אלה וכן את האחריות האישית הנוספת של ספקי צד ג' ועובדים (לרבות עצמאיים).

1.3.6. **נדגיש:** מסמך זה והנחיותיו הינו מנדטורי וחלק בלתי נפרד מהמכרז והספק מתחייב לפעול על פי הנחיות אלה במהלך כל תקופת ההתקשרות ואספקת השירות ללמ"ס. הנחיות אלה ונהלי העבודה של הלמ"ס גוברים על נהלי העבודה והנחיות מכרז דיגיטק. **בעת מחלוקת – נהלי הלמ"ס והנחיות אגף הסייבר בלמ"ס יהיו ההנחיות המחייבות הקובעות. כמו כן לראש אגף הגנת הסייבר בלמ"ס הסמכות לפסול ספק שלא יעמוד בכל הנחיות נספח זה.**

1.3.7. המסמך אינו מתייחס לדרישות עיצוב, מבניות, או הנגשה (חוק) וכן נושאים שאינם רלוונטיים להגנה בסייבר או רגולציה רלוונטית לנושא זה.

1.3.8. כתיבת הנחיות אבטחת המידע נעשו בטרם הספק הזוכה הציג תכנון "על" (HLD) או תכנון מפורט (LLD). לפיכך הספק מאשר כי ידוע לו שיתכן כי יועברו הנחיות פרטיות נוספות במהלך יישום הפתרון.

1.3.9. הספק מאשר כי ידוע לו כי בעת מתן השירותים, יתכן כי יועברו לספק המבצע הנחיות נוספות. ככל שיועברו הנחיות נוספות, יידרש הספק לפעול ליישומן.

1.3.10. ראש אגף הגנת הסייבר בלמ"ס הינו הגורם היחיד הרשאי להקל בהנחיות המסמך. הלמ"ס אינה מתחייבת לאשר בקשות להחרגה או הקלה החורגות מנספח זה.

1.3.11. הספק יישא בכל עלות כתוצאה מאי עמידה בהנחיות מסמך זה.

1.4. חריגים למסמך זה

1.4.1. לראש אגף הגנה בסייבר בלמ"ס הסמכות הבלעדית להקל בהנחיות המפורטות במסמך זה.

1.5. אחריות

1.5.1. ראש אגף הגנת הסייבר בלמ"ס – קביעת ההנחיות ובקרה על אופן יישומן.

1.5.2. מנמ"רית הלמ"ס ועובדי אגף טד"מ ומנהלי הפרויקט מטעם הלמ"ס – מסירה ואכיפת ההנחיות בתהליכי העבודה מול הספק (הקמה, תחזוקה, פיתוח, ייעוץ טכנולוגי וכיו"ב).

1.5.3. הספק המבצע (במסגרת דיגיטק או כל התקשרות אחרת) – עמידה מלאה בכל ההנחיות ואכיפת ההנחיות מול עובדיו או ספקי משנה (שאושר לספק לעבוד איתם במסגרת התקשרות זו) ובהתאם לדרישות העסקיות של הפרויקט.

1.6. מונחים

1.6.1. מערכת אנ"ס – מערכת האיסוף המרכזית של הלמ"ס.

1.6.2. הספק הזוכה – הספק שהוגדר כזוכה ועונה על תנאי המכרז.

1.6.3. קבלן משנה - כל גורם חיצוני לספק הזוכה, לרבות חברה, שותפות, עוסק מורשה, עוסק פטור, יועץ, מומחה, פרילנסר, עצמאי או כל אדם אחר, אשר מספק שירותים, עבודות, תוצרים, ייעוץ, תמיכה, פיתוח, תחזוקה, בדיקות, תפעול או כל פעילות אחרת עבור הספק הזוכה או מטעמו בקשר למכרז או להסכם ההתקשרות, במישרין או בעקיפין.

1.6.4. MDM / EMM – פתרון טכנולוגי לניהול ושליטה מרחוק בהתקני מחשוב ניידים.

2. תיאור תהליך האיסוף

2.1. תיאור כללי

2.1.1. במסגרת ההסכם תעשה ההשבה (איסוף המידע) באמצעות מתן גישה תקשורתית על גבי תשתית VPN בין הספק ללמ"ס ולסביבת האיסוף המחזיקה את מערכת אנ"ס.

2.1.2. סביבת מערכת אנ"ס תחזיק מידע מסוגים שונים על נדגמים, לרבות תעודות זהות ושאלונים חלקיים בעלי מידע (להלן: "תהליך ההשבה").

2.1.3. במסגרת האיסוף הספק יעמיד לרשות הלמ"ס סוקרי מיקור חוץ אשר יבצעו את הסקרים מסביבת Call Center (מוקד טלפוני של הספק) ובסקר המרכזי גם סוקרי מיקור חוץ ניידים (להלן: "סוקרי שטח"). כאשר:

2.1.3.1. איסוף באמצעות מוקד הטלפוניה יעשה באמצעות תשתיות טלפוניה ומחשוב של הספק.

2.1.3.2. איסוף באמצעות סוקרי שטח יעשה באמצעות מחשבים ניידים שיסופקו על ידי הלמ"ס.

2.1.4. רשומות הנסקרים (מנות המידע) יוחזקו, יעובדו וימולאו אך ורק בתשתית אנ"ס ולא יועברו לספקים או למערכותיהם.

3. הנחיות התקשרות עם הספק

3.1. אחריות ומומחיות אבטחת המידע של הספק

3.1.1. הספק ימנה ממונה אבטחת מידע בעל ניסיון, ידע וכישורים מקצועיים מתאימים להיקף השירותים, לתשתיות המחשוב, לארכיטקטורה ולסיכוני הסייבר בפרויקט. פרטי הממונה, קורות חייו ואסמכתאות לניסיונו יועברו לאישור הלמ"ס.

3.1.2. ממונה אבטחת המידע יחתום על נספח אבטחת המידע, לצד מורשה החתימה מטעם הספק, ויהיה אחראי מטעם הספק להנחיה, ליווי ובקרה על יישום דרישות אבטחת המידע והגנת הסייבר לאורך כל תקופת ההתקשרות.

3.1.3. הממונה ילווה את תכנון הפרויקט ויישומו, לרבות ארכיטקטורת המחשוב והתקשורת, הפרדת סביבות, הגנה על מידע, בקרות אבטחת מידע ותהליכי פיתוח מאובטח, ככל שרלוונטיים לפרויקט.

3.1.4. ממונה אבטחת המידע יבחן ויחתום על מסמכי התכנון והאפיון, לרבות HLD ו־LLD, ובחתימתו יאשר כי התכנון והבקרות המוצעות עומדים בדרישות נספח זה ונותנים מענה לסיכוני אבטחת המידע שזוהו.

3.1.5. ככל שלממונה אבטחת המידע אין מומחיות מספקת בתחום מקצועי מסוים, הספק יעמיד מומחים נוספים בעלי ניסיון מתאים לצורך תכנון, יישום ובדיקת הדרישות, מבלי לגרוע מאחריות הממונה ומהתחייבויות הספק.

3.1.6. החלפת ממונה אבטחת המידע במהלך ההתקשרות תחייב אישור מראש ובכתב של ראש אגף הגנת הסייבר בלמ"ס. הספק יבטיח רציפות במילוי התפקיד לאורך כל תקופת ההתקשרות.

3.1.7. להלן פרטי ממונה אבטחת המידע בפרויקט:

שם ממונה אבטח"מ	ת.ז	טלפון נייד – עובד	חתימת ממונה אבטח"מ

3.2. סיווג הספק, קבלני משנה ועובדים

3.2.1. הספק יידרש בסיווג בטחוני, בתיאום עם קב"ט הלמ"ס.

3.3. עמידה בתקנות הגנת הפרטיות

3.3.1. במסגרת פעילות זו נידרש הספק להצהיר ולקיים את תקנות הגנת הפרטיות למשך כל זמן אספקת השירות. בין היתר באמצעות שמירה על מידע אישי, ביצוע סקרי סיכונים ומבדקי חדירות, הנחיה ופיקוח אחר פעילות עובדים, קבלני משנה, חולשות וסיכונים טכנולוגיים וסייבר וינקוט את מירב האמצעים לשמירה על המידע מפני סיכוני סודיות/דלף מידע וחשיפתו לגורם זר שאינו מורשה לכך.

3.4. נהלי הלמ"ס

3.4.1. הספק נדרש ומתחייב לפעול על פי נהלי הגנת הסייבר של הלמ"ס ויוודא כי העובדים וקבלני המשנה מטעמו (ועובדיהם) פועלים על פי נהלים אלה.

3.4.2. אגף הסייבר מנחה את העובדים והספקים לנקיטת אמצעי בטיחות להגנה על המידע באמצעות נהלים והנחיות טכניות. מסמכים אלה מפורסמים בפורטל הנהלים של אגף הסייבר והספק נדרש לצפות בהם ולפעול על פיהם במהלך תקופת ההתקשרות ולאחריה (ככל שיהיה רלוונטי).

3.4.3. הנחיות המפורטות בנספח זה נגזרות על פי נהלי הלמ"ס , יחד עם לאור זאת כי הנחיות אלה עלולות להשתנות במהלך ההתקשרות על הספק להתעדכן בשינויים מול פורטל הנהלים. נדגיש כי בכל מקרה של מחלוקת בין הספק, הנחיות מכרז דיגיטק או תפיסות הגנה אחרות, **נהלי הלמ"ס הן והנחיות אגף הסייבר בלמ"ס יהיו ההנחיות המחייבות הקובעות.**

3.1. חובת הספק וספקי המשנה לעמידה בהנחיות מערך הסייבר הלאומי – רמה A

3.1.1. הספק וספקי המשנה המעורבים בפרויקט יוגדרו על ידי הלמ"ס כ-**ספק רמה A**. לפיכך הספק וכן חברות בנות ו/או ספקים, קבלני משנה ונותני שירות צד ג', המעורבים בפרויקט יידרשו בביצוע סקר על בסיס שאלון יעדים ובקרות לארגון (יוב"ל). הסקר יכלול מילוי שאלון הערכת סקר ספק על בסיס שאלון מערך הסייבר העדכני ביותר במערכת מצפ"ן (ממשל, ציות, פרמטרים וניהול סיכונים) [1].

3.1.2. הספק **<u>מחוייב</u>** בתהליך התעדה באמצעות ועדת ההתעדה של מערך הסייבר הלאומי ועל ידי גורם שהוסמך לכך על ידי מערך הסייבר הלאומי. התהליך יבוצע באופן ממוקד **<u>ורק</u>** על השירות הניתן ללמ"ס או על שירותים שעלולים להשפיע עליה, ולא על כלל שירותי הספק או שירותים אחרים שהספק מספק ללקוחות אחרים מטעמו.

3.1.3. הספק יעביר את תוצאות הסקר לראש אגף הגנת הסייבר בלמ"ס אחרי בחירה בספק הזוכה, אך לפני מועד אספקת השירות בפועל. אי עמידה בתנאי זה לא תאפשר הפעלת הספק.

3.1.4. יתרון יינתן לספקים שכבר ביצעו את התהליך, והתעודה שניתנה להם בתוקף והם מופיעים במאגר הספקים להסמכה ברמה A [2].

3.1.5. **קבלני משנה ועצמאים:** הנחיות מערך הסייבר (והתעדה על בסיס מצפ"ן) יחולו על הספק הזוכה ועל ספקי צד ג' שיופעלו על ידו במהלך ההתקשרות. בכל מקרה בו הספק הזוכה או מי מטעמו יפעילו גורם מומחה שאינו חברה (לדוגמה: יחיד או עצמאי) – האחריות לעמידה בהנחיות יוב"ל תחול על הספק **<u>הזוכה</u>** והוא יחוייב להעמיד לרשות המומחה היחיד את כלל האמצעים לעמידה בהנחיות נספח זה וכן יישא באחריות מלאה בכל חריגה מהנחיות אלה.

3.2. סקר חצרות ספקים

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

3.2.2. סקר חצרות הספקים יתבסס בין היתר גם בעמידה בהנחיות אבטחת המידע המפורטות בנספח זה, ופערים למול שאלון מצפ"ן לרבות: בדיקות אבטחה פיזית ולוגית, הקשחת מערכות, ארכיטקטורה, ניהול משתמשים והרשאות, בדיקות אפליקטיביות, אחסון מידע ועוד. הספק מחויב לתקן כל ממצא שיתגלה, ובפרט ממצאים אשר עלולים לפגוע בלמ"ס או במידע שלה בהיבטי סודיות, זמינות ואמינות.

3.2.3. הספק מסכים ומאשר כי יתכנו סקרים נוספים שיבוצעו גם על ידי מערך הסייבר הלאומי ו/או מי מטעמו המוסמך לכך.

---

[1] https://www.gov.il/he/pages/yuvalinfo , https://grc.cyber.gov.il/login

[2] https://www.gov.il/he/departments/dynamiccollectors/supply_chain_stock_a?skip=0

3.2.4. הספק יתחייב לתקן כל ממצא מהותי (רגולטורי, טכנולוגי או הנוגע להגנת פרטיות) אשר עלול לחשוף את המידע של הלמ"ס לסיכון לפגוע באמינות, סודיות או זמינות, וזאת עד למועד אספקת השירות ללמ"ס. תנאי זה מהווה דרישה מנדטורית להעלאת השירות לאוויר.

3.2.5. הספק יתחייב לספק מסמך המפרט את אופן הטיפול בממצאים, וכן התחייבות לכך שהממצאים טופלו במלואם. כל ממצא חריג או חריגה מאופן טיפול הליקויים תובא לאישור ראש אגף הגנת הסייבר בלמ"ס, ונתונה לשיקול דעתו הבלעדי.

3.2.6. הספק וקבלני המשנה יסכימו כי מנהל ההתקשרות או מי מטעמו תהא רשאית לבצע ביקורות בכל עת, כולל סקרים חוזרים וביקורות פתע, בתיאום עם הספק.

3.2.7. בהסכם השירות עם הספק יצוין כי במידה והספק ו/או קבלן המשנה לא פעלו לתיקון הליקויים תוך חודש (אלא אם יאושר אחרת ובכתב על ידי מנהל ההתקשרות או מי מטעמו), יפסק ההסכם עם הספק ו/או קבלן המשנה באופן מידי. חריגים יאושרו על ידי ראש אגף הגנת הסייבר בלמ"ס.

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

3.2.9. סקר הספקים יבוצע על בסיס הנחיות המסמך וכן על בסיס שאלון ממשל, ציות, פרמטרים וניהול סיכונים של מערך הסייבר הלאומי (מצפ"ן).

3.2.10. הספק מאשר ומסכים כי הלמ"ס ו/או מי מטעמה תהיו רשאים לבצע סקר סיכונים טכנולוגי לכל המערכות והרכיבים המעורבים בביצוע הפרויקט המנוהל על ידי הספק ויימצאו כרלוונטיים לבדיקה (כגון: מערכת ניהול המידע, אפליקציה, תקשורת, סיסטם וטלפוניה, מערכות הגנה בסייבר, אבטחה פיזית ורשת בטחון פיזי).

3.2.11. הלמ"ס תהא רשאית (בתיאום עם הספק), בכל עת, לבקר את מחשבים ו/או מערכות המידע של הספק, בהן נמצא מידע שהתקבל מהלמ"ס או נוצר במהלך ההתקשרות, בהתאם לשיקול דעתו הבלעדית של מנהל ההתקשרות או מי מטעמו .

3.3. סקרי אבטחת מידע וביקורות ספקים

הנחיות אלה יחולו על הספק הזוכה וספקי משנה רלוונטיים בפרויקט:

3.3.1. הספק יבצע, על חשבונו, סקר סיכונים ומבדק חדירות למערכות ולסביבות המשמשות את הפרויקט, טרם תחילת אספקת השירות ולפחות אחת ל־18 חודשים במהלך ההתקשרות, ככל שהיא נמשכת מעבר לתקופה זו.

3.3.2. הספק יעביר ללמ"ס את ממצאי הבדיקות, תוכנית הטיפול, לוחות הזמנים ואסמכתאות לתיקון הליקויים, בהתאם לדרישות הלמ"ס ובכפוף להגנה על מידע שאינו קשור לפרויקט.

3.3.3. הלמ"ס, מערך הסייבר הלאומי או גורם שהוסמך מטעמם יהיו רשאים לבצע סקרי אבטחת מידע וביקורות בסביבות הספק וקבלני המשנה הרלוונטיות לשירות, לרבות בדיקות אבטחה פיזית ולוגית, ארכיטקטורה, הרשאות, תשתיות, מערכות ואפליקציות. הלמ"ס תהיה רשאית לבצע בדיקות חוזרות, ביקורות תקופתיות ובדיקות לאימות תיקון הממצאים, בתיאום עם הספק ובהתאם להוראות ההתקשרות. **<u>נדגיש:</u>** ביצוע סקרים או אישור ממצאים על ידי הלמ"ס לא יגרעו מאחריות הספק לעמידה בדרישות אבטחת המידע. סמכות הלמ"ס להשהות או להפסיק פעילות בשל ליקויים שאינם מטופלים באופן אפקטיבי הממזער את הסיכון או מונע אותו.

3.3.4. הספק יתקן את הממצאים שהתגלו בבדיקות ובסקרים בהתאם לחומרתם ולמועדים שתקבע הלמ"ס. ממצאים מהותיים העלולים לסכן את מידע הלמ"ס או את השירות יטופלו לפני תחילת הפעילות או חידושה, אלא אם אושרה חריגה מראש ובכתב.

3.4. גיוס וסיווג עובדי הספק המספקים את השירות

3.4.1. הספק יוודא כי כלל העובדים המועסקים בפרויקט, לרבות עובדים חדשים, עובדי קבלני משנה ועצמאים, יאושרו מראש על ידי מנב"ט הלמ"ס ויעמדו בדרישות הסיווג והבדיקות הביטחוניות שנקבעו לתפקידם.

3.4.2. הספק יבצע את בדיקות הרקע הנדרשות בהתאם להנחיות הלמ"ס ולהוראות הדין, ויציג את האישורים והאסמכתאות הנדרשים טרם תחילת עבודת העובד בפרויקט.

3.4.3. כל עובד יחתום, טרם תחילת עבודתו, על התחייבות לשמירת סודיות ועמידה בהנחיות אבטחת המידע, ויקבל הדרכת מודעות (על ידי הספק וממונה אבטחת המידע) בהתאם למפורט בנספח זה.

3.4.4. הלמ"ס תהיה רשאית לסרב לאשר העסקת עובד בפרויקט או לדרוש את החלפתו, בהתאם להוראות המכרז והדין. אישור עובד על ידי הלמ"ס לא יגרע מאחריות הספק למעשיו ולמחדליו.

3.4.5. הספק וממונה אבטחת המידע יהיו אחראים להנחיית העובדים וקבלני המשנה ויבצעו פיקוח על פעילותם ולעמידתם בדרישות אבטחת המידע במהלך כל תקופת העסקתם בפרויקט, לרבות דיווח על שינויים בתפקידם, הפסקת עבודתם וביטול הרשאות שאינן נדרשות.

3.4.6. הספק ינהל רשימה עדכנית של כלל העובדים המורשים לפעול בפרויקט ,לרבות תפקידם ,סטטוס אישורם ומועדי תחילת וסיום פעילותם ,ויעבירה ללמ"ס לפי דרישתה.

3.5. קבלני משנה

3.5.1. כלל הדרישות וההתחייבויות המפורטות במכרז ובנספח אבטחת מידע זה יחולו גם על קבלני משנה, עצמאים, פרילנסרים, יועצים, מומחים, ספקי צד שלישי וכל גורם הפועל מטעם הספק הזוכה, במישרין או בעקיפין, בהתאם לאופי פעילותו.

3.5.2. הספק הזוכה יישא באחריות מלאה וישירה לעמידת כלל הגורמים מטעמו בדרישות אבטחת המידע, לרבות מעשיהם ומחדליהם. הפעלת קבלן משנה או גורם אחר לא תגרע מאחריות הספק כלפי הלמ"ס.

3.5.3. הספק יעביר ללמ"ס מראש ובכתב רשימה של כלל קבלני המשנה והגורמים שבכוונתו להפעיל בפרויקט, לרבות השירות הניתן על ידם, תפקידם, המערכות המעורבות והגישה הנדרשת למידע או למערכות הלמ"ס. הספק יעדכן את הרשימה בכל שינוי.

3.5.4. הפעלת קבלני משנה או גורמים אחרים במסגרת הפרויקט תחייב אישור מראש ובכתב של אגף הגנת הסייבר בלמ"ס או מי שהוסמך לכך מטעמו. לא תתאפשר תחילת פעילות של גורם שלא אושר.

3.5.5. לא תתאפשר גישה פיזית או לוגית, ישירה או עקיפה, למידע של הלמ"ס, למערכותיה או למערכות הספק המשמשות את הפרויקט, ללא אישור מראש ובכתב. הדרישה תחול גם על גישה לצורכי פיתוח, תחזוקה, תמיכה, בדיקות, אינטגרציה, ניטור ותפעול.

3.5.6. הספק יישם ויאכוף בקרות גישה ואבטחת מידע עבור כלל הגורמים מטעמו, לרבות זיהוי אישי, הרשאות בהתאם לצורך, הזדהות מאובטחת, הגבלת חיבורים, ניטור ותיעוד פעולות וביטול הרשאות בסיום הפעילות, בהתאם לדרישות נספח זה.

3.5.7. קבלן משנה לא יהיה רשאי להעביר את השירות, כולו או חלקו, לגורם נוסף או לאפשר לו גישה למידע או למערכות הפרויקט, ללא אישור מראש ובכתב של הלמ"ס. הספק הזוכה יהיה אחראי לאכיפת דרישה זו לאורך כל שרשרת האספקה.

3.6. אירועי בטחון וסייבר

3.6.1. הספק ייערך לטיפול באירועי ביטחון, אבטחת מידע וסייבר העלולים להשפיע על השירות או על מידע הלמ"ס, לרבות באמצעות נהלים, הגדרת תחומי אחריות ומינוי גורם מקצועי אחראי לניהול האירועים. פרטי הגורם האחראי וממלא מקומו יועברו ללמ"ס מראש.

3.6.2. הספק ידווח באופן מיידי לאגף הגנת הסייבר ולמנב"ט הלמ"ס על כל אירוע או חשד לאירוע העלול להשפיע על מידע הלמ"ס, מערכותיה או השירות הניתן לה, לרבות אובדן או גניבת ציוד, חשיפת מידע, גישה בלתי מורשית, פגיעה בזמינות או אירוע המתרחש אצל קבלני משנה וספקי צד שלישי.

3.6.3. הדיווח הראשוני יבוצע מיד עם גילוי האירוע, באמצעות חמ"ל הסייבר של הלמ"ס בטלפון 02-6593124 ובאמצעי הדיווח שתקבע הלמ"ס. דיווח כתוב הכולל את פרטי האירוע הידועים, השפעתו והפעולות שננקטו יועבר בתוך 24 שעות לכל היותר, ויעודכן בהתאם להתפתחויות.

3.6.4. הספק יפעל באופן מיידי לצמצום הנזק, לבידוד מערכות שנפגעו ולמניעת המשך חשיפת מידע, תוך תיאום עם הלמ"ס ובהתאם להנחיותיה. פעולות העלולות להשפיע על מערכות הלמ"ס או על זמינות השירות יתואמו עמה, למעט פעולות חירום הנדרשות למניעת נזק מיידי.

3.6.5. הספק ישמור ראיות, לוגים ותיעוד רלוונטיים, יתחקר את האירוע, יזהה את גורמיו ויפעל לתיקון הליקויים ולמניעת הישנותו. ממצאי התחקיר, הפעולות המתקנות והאסמכתאות לביצוען יועברו ללמ"ס בהתאם לדרישתה.

3.6.6. הספק יישם הנחיות ואמצעי הגנה נוספים שתעביר הלמ"ס בעקבות אירוע או התרעה רלוונטית, וידווח על אופן יישומם. חזרה לפעילות של מערכות שהושבתו עקב אירוע מהותי תהיה בכפוף לאישור הלמ"ס.

3.7. הפסקת פעילות עם הספק בשל אי־עמידה בדרישות אבטחת המידע

3.7.1. ראש אגף הגנת הסייבר יהא ראשי להורות על השהיה או הפסקה מיידית של פעילות הספק, כולה או חלקה, במקרה של אי־עמידה בדרישות אבטחת המידע, גילוי סיכון מהותי, ממצאים קריטיים או גבוהים, או ליקויים חוזרים שלא טופלו, העלולים לפגוע בסודיות, בשלמות או בזמינות המידע והמערכות של הלמ"ס.

3.7.2. הספק יפעל לתיקון הליקויים ולצמצום הסיכונים בהתאם להנחיות הלמ"ס ובמועדים שייקבעו על ידה. כל בקשה לחריגה או להקלה בדרישות אבטחת המידע תוגש מראש ובכתב ותטופל בהתאם להחלטת ראש אגף הסייבר בלמ"ס.

3.7.3. חידוש פעילות שהושהתה או הופסקה בשל סיכוני אבטחת מידע יתאפשר רק לאחר תיקון הליקויים, הצגת אסמכתאות המעידות על הטיפול בהם וקבלת אישור מראש ובכתב של ראש אגף הגנת הסייבר בלמ"ס.

3.7.4. בהתאם לחומרת הליקויים ולשיקול דעת הלמ"ס, הספק יידרש לבצע, על חשבונו, בדיקת אבטחת מידע חוזרת באמצעות גורם מקצועי חיצוני ובלתי תלוי, ולהציג דוח בדיקה, אסמכתאות לתיקון הממצאים והצהרה חתומה על עמידתו בדרישות. הלמ"ס תהיה רשאית לבצע בדיקות נוספות בעצמה או באמצעות גורם מטעמה.

3.7.5. הספק יישא בעלויות הנובעות מאי־עמידתו בדרישות אבטחת המידע, לרבות תיקון ליקויים ובדיקות חוזרות שיידרשו בעקבותיהם, בהתאם להוראות המכרז וההסכם. אין בהשהיית הפעילות, בהפסקתה או באישור חידושה כדי לגרוע מאחריות הספק או מזכויות הלמ"ס לפי ההתקשרות והדין.

3.8. סיום התקשרות עם ספקים

3.8.1. בסיום ההתקשרות, או עם סיום פעילותו של גורם מטעם הספק בפרויקט, יוודא הספק ביטול וחסימה של כלל הרשאות הגישה שניתנו לספק, לעובדיו, לקבלני המשנה ולכל גורם מטעמו, לרבות חשבונות משתמש, הרשאות ניהול, גישה מרחוק, תעודות דיגיטליות ואמצעי אימות, בהתאם לתחומי אחריותו ובתיאום עם הלמ"ס.

3.8.2. הספק ישיב ללמ"ס את כלל הציוד, אמצעי המחשוב, אמצעי הגישה, המסמכים והמידע שנמסרו לו או למי מטעמו במסגרת ההתקשרות, בהתאם להנחיות הלמ"ס ולתהליך מסירה מתועד.

3.8.3. הספק יעביר ללמ"ס, בהתאם לדרישתה, את כלל המידע והתוצרים שנצברו במסגרת ההתקשרות, לרבות הקלטות שיחות והמידע הנלווה אליהן, באמצעי מאובטח ובפורמט מוסכם המאפשר שימוש במידע, איתורו ואחזורו.

3.8.4. לאחר השלמת העברת המידע וקבלת אישור הלמ"ס בכתב, הספק ימחק או ישמיד באופן מאובטח את כלל עותקי המידע שנותרו ברשותו או בשליטתו, לרבות קובצי עבודה, קבצים זמניים, עותקים במערכות אחסון וגיבוי ומידע המוחזק אצל קבלני משנה, בכפוף להוראות הדין ולתקופות השמירה שנקבעו במסמך זה.

3.8.5. מידע אשר קיימת חובה לשמרו לאחר סיום ההתקשרות, לרבות לוגים או הקלטות, יישמר לתקופה הנדרשת בלבד, תוך הגבלת הגישה אליו, מניעת שימוש בו לכל מטרה אחרת ומחיקתו המאובטחת בתום תקופת השמירה, בהתאם להנחיות הלמ"ס ולהוראות הדין.

3.8.6. הספק יעביר ללמ"ס אישור חתום המעיד על השלמת החזרת הציוד, ביטול ההרשאות, העברת המידע ומחיקתו או השמדתו בהתאם להנחיות הלמ"ס. האישור יכלול פירוט חריגים ומידע שנותר בשמירה מכוח הוראות הדין או אישור הלמ"ס.

3.8.7. חובות הסודיות, הגנת המידע ואיסור השימוש או החשיפה של מידע הלמ"ס ימשיכו לחול על הספק וכל גורם מטעמו גם לאחר סיום ההתקשרות, למשך שלוש שנים לפחות או לתקופה ארוכה יותר ככל שנקבעה בדין, במכרז או בהסכם.

4. תכנון ארכיטקטורה, רכש ואישור טכנולוגיות

4.1. תכנון ואישור ארכיטקטורת הפתרון

4.1.1. הספק יגיש ללמ"ס מסמכי תכנון וארכיטקטורה בהתאם לשלבי הפרויקט, לרבות תכנון־על (HLD), תכנון מפורט (LLD), מיפוי מערכות וממשקים, רכיבי התשתית והאבטחה, תהליכי עבודה, סיכונים ובקרות אבטחת מידע.

4.1.2. מסמך תכנון־העל (HLD) יוצג לאחר בחירת הספק וטרם תחילת היישום. המסמך יכלול את ארכיטקטורת הפתרון, רכיבי המחשוב והתקשורת, הפרדת סביבות, ממשקים למערכות הלמ"ס ולמערכות חיצוניות, זרימות מידע, מנגנוני הזדהות והרשאות ובקרות אבטחת מידע.

4.1.3. מסמך התכנון המפורט (LLD) יוצג לאחר אישור ה־HLD ולפני תחילת יישום הפתרון. המסמך יכלול את תצורות הרכיבים, רשימות הציוד והיצרנים, הגדרות התקשורת והאבטחה, הממשקים, הרשאות הגישה, תוכנית המימוש, תוכנית הבדיקות ואמצעי ההגנה המתוכננים.

4.1.4. הספק יגיש במסגרת התכנון המפורט תוכנית ביצוע הכוללת לוחות זמנים, שלבי הקמה, רכש, התקנה, בדיקות קבלה (ATP), מסירה, רשימת רכיבים וכתב כמויות (BOQ), ככל שרלוונטיים לפרויקט. התכנון יוצג לאישור במסגרת סקר תכנון מפורט (CDR), בהתאם לדרישת הלמ"ס.

4.1.5. מסמכי התכנון יועברו לאישור הגורמים המוסמכים בלמ"ס, לרבות אגף הגנת הסייבר, אגף מערכות המידע והגורם העסקי הרלוונטי. לא יבוצע יישום או שינוי מהותי בארכיטקטורה ללא קבלת האישורים הנדרשים.

4.1.6. הספק יבטיח כי הארכיטקטורה, הטכנולוגיות ובקרות האבטחה מספקות מענה לדרישות נספח זה ולסיכונים שזוהו בתכנון ובסקרי אבטחת המידע. פערים שיזוהו במסמכי התכנון או ביישום יתוקנו על ידי הספק ויועברו לאישור חוזר בהתאם לצורך.

4.2. תיעוד מערכות ושינויים

4.2.1. הספק יתעד את המערכות, התשתיות, רכיבי התקשורת, הממשקים, התצורות והשינויים הטכנולוגיים הרלוונטיים לפרויקט, ויעדכן את התיעוד במהלך תקופת ההתקשרות.

4.2.2. עם השלמת הקמת הפתרון, הספק יגיש תיק תיעוד מעודכן (As-Built), המשקף את התצורה שיושמה בפועל, לרבות שינויים שאושרו במהלך הפרויקט.

4.2.3. התיעוד יישמר באופן מאובטח ויועבר ללמ"ס בהתאם לדרישתה, תוך הגבלת הגישה למידע טכנולוגי רגיש ולפרטי תצורה ואבטחה.

4.3. רכש ושימוש בטכנולוגיות

4.3.1. הספק לא ירכוש, יטמיע או יעשה שימוש במסגרת הפרויקט במוצרי חומרה, תוכנה, שירותים, רכיבי צד שלישי או טכנולוגיות שלא אושרו על ידי הגורמים המוסמכים בלמ"ס, בהתאם להוראות המכרז.

4.3.2. רכש או שילוב של מוצרים ושירותים מצד שלישי המחייבים אישור הלמ"ס, לרבות ועדת תוכנה ורכש, אגף מערכות המידע, הייעוץ המשפטי ואגף הגנת הסייבר, יבוצעו רק לאחר קבלת האישורים הנדרשים ובהתאם לתחומי סמכותם.

4.3.3. שימוש במוצרי מדף, בתוכנה שפותחה על ידי הספק או בטכנולוגיות צד שלישי יחייב הצגת מסמכי אבטחת מידע, לרבות תוצאות בדיקות אבטחה שבוצעו על ידי גורם מקצועי מתאים, בהתאם לדרישת הלמ"ס.

4.3.4. הספק יעשה שימוש במוצרים ובטכנולוגיות נתמכים ומתוחזקים, העומדים בתקני אבטחת מידע ובפרקטיקות מקובלות, ובעלי אופק תחזוקה ועדכוני אבטחה של שלוש שנים לפחות ממועד ההטמעה המתוכנן.

4.3.5. שינוי או החלפה של רכיב טכנולוגי שאושר, לרבות שינוי יצרן, מוצר, גרסה מהותית או ארכיטקטורה, המחייבים בחינה מחודשת של סיכוני אבטחת המידע, יובאו לאישור הלמ"ס מראש ובכתב.

4.3.6. אין באישור מוצר, טכנולוגיה או מסמך תכנון על ידי הלמ"ס כדי לגרוע מאחריות הספק לתקינות הפתרון, לאבטחתו ולעמידתו בהוראות המכרז וההסכם.

5. הגנה על המידע

5.1. עקרונות לניהול ושמירת המידע

5.1.1. מידע מהסקרים ונתוני הנסקרים, לרבות פרטים מזהים, תשובות לשאלונים, נתונים פיננסיים ומידע אישי או רגיש שנאסף במסגרת הפרויקט, יישמרו, ינוהלו ויעובדו במערכות הלמ"ס המאושרות בלבד, ובפרט במערכת אנ"ס, אלא אם ניתן אישור חריג מראש ובכתב מאת אגף הגנת הסייבר בלמ"ס. במידה ויוחלט כי פרטים מסויימים אודות המתנדבים יוחזקו במערכות הספק, יוגדרו על ידי הלמ"ס הנחיות מתאימות לנושא המידע הנשמר, מטרת שמירת המידע, תקופת השמירה והבקרות הנדרשות.

5.1.2. הספק יהיה רשאי לנהל במערכותיו מידע תפעולי הדרוש למתן השירות, ובלבד שסוגי המידע, המערכות, הרשאות הגישה ואמצעי ההגנה אושרו מראש על ידי הלמ"ס. לא יישמר במערכות הספק מידע אישי או רגיש על נסקרים, אלא באישור מפורש.

5.1.3. הספק ינקוט אמצעים להגנה על מידע הלמ"ס מפני חשיפה, העתקה, שינוי, מחיקה, אובדן, שימוש בלתי מורשה או פגיעה בזמינותו, בכל שלבי הטיפול במידע

5.2. קבלה, העברה והוצאת מידע

5.2.1. העברת מידע בין הלמ"ס לספק, ככל שנדרשת ואושרה, תתבצע באמצעות ממשקי API מאובטחים, כספות להעברת קבצים או ערוצי תקשורת מוצפנים ומבוקרים שאושרו על ידי הלמ"ס, לרבות שימוש בתשתית VPN בהתאם לארכיטקטורה המאושרת.

5.2.2. חל איסור להעביר מידע אישי, רגיש, עסקי או טכנולוגי של הלמ"ס באמצעות דוא"ל פרטי, שירותי ענן, יישומי מסרים, שירותי שיתוף קבצים, מדיה נתיקה או כל ערוץ בלתי מאושר אחר.

5.2.3. העברת מידע תפעולי שאינו רגיש תתאפשר באמצעי תקשורת ארגוניים מאושרים, בהתאם לסיווג המידע ולהנחיות הלמ"ס. לא ייעשה שימוש בשירותים ציבוריים או בלתי מנוהלים לצורך העברת מידע הלמ"ס.

5.2.4. הוצאת מידע ממערכות הלמ"ס או מסביבת הפרויקט, לרבות נתונים, קבצים, מסמכי ארכיטקטורה, תצורות מערכת ותיעוד טכנולוגי רגיש, תחייב אישור מראש של הלמ"ס ותתבצע באמצעים המאושרים בלבד. מידע שנאסר לייצוא יהיה זמין לעיון בסביבה מאושרת בלבד.

5.3. גישה למידע והעברתו לסוקרים

5.3.1. הגישה למידע הלמ"ס תוגבל למשתמשים ולגורמים שאושרו מראש, בהתאם לתפקידם, לצורך העסקי ולעקרון ההרשאה המזערית (Least Privilege).

5.3.2. הסוקרים יקבלו גישה למנות מידע מדודות, בהתאם למשימות שהוקצו להם ולמידע ההכרחי לביצוע הסקרים. לא תתאפשר גישה גורפת לכלל רשומות הנסקרים או למידע שאינו נדרש לתפקידם.

5.3.3. הצגת מידע לסוקרים והעברת נתונים בין מערכות הפרויקט יתבצעו באמצעות ממשקים אפליקטיביים מאובטחים ומוצפנים, בהתאם לארכיטקטורה ולהרשאות שאושרו על ידי הלמ"ס, ללא שמירה מקומית בלתי מאושרת בתחנות הקצה.

5.3.4. הספק יבטיח תיעוד פעולות גישה ושימוש במידע במערכות שבאחריותו, לרבות זהות המשתמש, מועד הגישה, המערכת או המשאב, סוג הפעולה ותוצאתה, בהתאם לדרישות הניטור המפורטים בנספח זה

5.4. שמירה על מידע וסודיות

5.4.1. הספק ישמור על סודיות מידע הלמ"ס וימנע את חשיפתו לעובדים, לקבלני משנה, לספקים או לגורמים אחרים שלא אושרו לגשת אליו במסגרת השירות.

5.4.2. הספק לא יעתיק, יפרסם, יעביר, ישתף או יעשה שימוש במידע של הלמ"ס או במידע שנצבר במסגרת הפרויקט, אלא לצורך מתן השירות ובהתאם להוראות ההתקשרות ולאישורי הלמ"ס.

5.4.3. הספק יישם נהלים ובקרות להגנה על מידע ולמניעת דלף מידע, לרבות בקרות גישה, הצפנה, הגבלת אפשרויות העתקה וייצוא, אבטחת אמצעי אחסון ותיעוד פעולות רגישות, בהתאם לסוג המידע ולמערכות שבהן הוא מנוהל.

5.5. מחיקת מידע

5.5.1. מידע של הלמ"ס המוחזק במערכות הספק באישור, ואשר אינו נדרש עוד לצורך מתן השירות או מכוח חובת שמירה, יימחק באופן מאובטח בהתאם להנחיות הלמ"ס.

5.5.2. מחיקת מידע תבוצע באמצעות מנגנון מחיקה מאובטח המתאים לסוג אמצעי האחסון ולסיווג המידע, תוך תיעוד הפעולה והצגת אסמכתאות לפי דרישת הלמ"ס.

5.5.3. החזרת מידע, מחיקתו והשמדתו בסיום ההתקשרות יבוצעו בהתאם להוראות מסמך זה.

6. שימוש בשירותי בינה מלאכותית

6.1. שירותי בינה מלאכותית (AI)

6.1.1. הספק, עובדיו וקבלני המשנה מטעמו לא יעשו שימוש בכלי בינה מלאכותית, לרבות שירותים חיצוניים, מודלי שפה, כלי פיתוח מבוססי AI, תוספים, Agents או שירותי API, במסגרת מתן השירותים ללמ"ס, אלא באישור מראש ובכתב של אגף הגנת הסייבר בלמ"ס.

6.1.2. האיסור יחול גם על שימוש עקיף בכלי AI לצורכי פיתוח קוד, ניתוח תקלות, כתיבת סקריפטים, בדיקת תצורות, ניתוח לוגים, הכנת מסמכים, תיעוד מערכות, תמיכה טכנית או כל פעילות אחרת הקשורה לפרויקט, ככל שלא ניתן לה אישור כאמור.

6.1.3. חל איסור להזין, להעלות, להעתיק, להעביר או לחשוף לכלי בינה מלאכותית מידע רגיש, אישי, מסווג, עסקי או טכנולוגי של הלמ"ס, בין במישרין ובין בעקיפין, לרבות באמצעות קבצים, שאילתות (Prompts), ממשקי API, תוספים, Agents או חיבור למאגרי מידע. האיסור יחול, בין היתר, על סוגי המידע הבאים:

6.1.3.1. מסמכי ארכיטקטורה ותכנון של רשתות, מערכות מידע, אפליקציות, תשתיות מחשוב, סביבות ענן, ממשקים וזרימות מידע, לרבות מסמכי HLD ו־LLD.

6.1.3.2. דוחות מבדקי חוסן, מבדקי חדירות, סקרי סיכונים, סקרי קוד, ממצאי ביקורת אבטחת מידע ותוצאות בדיקות אבטחה.

6.1.3.3. מידע על חולשות אבטחה, פערי הגנה, ליקויים בתצורות מערכות, דרכי ניצול חולשות, אירועי סייבר וממצאי תחקור.

6.1.3.4. מידע הנוגע לתהליכים עסקיים או תפעוליים קריטיים ורגישים של הלמ"ס, לרבות נהלים פנימיים, תוכניות עבודה רגישות, פרוטוקולים וסיכומי דיונים שאינם מיועדים לפרסום.

6.1.3.5. פרטי ספקים, קבלני משנה ונותני שירותים של הלמ"ס, לרבות שמות, כתובות, פרטי התקשרות, תפקידים, שירותים הניתנים על ידם והקשרים שלהם למערכות ולתשתיות הלמ"ס.

6.1.3.6. מידע אישי, מידע מזהה פרט, מידע פיננסי, נתוני סקרים, פרטי נדגמים, נתוני משקי בית, תשובות לשאלונים וכל מידע רגיש או מסווג, לרבות מידע המסווג ברמת "שמור" ומעלה או מידע הנגזר ממנו.

6.1.3.7. שמות מערכות רגישות, מערכות הגנת סייבר, מוצרי אבטחת מידע, רכיבי תשתית, כתובות IP, שמות שרתים, פרטי רשת, תצורות אבטחה ומנגנוני הגנה המשמשים את הלמ"ס.

6.1.3.8. קוד מקור, סקריפטים, ספריות, קובצי תצורה, רכיבי תוכנה, תהליכי CI/CD, תיעוד פיתוח ופרטי סביבות פיתוח, בדיקות וייצור של מערכות רגישות של הלמ"ס.

6.1.3.9. מידע על גרסאות תוכנה, רכיבי תשתית, מוצרי אבטחה, חולשות ידועות, פערים ותצורות המאפשרים לזהות את רמת החשיפה של מערכות הלמ"ס או לתכנן מתקפה ממוקדת נגדן.

6.1.3.10. פרטי הזדהות, סיסמאות, מפתחות הצפנה, תעודות דיגיטליות, Tokens, API Keys, Secrets, קובצי חיבור למערכות, חשבונות שירות והרשאות גישה.

6.1.3.11. לוגים, התרעות אבטחה, תעבורת תקשורת, קובצי Dump, צילומי מסך, קובצי גיבוי, נתוני תחקור ותיעוד תפעולי העלולים לחשוף מידע רגיש או פרטים על מערכות הלמ"ס.

6.1.3.12. כל מידע אחר אשר חשיפתו עלולה לפגוע בסודיות, בשלמות או בזמינות מידע הלמ"ס, במערכותיה, בתהליכיה או באבטחת המידע שלה.

איסורים אלה יחולו גם כאשר השימוש בכלי הבינה המלאכותית עצמו אושר על ידי הלמ"ס. עיבוד סוג מידע כאמור יתאפשר רק לאחר קבלת אישור מפורש ונפרד מראש ובכתב של הגורמים המוסמכים בלמ"ס, בכפוף לסיווג המידע, למדיניות הלמ"ס ולהוראות הדין.

6.1.4. חל איסור להשתמש במידע של הלמ"ס לצורכי אימון, אימון חוזר (Fine-Tuning), שיפור מודלים, העברה לצד שלישי או שימוש למטרות אחרות שאינן נדרשות לשירות שאושר, ללא אישור מפורש מראש ובכתב של הלמ"ס.

6.1.5. הספק לא יחבר כלי AI או רכיב אוטומציה למערכות הלמ"ס, למערכות הספק המשמשות את הפרויקט, לסביבות פיתוח, לדפדפנים, למערכות הפעלה או לכלי ניהול ותפעול, אלא לאחר בחינת סיכוני אבטחת המידע וקבלת אישור מראש ובכתב של אגף הגנת הסייבר בלמ"ס.

6.1.6. כל בקשה לשימוש בכלי AI תכלול פירוט של מטרת השימוש, זהות הכלי והספק המפעיל אותו, סוגי המידע המעובדים, מיקום העיבוד והאחסון, הרשאות הגישה, אופן שמירת המידע ומחיקתו, מניעת שימוש במידע לאימון מודלים, העברתו לצדדים שלישיים ואמצעי האבטחה והניטור. הלמ"ס תהיה רשאית לדרוש שאלון הערכת סיכונים ומסמכים משלימים כתנאי לאישור השימוש.

6.1.7. עיבוד או אחסון מידע של הלמ"ס מחוץ לישראל באמצעות שירותי AI יחייבו אישור מראש ובכתב של הגורמים המוסמכים בלמ"ס, לרבות אגף הגנת הסייבר והייעוץ המשפטי, ובהתאם לסיווג המידע, למדיניות הלמ"ס ולהוראות הדין. לא תותר העברת מידע למיקום או למדינה שלא אושרו, והספק יוודא מחיקת המידע בתום העיבוד או תקופת השמירה שאושרה.

6.1.8. ככל שאושר שימוש בכלי AI, הספק יפעל לפי עקרון מזעור המידע, יגביל את השימוש למטרות שאושרו, ינקוט אמצעים למניעת חשיפת מידע בלתי מורשית ויתעד את מטרת השימוש, זהות המשתמש, הכלי שבו נעשה שימוש, סוגי המידע המעובדים והפעולות שבוצעו, בהתאם להנחיות הלמ"ס.

6.1.9. שימוש במודלי AI במסגרת פיתוח, הטמעה או הפעלה של רכיבי תוכנה עבור הלמ"ס יחייב בנוסף עמידה בדרישות אבטחת הפיתוח ובדרישות הייעודיות לאבטחת מודלי AI המפורטות בנספח הפיתוח המאובטח.

7. מחשוב ענן

7.1. שימוש בשירותי ענן והגנה על מידע הלמ"ס

7.1.1. הספק, עובדיו וקבלני המשנה מטעמו לא ישמרו, יאחסנו, יעבדו, ינהלו, יגבו או יעבירו מידע של הלמ"ס באמצעות שירותי ענן, שירותים מקוונים או פלטפורמות חיצוניות, אלא באישור מראש ובכתב של אגף הגנת הסייבר בלמ"ס.

7.1.2. האיסור יחול על כל סוגי המידע הקשורים לפרויקט, לרבות מידע אישי ורגיש, נתוני נסקרים, מידע עסקי, תפעולי וטכנולוגי, מסמכי תכנון וארכיטקטורה, קובצי תצורה, לוגים, קוד מקור, קובצי עבודה, גיבויים ומידע על מערכות ותשתיות הלמ"ס.

7.1.3. שימוש בשירותי דוא"ל, שיתוף קבצים ואחסון ארגוניים מבוססי ענן, לרבות Microsoft 365, Google Workspace ושירותים דומים, יתאפשר לצרכים תפעוליים שאושרו בלבד. לא יישמר או יועבר באמצעותם מידע של הלמ"ס שלא אושר במפורש, והספק יישם בקרות אבטחה מתאימות, לרבות MFA, בקרת הרשאות, הגנה מפני תוכן זדוני ומניעת דלף מידע (DLP).

7.1.4. בקשה לאישור שימוש בשירות ענן תכלול פירוט של השירות וספק השירות, מטרת השימוש, סוגי המידע, מיקום האחסון והעיבוד, הגורמים בעלי הגישה, מנגנוני ההגנה, העברת מידע לצדדים שלישיים, תקופות השמירה ואופן מחיקת המידע. האישור יחול רק על השימוש והמידע שהוגדרו בו.

7.1.5. הספק יוודא כי הוראות פרק זה חלות גם על שירותי ענן המופעלים על ידי קבלני משנה וספקי צד שלישי מטעמו, לרבות שירותי גיבוי, ניטור, תמיכה, אחסון ושיתוף מידע.

7.1.6. ככל שהספק יבקש לעשות שימוש בשירותי ענן במסגרת הפרויקט, יובהר כי השימוש מותנה, בין היתר, בקבלת אישור ועדת הענן של מערך הסייבר הלאומי, בהתאם להנחיות החלות על הלמ"ס. הספק מאשר כי ידוע לו שתהליך הבחינה והאישור עלול להימשך זמן ממושך ולעכב באופן משמעותי את הקמת הפרויקט או את אספקת השירותים, וכי אין כל התחייבות מצד הלמ"ס או מערך הסייבר הלאומי למתן האישור. הספק יישא באחריות לתכנון הפתרון וללוחות הזמנים בהתאם למגבלות אלו, ולא יסתמך על קבלת האישור במסגרת הצעתו או תוכנית העבודה ללא אישור מראש ובכתב.

8. תשתית סוקרי שטח

8.1. אמצעי מחשוב לסוקרי שטח (CAPI)

8.1.1. ביצוע הסקרים על ידי סוקרי השטח מטעם הספק יתבצע באמצעות מחשבים ניידים מוקשחים ומנוהלים באמצעות פתרון MDM **<u>שיסופקו על ידי הלמ"ס.</u>**

8.1.2. חל איסור לבצע את פעילות הסקרים באמצעות מחשבים אחרים של הספק או אמצעי מחשוב פרטיים אחרים שלא אושרו במפורש על ידי הלמ"ס.

8.1.3. הספק יוודא באופן מחזורי, כי סוקרי השטח עושים שימוש במחשבי הלמ"ס בלבד שהוקצו להם בלבד, ללא שינוי הגדרות האבטחה, התקנת תוכנות בלתי מורשות, הסרת אמצעי הגנה או חיבור התקנים שאינם מאושרים.

8.2. הזדהות וגישה למערכות הלמ"ס

8.2.1. ניהול זהויות המשתמשים, הרשאות הגישה ואמצעי ההזדהות למערכת אנ"ס יהיו באחריות הלמ"ס. הגישה תתבצע באמצעות חשבון משתמש אישי ואימות באמצעות סיסמה חד־פעמית (OTP), בהתאם למנגנון ההזדהות שתקבע הלמ"ס.

8.2.2. סוקרי השטח יורשו לגשת למערכות ולשירותים שהוגדרו לצורך ביצוע הסקרים בלבד, באמצעות ערוצי תקשורת מאובטחים ואמצעי גישה שאושרו על ידי הלמ"ס.

8.2.3. לא תתאפשר גישה מרחוק אחרת לרשתות או למערכות הלמ"ס, או למערכות הספק הרלוונטיות לשירות, לרבות גישה לצורכי ניהול, תחזוקה ותמיכה, אלא באישור מראש ובכתב של אגף מערכות המידע ואגף הגנת הסייבר בלמ"ס.

8.3. אבטחת ציוד ומניעת חשיפת מידע

8.3.1. הספק יוודא כי סוקרי השטח פועלים בהתאם להנחיות הלמ"ס לשמירה על אמצעי המחשוב שנמסרו להם, הגנה מפני גישה בלתי מורשית ומניעת חשיפת מידע בעת עבודה מחוץ לחצרות הלמ"ס.

8.3.2. מידע הסקרים יישמר ויעובד במערכות הלמ"ס המאושרות בלבד. לא תתאפשר שמירה מקומית של מידע הסקרים במחשבי הסוקרים או העברתו למערכות ולשירותים שאינם מאושרים, בהתאם להוראות פרק 5 במסמך זה.

8.3.3. הספק יבצע בקרות אפקטיביות לזיהוי ואיתור מחשבים שאבדו או נגנבו, בין היתר באמצעות בדיקות מדגמיות מול הסוקרים.

8.3.4. דיווח על אובדן או גניבת ציוד, חשד לחשיפת מידע או אירוע אבטחת מידע יבוצע בהתאם להנחיות בנושא החזרת ציוד וביטול הרשאות בסיום פעילות הסוקר יבוצעו בהתאם לאמור במסמך זה.

9. סביבת המחשוב והתקשורת של הפרויקט (סביבת הספק וה- call Center)

9.1. הפרדת סביבות ותשתיות

9.1.1. הספק יקים ויפעיל סביבת מחשוב וטלפוניה ייעודית לפרויקט, באמצעות תשתיות קיימות או חדשות, בכפוף לעמידה בדרישות אבטחת המידע של הלמ"ס.

9.1.2. סביבת הפרויקט תופרד פיזית או לוגית מיתר רשתות הספק, מסביבות של לקוחות אחרים ומסביבות שאינן משמשות את הפרויקט. ההפרדה תכלול בקרות תקשורת, הרשאות וניהול המונעות גישה בלתי מורשית בין הסביבות.

9.1.3. תשתית הפרויקט תכלול סגמנטים נפרדים לתחנות עבודה, שרתים, תשתיות טלפוניה ומערכות ניהול, באמצעות VLAN, סגמנטציה לוגית או הפרדה פיזית, בהתאם לארכיטקטורה שתאושר על ידי הלמ"ס.

9.1.4. התקשורת בין הסגמנטים ובין סביבת הפרויקט לרשתות אחרות תוגבל באמצעות Firewall לשירותים, כתובות, פרוטוקולים ופורטים שאושרו בלבד. כל תקשורת שאינה מאושרת תיחסם כברירת מחדל (Deny by Default).

9.1.5. הספק יפעיל בקרות הגנה וניטור לתעבורת הרשת, לרבות Firewall בעל יכולות IPS/IDS, Anti-Malware, Anti-Bot וסינון תוכן, בהתאם לארכיטקטורה ולסיכוני הפרויקט.

9.2. תקשורת וגישה למערכות הלמ"ס

9.2.1. הגישה מסביבת מוקד הספק למערכת אנ"ס ולמערכות נוספות שאושרו לצורך הפרויקט תתבצע באמצעות קישור VPN מאובטח בין רשת הספק לתשתית הלמ"ס, בהתאם לארכיטקטורת התקשורת שתאושר.

9.2.2. תחנות העבודה של סוקרי המוקד יורשו לגשת למערכות, ליישומים ולשירותים הנדרשים לביצוע הסקרים בלבד. הגישה תוגבל בהתאם להרשאות המשתמש ולחוקי התקשורת שאושרו.

9.2.3. לא תתאפשר גלישה ישירה לאינטרנט, גישה לרשתות זרות או שימוש בשירותים חיצוניים מתחנות העבודה של סוקרי המוקד, אלא באישור מראש ובכתב של אגף הגנת הסייבר בלמ"ס.

9.2.4. גישה נכנסת לסביבת הפרויקט תוגבל למערכות, לכתובות ולשירותים שאושרו במפורש. לא תתאפשר גישה מרשתות אחרות של הספק או מגורמים חיצוניים, למעט חיבורים שאושרו מראש ובכתב לצורכי ניהול, תחזוקה או תמיכה.

9.2.5. הגישה למערכת אנני"ס תתבצע באמצעות חשבון משתמש אישי ואימות באמצעות סיסמה חד־פעמית (OTP), בהתאם למנגנוני ההזדהות וההרשאות שתקבע הלמ"ס.

9.3. רשת ניהול ותשתיות תקשורת

9.3.1. הספק יפעיל רשת ניהול ייעודית ומופרדת לצורך ניהול שרתים, תשתיות וירטואליזציה, רכיבי תקשורת, מערכות אבטחת מידע ותשתיות נוספות המשמשות את הפרויקט.

9.3.2. הגישה לרשת הניהול ולממשקי הניהול תותר לגורמים מורשים בלבד, באמצעות חשבונות אישיים, הזדהות רב־שלבית (MFA) והרשאות בהתאם לתפקיד ולעקרון ההרשאה המזערית.

9.3.3. ניהול רכיבי התקשורת והתשתית יתבצע באמצעות פרוטוקולים מאובטחים בלבד, כגון HTTPS, SSH, SFTP ו־SNMPv3, בהתאם לתמיכת הרכיב ולצורך התפעולי. שימוש בפרוטוקולים בלתי מאובטחים, כגון Telnet, HTTP, FTP ו־SNMPv1/v2c, ייחסם אלא אם אושר חריג במפורש.

9.3.4. גישה מרחוק לצורכי ניהול, תחזוקה או תמיכה בסביבת הפרויקט לא תתאפשר ללא אישור מראש ובכתב של הגורמים המוסמכים בלמ"ס. כל גישה שאושרה תוגבל למערכות ולפעולות הנדרשות, תחייב הזדהות חזקה ותהיה נתונה לניטור ולתיעוד.

9.3.5. גישה לאינטרנט מרשת הניהול, ככל שנדרשת ואושרה על ידי הלמ"ס, תתבצע באמצעות מנגנוני סינון, בקרת גלישה ובדיקת קבצים. לא תתאפשר גלישה ישירה ובלתי מבוקרת.

9.3.6. הקשחת רכיבי התקשורת והתשתיות, ניהול עדכוני אבטחה, תיעוד שינויי תצורה וניטור פעילות יתבצעו בהתאם לדרישות הפרקים הייעודיים במסמך זה.

10. אבטחת מערכות המחשוב של הספק

10.1. הנחיות הקשחה כלליות

10.1.1. הספק יקשיח את כלל מערכות המחשוב המשמשות את הפרויקט, לרבות תחנות עבודה, שרתים, מערכות הפעלה, תשתיות וירטואליזציה ורכיבי אחסון, בהתאם להנחיות היצרן, לתקני הקשחה מקובלים ולתצורה שתאושר על ידי הלמ"ס.

10.1.2. הספק יפעיל מערכות הפעלה, תוכנות ורכיבי תשתית בגרסאות נתמכות ומעודכנות, ויבצע עדכוני אבטחה בהתאם לחומרת החולשות ולהנחיות הלמ"ס. עדכוני אבטחה יותקנו לא יאוחר מחודש ממועד פרסומם, אלא אם נקבע מועד מחמיר יותר במסמך זה או בהנחיות אגף הגנת הסייבר בלמ"ס.

10.1.3. בתחנות העבודה ובשרתים יופעל פתרון EDR מאושר על ידי הלמ"ס, הכולל הגנה בזמן אמת, זיהוי איומים, התראות וניהול מרכזי.

10.1.4. הספק יפעיל חומת אש מקומית ברכיבים הרלוונטיים, יחסום שירותים ופורטים שאינם נדרשים וימנע הפעלת יישומים בלתי מורשים.

10.2. ניהול תחנות באמצעות MDM/EMM ובקרת תאימות

10.2.1. כל תחנה תירשם למערכת MDM/EMM לפני הפעלתה ותזוהה באמצעות מזהה חד־ערכי ותעודה דיגיטלית ייעודית (Device Certificate), שתנוהל לאורך מחזור חיי התחנה.

10.2.2. הספק ינהל מלאי מעודכן של התחנות הכולל מזהה, מספר סידורי, גרסת מערכת הפעלה, שיוך לעמדה או לעובד, מצב הצפנה, מצב EDR וסטטוס תאימות.

10.2.3. מערכת הניהול תאכוף מדיניות אבטחת מידע אחידה ומאושרת, תוך הפרדה לוגית בין תחנות הפרויקט, מדיניותן, הלוגים והרשאות הניהול שלהן לבין סביבות אחרות של הספק ולקוחותיו.

10.2.4. חיבור תחנה לרשת הפרויקט או למערכות המוקד יותנה בעמידתה במדיניות התאימות (Device Compliance), הכוללת לפחות:

10.2.4.1. רישום תקין במערכת MDM/EMM וזיהוי התקן מאומת.

10.2.4.2. מערכת הפעלה נתמכת ומעודכנת.

10.2.4.3. הצפנת דיסק פעילה ותקינה.

10.2.4.4. EDR ו־Firewall מקומי פעילים ותקינים.

10.2.4.5. הפעלת מנגנוני תיעוד ואיסוף אירועי אבטחה.

10.2.4.6. היעדר תוכנות אסורות, שינויי תצורה בלתי מורשים או אינדיקציות לפגיעה באמצעי ההגנה.

10.2.4.7. סטטוס תאימות עדכני בהתאם למדיניות המאושרת

10.2.5. תחנה שאינה עומדת בדרישות התאימות, או שלא דיווחה למערכת הניהול במשך פרק הזמן שהוגדר, תיחסם מגישה למערכות הפרויקט עד להסדרת הפער.

10.2.6. אכיפת הגישה לרשת הס]ק תתבצע באמצעות מנגנון בקרת גישה לרשת או למערכות (כגון NAC), המשולב עם סטטוס התאימות של התחנה (Host Check על המוודא הקשחת העמדה כאמור לעיל).

10.3. משתמשים, הזדהות והרשאות

10.3.1. הגישה לתחנות ולמערכות הפרויקט תתאפשר באמצעות חשבונות משתמש אישיים בלבד, בהתאם לתפקיד ולעקרון ההרשאה המזערית. לא יתאפשר שימוש בחשבונות משותפים.

10.3.2. משתמשי המוקד יפעלו בהרשאות Standard User בלבד. הרשאות ניהול יוקצו לחשבונות נפרדים של מנהלנים מורשים, תוך שימוש ב־MFA ותיעוד פעולות הניהול.

10.3.3. חשבונות ברירת מחדל ו־Guest שאינם נדרשים יושבתו. סיסמאות של חשבונות ניהול מקומיים ינוהלו באמצעות מנגנון מרכזי לסיסמאות ייחודיות ומבוקרות.

10.3.4. הגישה למערכות המוקד ולמערכות הלמ"ס תתבצע באמצעות מנגנוני הזדהות ובקרת גישה מאושרים, לרבות MFA בהתאם לרגישות המערכת ולמדיניות הלמ"ס.

10.3.5. תחנות העבודה יינעלו לאחר עשר דקות לכל היותר של חוסר פעילות, ושחרור הנעילה יחייב הזדהות מחודשת.

10.3.6. הקצאת הרשאות, סקירתן וביטולן יבוצעו בהתאם לפרק ניהול המשתמשים וההרשאות במסמך זה.

10.4. הקשחת תחנות העבודה

10.4.1. התחנות יפעלו באמצעות Windows 11 בגרסה נתמכת ומעודכנת ויוקשחו בהתאם ל־Microsoft Security Baseline או CIS Benchmark, ולתצורת ההקשחה שתאושר על ידי הלמ"ס.

10.4.2. הספק יפעיל פתרון EDR מרכזי ומנוהל, Firewall מקומי ומנגנון Application Allowlisting, המאפשרים הפעלה של יישומים, רכיבים וסקריפטים מאושרים בלבד.

10.4.3. ייחסמו יישומים וכלים שאינם נדרשים לפעילות המוקד, לרבות Office, Notepad, PowerShell, כלי צילום מסך, תוכנות שיתוף קבצים, כלי ניהול וממשקי פקודות, למעט חריגים שאושרו במפורש.

10.4.4. כלל הכוננים הפנימיים יוצפנו באמצעות BitLocker או פתרון מאושר שווה ערך. מפתחות השחזור ינוהלו מרכזית, בגישה מוגבלת ומתועדת. במחשבים ניידים תוגדר גם הזדהות לפני אתחול (Pre-Boot Authentication), באמצעות TPM+PIN או מנגנון מאושר שווה ערך.

10.4.5. הגדרות BIOS/UEFI יוגנו מפני שינוי בלתי מורשה, יופעל Secure Boot וייחסם אתחול ממדיה חיצונית שאינה מאושרת.

10.4.6. הספק יישם Device Control לחסימת התקני אחסון, USB, טלפונים ניידים, מדפסות, Bluetooth והתקנים היקפיים בלתי מורשים. התקנים הנדרשים לפעילות המוקד יוגדרו כחריגים מאושרים.

10.4.7. לא תתאפשר התקנה או הפעלה של מכונות וירטואליות מקומיות, לרבות באמצעות Hyper-V או VMware, אלא באישור מראש של הלמ"ס.

10.4.8. הספק יבצע עדכוני אבטחה למערכת ההפעלה, לתוכנות, לדרייברים ולקושחה באמצעות מנגנון ניהול מרכזי, בהתאם למועדים שנקבעו במדיניות אבטחת המידע.

10.4.9. חל איסור על עובדים להשבית אמצעי הגנה, לשנות תצורות אבטחה, להסיר את התחנה ממערכת הניהול או להתקין מערכת הפעלה מחדש. ניסיונות לביצוע פעולות אלה ינוטרו ויתוחקרו.

10.5. הגבלות תקשורת וגלישה

10.5.1. תחנות העבודה יחוברו לרשת הפרויקט באמצעות תקשורת קווית בלבד. לא תתאפשר התחברות באמצעות Wi-Fi, רשת סלולרית או התקני תקשורת אלחוטיים.

10.5.2. התחנות יורשו לתקשר רק עם מערכות הפרויקט, מערכות הלמ"ס ושרתי הניהול, העדכון והאבטחה שאושרו לצורך הפעלתן.

10.5.3. הגישה ליעדי התקשורת תוגבל באמצעות רשימת כתובות IP, שמות FQDN, פרוטוקולים ופורטים מאושרים (Allowlist). לא תתאפשר גלישה חופשית לאינטרנט.

10.5.4. עדכוני מערכת הפעלה, EDR ו־MDM/EMM יבוצעו באמצעות שרתי הספק או שירותי עדכון מאושרים בלבד, ללא פתיחת גישה חופשית לאינטרנט.

10.5.5. ייחסמו גישה לשיתופי קבצים, משאבי רשת, שירותי הדפסה, ממשקי ניהול ויעדים אחרים שאינם נדרשים לפעילות המוקד, לרבות משאבים ברשת המקומית.

10.5.6. לא תתאפשר הפעלת Routing, Network Bridging, שיתוף חיבור אינטרנט או שירותי Proxy בלתי מורשים בתחנות העבודה.

10.5.7. תיחסם גלישה לאתרים שאינם מאושרים, הורדת קבצים, התקנת תוספי דפדפן ושימוש בשירותי דוא"ל חיצוניים. שימוש בדוא"ל פנימי של הספק יתאפשר רק באישור הלמ"ס ובתנאים שייקבעו.

10.6. מניעת דלף מידע

10.6.1. לא תתאפשר שמירה מקומית של מידע סקרים או מידע רגיש של הלמ"ס בתחנות העבודה, בפרופילי המשתמשים או בשיתופים מקומיים, למעט מידע טכני הנדרש להפעלת התחנה ואושר.

10.6.2. הספק יפעיל בקרות למניעת העתקה, הורדה, הדפסה, צילום מסך, העברת קבצים ושימוש בלתי מורשה בלוח הגזירים (Clipboard), בהתאם לדרישות הלמ"ס.

10.6.3. חל איסור להעביר מידע של הלמ"ס לשירותי ענן, לדוא"ל, לתוכנות שיתוף קבצים או למערכות שאינן מאושרות.

10.6.4. הספק ינקוט אמצעים פיזיים ולוגיים למניעת צפייה בלתי מורשית במידע המוצג על מסכי התחנות ולמניעת גישה לעמדות העבודה.

10.7. ניטור, זיהוי חריגות וטיפול באירועים

10.7.1. הספק ינטר באופן מרכזי את מצב התחנות, לרבות סטטוס MDM/EMM, EDR, הצפנה, עדכונים, התקנת תוכנות, שינויי תצורה וניסיונות עקיפת מדיניות האבטחה.

10.7.2. לוגים ממערכת ההפעלה, MDM/EMM, EDR ו־Device Control יועברו למערכת SIEM. התיעוד יכלול אירועי הזדהות, פעולות מנהלנים, שינויי מדיניות, התקנת תוכנות, חיבור התקנים וניסיונות גישה בלתי מורשים.

10.7.3. אירועים חריגים יפיקו התראה למוקד הניטור של הספק. במקרה של פגיעה באבטחת התחנה תתאפשר חסימת גישה, בידוד או נעילה מרחוק בהתאם לחומרת האירוע.

10.7.4. הספק יידע את העובדים מראש על אמצעי הניהול והניטור המופעלים בתחנות, סוגי המידע הנאספים, מטרות השימוש והגורמים הרשאים לגשת אליו, בהתאם להוראות הדין.

10.7.5. אירועים העלולים להשפיע על מידע הלמ"ס או מערכותיה ידווחו ויטופלו בהתאם להוראות פרק ניהול אירועי אבטחת המידע במכרז.

10.8. ניהול מרחוק, תחזוקה וגריעת תחנות

10.8.1. מערכת הניהול תאפשר הפצת מדיניות, התקנת עדכונים, נעילה מרחוק, חסימת גישה, בידוד מחשב ומחיקה מרחוק (Remote Wipe), בהתאם ליכולות הפתרון המאושר.

10.8.2. ממשקי הניהול של מערכת MDM/EMM לא ייחשפו ישירות לאינטרנט. גישת מנהלנים תתבצע באמצעות ערוץ ניהול מאובטח, חשבונות אישיים, MFA והרשאות מזעריות, תוך תיעוד הפעולות.

10.8.3. השתלטות מרחוק, צפייה במסך, העברת קבצים או שימוש בלוח הגזירים במסגרת תמיכה ותחזוקה יחייבו אישור מראש ובכתב של אגף הגנת הסייבר בלמ"ס. אישור תמיכה לא יהווה היתר לגישה למידע סקרים או להעברתו.

10.8.4. פעולות ניהול ותחזוקה לא יאפשרו עקיפה של מנגנוני הגישה או יצירת נתיב בלתי מבוקר למערכות הלמ"ס. תחזוקת תחנה שאינה עומדת בדרישות התאימות תתאפשר באמצעות ערוץ מוגבל ומאושר בלבד, ללא גישה למידע הסקרים.

10.8.5. במקרה של אובדן, גניבה או חשד לפגיעה בתחנה, הספק יחסום את הגישה למערכות הפרויקט, יבטל אישורי גישה רלוונטיים ויבצע נעילה או מחיקה מרחוק ככל שנדרש, תוך תיעוד הפעולות ושימור ראיות בהתאם לנוהל האירועים.

10.8.6. הספק ינהל מעקב אחר שיוך התחנות, העברתן בין עובדים, הוצאתן לתיקון וגריעתן. לפני העברה, תיקון חיצוני או גריעה יבוצעו ביטול גישה, מחיקת מידע מאובטחת ותיעוד מתאים.

10.9. בדיקות ואישור הפעלה

10.9.1. לפני הפעלת התחנות בפרויקט יבצע הספק בדיקות לאימות מנגנוני ההקשחה, חסימת תוכנות והתקנים, הגבלות תקשורת, מניעת דלף מידע, ניטור ואכיפת מדיניות התאימות.

10.9.2. הבדיקות יכללו ניסיונות התחברות באמצעות מחשב בלתי מנוהל או שאינו עומד בדרישות האבטחה, וניסיונות לעקיפת בקרות באמצעות ממשקי הניהול והתחזוקה.

10.9.3. הספק יעביר ללמ"ס את תוצאות הבדיקות ואסמכתאות ליישום הבקרות, ויטפל בפערים שיזוהו לפני הפעלת השירות.

10.9.4. הפעלת התחנות במסגרת הפרויקט תותנה באישור אגף הגנת הסייבר בלמ"ס.

10.10. דרישות נוספות לסביבת VDI

10.10.1. במידה והספק יפעיל סביבת VDI אזי היא תוקם ותנוהל בתצורה מאושרת ומוקשחת, תוך הפרדה בין משתמשים ומניעת גישה לסביבות עבודה אחרות.

10.10.2. תיחסם העברת מידע בין סביבת VDI לתחנת הקצה, לרבות באמצעות Clipboard, העברת קבצים, כוננים ממופים, הדפסה והפניית התקנים מקומיים (Device Redirection), אלא באישור מראש של הלמ"ס.

10.10.3. הספק ימנע שמירת מידע הסקרים בפרופילי המשתמשים, במערכות המקומיות או בתחנות המתחברות לסביבת VDI, למעט מידע טכני הנדרש להפעלת השירות ואושר.

10.11. הקשחת שרתים ותשתיות וירטואליזציה

10.11.1. הספק יקצה תשתית שרתים ייעודית או מופרדת לוגית עבור הפרויקט, תוך הפרדה מיתר מערכות הספק ומסביבות לקוחות אחרים.

10.11.2. השרתים יפעלו באמצעות מערכות הפעלה נתמכות ומעודכנות ויוקשחו בהתאם להנחיות היצרן ולתצורה שתאושר על ידי הלמ"ס.

10.11.3. ממשקי ניהול שרתים, תשתיות וירטואליזציה ומערכות אחסון יופרדו מממשקי השירות והיישומים, והגישה אליהם תתאפשר מרשת הניהול המאושרת בלבד.

10.11.4. הספק יחסום חיבור התקני אחסון חיצוניים בלתי מורשים לשרתים באמצעות בקרות Device Control, בהתאם ליכולות המערכת.

10.11.5. כונני שרתים פיזיים המכילים מידע של הלמ"ס יוצפנו באמצעות BitLocker או פתרון הצפנה שווה ערך, תוך ניהול מאובטח של מפתחות השחזור.

10.11.6. ייחסמו חשבונות ושירותים שאינם נדרשים, יוגבלו הרשאות ניהול וייאסר שימוש בשיתופי קבצים בעלי הרשאות גורפות כגון Everyone או Domain Users.

10.12. אחסון וגיבוי

10.12.1. מערכות האחסון המשמשות את תשתיות הפרויקט יופרדו לוגית או פיזית ממערכות אחסון של לקוחות אחרים ומסביבות שאינן משמשות את הפרויקט.

10.12.2. הגישה למערכות האחסון והגיבוי תוגבל לגורמים ולמערכות מורשים בלבד, תוך הפרדה בין הרשאות צפייה, ניהול, שחזור ומחיקה.

10.12.3. הספק יגן על מערכות האחסון והגיבוי באמצעות בקרות גישה, הצפנה, הגנה מפני מחיקה בלתי מורשית ובדיקות שחזור תקופתיות.

10.12.4. הספק לא יגבה ולא ישמור במערכותיו מידע סקרים, מידע אישי על נסקרים או נתונים המנוהלים במערכת אנ"ס, אלא באישור מראש ובכתב של הלמ"ס. גיבוי תשתיות, תצורות ומידע תפעולי שאושר יתבצע בהתאם לפרק הרציפות התפעולית במסמך זה.

11. אבטחת תשתיות טלפוניה

11.1. הפרדה והגנת רשת הטלפוניה

11.1.1. הספק יהיה רשאי להשתמש בתשתיות הטלפוניה הקיימות אצלו, לרבות מערכות VoIP, בכפוף לעמידה בדרישות אבטחת המידע של הלמ"ס ולאישור הארכיטקטורה בהתאם להנחיות מסמך זה.

11.1.2. תשתיות הטלפוניה של הפרויקט יופרדו פיזית או לוגית מסביבות מחשוב וטלפוניה אחרות באמצעות VLAN ייעודי, סגמנטציה לוגית או הפרדה פיזית, ובאמצעות בקרות Firewall המגבילות את התקשורת בין הסביבות.

11.1.3. לא תתאפשר גישה ישירה מטלפוני IP לאינטרנט, לרשתות מחשוב אחרות של הספק או לתחנות הסוקרים, למעט תקשורת הנדרשת להפעלת השירות ואושרה במפורש.

11.1.4. התקשורת בין טלפוני IP, המרכזייה, מערכות הניהול ושרתי ההקלטות תוגבל לכתובות, פרוטוקולים ופורטים מאושרים בלבד. תקשורת ישירה בין טלפוני קצה (Point to Point) תיחסם, אלא אם אושרה מראש.

11.1.5. הספק יפעיל מנגנוני בקרה וניטור לתעבורת הטלפוניה, לרבות תעבורת SIP, לצורך זיהוי ניסיונות תקשורת חריגים, גישה בלתי מורשית ושינויים בלתי מאושרים, בהתאם לדרישות פרק הניטור במסמך זה.

11.1.6. הספק יגן על תעבורת האיתות והשמע של מערכות הטלפוניה באמצעות פרוטוקולי תקשורת מוצפנים, כגון SIP over TLS ו־SRTP, בהתאם ליכולות הפתרון ולתצורה שתאושר על ידי הלמ"ס.

11.2. הקשחת טלפוני IP ומערכות ניהול

11.2.1. הספק יקשיח את טלפוני ה־IP, המרכזיות ורכיבי הטלפוניה בהתאם להנחיות היצרן ולתצורה שאושרה, לרבות ביטול שירותים, ממשקים והגדרות ברירת מחדל שאינם נדרשים.

11.2.2. הגישה לממשקי הניהול של מערכות הטלפוניה תתאפשר מרשת הניהול המאושרת בלבד, באמצעות פרוטוקולים מאובטחים כגון HTTPS, SSH, SFTP ו־SNMPv3. פרוטוקולים בלתי מאובטחים ייחסמו.

11.2.3. לא ייעשה שימוש בממשקים אלחוטיים, לרבות Wi-Fi או Bluetooth, בטלפוני הקצה של הפרויקט, אלא באישור מראש ובכתב של הלמ"ס.

11.2.4. הספק יפעיל מנגנון זיהוי ייחודי ומאובטח בין טלפוני הקצה למערכות הניהול, באמצעות תעודה דיגיטלית או מנגנון זיהוי מאובטח שווה ערך.

11.2.5. גישה להגדרות ניהול מקומיות בטלפוני הקצה תחייב הזדהות באמצעות קוד טכנאי שאינו קוד ברירת מחדל. כאשר נתמכת הזדהות מספרית בלבד, יוגדר קוד בן 12 ספרות לפחות, ככל שהרכיב תומך בכך, ללא רצפים פשוטים או ספרות חוזרות.

11.2.6. הספק יתעד וינטר פעולות ניהול ושינויי תצורה במערכות הטלפוניה, לרבות פעולות באמצעות קוד טכנאי, זהות מבצע הפעולה, מועד השינוי ופרטי הפעולה, בהתאם ליכולות המערכת ולדרישות הניטור במסמך זה.

11.3. שימוש בתוכנת Softphone

11.3.1. שימוש בתוכנת Softphone במסגרת הפרויקט יחייב אישור מראש של הלמ"ס. התוכנה תותקן ותופעל בתצורה מאושרת ומוקשחת, בהתאם להנחיות היצרן ולדרישות אבטחת תחנות העבודה.

11.3.2. התקשורת של תוכנת ה־Softphone תוגבל לכתובות, פרוטוקולים, פורטים ושירותי טלפוניה מאושרים בלבד.

11.3.3. הספק יגביל את הרשאות התוכנה לגישה למיקרופון ולהתקני השמע לצרכים הנדרשים לביצוע השיחות בלבד, וימנע הקלטה או שימוש בלתי מורשה במיקרופון באמצעות התוכנה, בהתאם ליכולות מערכת ההפעלה והפתרון.

11.3.4. פעולות הקלטת שיחות, ככל שנדרשות במסגרת הפרויקט, יבוצעו באמצעות מערכת ההקלטות המאושרת בלבד ובהתאם לדרישות פרק 12 במסמך זה.

12. אבטחת מערכות הקלטת שיחות

12.1. ניהול ואבטחת מערכות ההקלטה

12.1.1. הספק יקליט את השיחות המבוצעות במסגרת הפרויקט באמצעות מערכת הקלטה מאושרת, המופעלת בחצרות הספק, אלא אם אישרה הלמ"ס אחרת מראש ובכתב. על אף האמור בפרק "הגנה על המידע", **שמירת הקלטות השיחות במערכת ההקלטות של הספק תותר בהתאם לדרישות פרק זה, ולא תהווה היתר לשמירת נתוני סקרים או מידע אחר של הלמ"ס במערכות אחרות של הספק.**

12.1.2. מערכת ההקלטות והמידע הנשמר בה יופרדו פיזית או לוגית מסביבות של לקוחות אחרים, ויוגנו מפני גישה בלתי מורשית, חשיפה, שינוי, העתקה או מחיקה בלתי מורשית.

12.1.3. הקלטות השיחות יישמרו באופן מוצפן ויועברו באמצעות ערוצי תקשורת מוצפנים ומאושרים. מפתחות ההצפנה ינוהלו באופן מאובטח והגישה אליהם תוגבל לגורמים מורשים בלבד.

12.2. ניהול הרשאות וגישה להקלטות

12.2.1. הגישה למערכת ההקלטות ולהקלטות עצמן תוגבל למשתמשים שאושרו בלבד, בהתאם לתפקידם ולצורך העסקי. הקצאת הרשאות תתבצע באישור ממונה אבטחת המידע של הספק או מי שהוסמך לכך מטעמו.

12.2.2. הספק יפריד בין הרשאות חיפוש, האזנה, ייצוא, ניהול ומחיקה של הקלטות, בהתאם לעקרון ההרשאה המזערית. גישה ניהולית וגישה מרחוק למערכת יחייבו הזדהות רב־שלבית (MFA).

12.2.3. פעולות ייצוא, הורדה, העתקה או מחיקה של הקלטות יחייבו אישור מראש של ממונה אבטחת המידע של הספק או גורם מורשה מטעמו, ויתועדו במערכת לצורכי בקרה. פעולות חריגות או בלתי מורשות יפיקו התראה.

12.2.4. לא תתאפשר שמירה מקומית בלתי מורשית של הקלטות בתחנות העבודה, במערכות המוקד או באמצעי אחסון אחרים שאינם מאושרים.

12.2.5. הלמ"ס תהיה רשאית לקבל גישה להקלטות באמצעות ממשק מאובטח, בהתאם להרשאות ולמתכונת הגישה שיאושרו על ידה.

12.3. תיעוד פעולות בהקלטות

12.3.1. הספק יתעד כל גישה או פעולה במערכת ההקלטות, לרבות חיפוש, האזנה, ייצוא, שינוי, מחיקה וניסיונות לביצוען. התיעוד יכלול את זהות המשתמש, מועד הפעולה, כתובת IP, מזהה ההקלטה, סוג הפעולה ותוצאתה, בהתאם ליכולות המערכת.

12.3.2. הספק יפעיל בקרות והתראות לזיהוי גישה בלתי מורשית, ייצוא הקלטות בהיקף חריג, מחיקה בלתי מורשית ושינוי חריג בהרשאות הגישה.

12.3.3. איסוף הלוגים, שמירתם, הגנה עליהם וניהול ההתראות יבוצעו בהתאם לדרישות פרק הניטור במסמך זה.

12.4. שמירת הקלטות וגיבוי

12.4.1. הקלטות השיחות יישמרו לתקופה של שישה חודשים לפחות, או לתקופה אחרת שתיקבע על ידי הלמ"ס בהתאם להוראות הדין ולדרישות הפרויקט.

12.4.2. בתום תקופת השמירה המאושרת יימחקו ההקלטות באופן מאובטח ומבוקר, אלא אם הורתה הלמ"ס אחרת בכתב או שקיימת חובה לשמרן לפי דין.

12.4.3. הספק יבצע גיבוי מוצפן ומאובטח של ההקלטות, יגביל את הגישה לגיבויים, יגן עליהם מפני שינוי ומחיקה בלתי מורשים ויבצע בדיקות שחזור תקופתיות. שמירת הגיבויים ומחיקתם יהיו בהתאם לתקופת השמירה שנקבעה להקלטות.

12.5. הנחיות לנושא הקלטות בסיום התקשרות

12.5.1. בסיום ההתקשרות, העברת הקלטות השיחות והמידע הנלווה אליהן, מחיקת העותקים שנותרו ברשות הספק והצגת אישור מחיקה יבוצעו בהתאם להוראות סיום ההתקשרות במסמך זה.

13. רציפות תפעולית

13.1. ניהול שינויים

13.1.1. הספק ינהל ויתעד שינויים במערכות, בתשתיות וברכיבי התקשורת והאבטחה המשמשים את הפרויקט, בהתאם לנוהל ניהול שינויים מסודר, הכולל בחינת השפעה, הערכת סיכונים, בדיקות ותוכנית חזרה לאחור (Rollback).

13.1.2. כל שינוי במערכות הלמ"ס או שינוי בסביבת הספק העלול להשפיע על אבטחת המידע, זמינות השירות, ארכיטקטורת הפתרון או הממשקים למערכות הלמ"ס, יחייב תיאום ואישור מראש ובכתב של הגורמים המוסמכים בלמ"ס, בהתאם לנהלי ניהול השינויים.

13.1.3. שינויים דחופים הנדרשים לטיפול בתקלה מהותית או באירוע אבטחת מידע יבוצעו בהתאם לנוהל שינויי חירום מאושר, תוך תיעוד הפעולות, דיווח ללמ"ס וביצוע בחינה בדיעבד בהתאם לצורך.

13.2. שרידות והמשכיות השירות

13.2.1. הספק יבטיח שרידות וזמינות של מערכות המחשוב, התקשורת, אבטחת המידע, הטלפוניה, מערכות ההקלטה, תשתיות הניהול ומערכות הניטור המשמשות את הפרויקט, בהתאם לדרישות הזמינות ורמת השירות שנקבעו בהסכם.

13.2.2. הספק ייערך להמשך אספקת השירות במקרה של תקלה משמעותית או השבתה, לרבות באמצעות תוכנית התאוששות וסביבת עבודה חלופית, ככל שנדרשת בהתאם להסכם.

13.2.3. סביבת עבודה חלופית שתשמש למתן השירות ללמ"ס תעמוד בכל דרישות אבטחת המידע של נספח זה, לרבות הפרדת סביבות, הגנה על תחנות עבודה, תקשורת מאובטחת, ניהול הרשאות וניטור.

13.2.4. הפעלת סביבת עבודה חלופית תחייב השלמת בדיקות אבטחת מידע וקבלת אישור מראש ובכתב של ראש תחום אבטחת המידע בלמ"ס או גורם מוסמך מטעמו. לא תתאפשר הפעלתה ללא אישור כאמור.

13.2.5. הספק יגדיר ויתעד יעדי התאוששות וזמינות למערכות המשמשות את הפרויקט, לרבות RTO ו־RPO, בהתאם לדרישות ההמשכיות ולרמות השירות שנקבעו בהסכם.

13.2.6. הספק יבצע בדיקות תקופתיות לתוכנית ההמשכיות וההתאוששות, לרבות תרגול מעבר לסביבה חלופית, ויתקן פערים שיתגלו בבדיקות.

13.3. גיבוי ובדיקת תקינות הגיבויים

13.3.1. הספק יבצע גיבוי של תצורות המערכות, הגדרות רכיבי התקשורת והאבטחה, מערכות התפעול ומידע תפעולי שאושר לשמירה בסביבתו, בהתאם לתוכנית גיבוי מתועדת ולצרכים הנדרשים להמשכיות השירות.

13.3.2. לפני ביצוע שינויים מהותיים במערכות ובתשתיות הפרויקט, הספק יבצע גיבוי מתאים של ההגדרות והמידע התפעולי הרלוונטיים, ויוודא כי קיימת אפשרות לשחזרם במקרה של תקלה.

13.3.3. חל איסור לגבות או לשמור במערכות הספק מידע סקרים, נתונים אישיים על נסקרים, מידע מזהה פרט או מידע המנוהל במערכת אנני"ס, אלא אם ניתן לכך אישור מראש ובכתב של הלמ"ס.

13.3.4. הגיבויים יישמרו בתצורה מאובטחת, תוך יישום בקרות הרשאה, הצפנה והגנה מפני שינוי או מחיקה בלתי מורשים. לא ייעשה שימוש במדיה נתיקה לצורך גיבוי מידע של הלמ"ס, אלא באישור מראש ובכתב.

13.3.5. הספק יבצע בדיקות שחזור תקופתיות ומדגמיות למערכות, לתצורות ולמידע התפעולי המגובים, לצורך אימות תקינות הגיבויים ויכולת ההתאוששות, ויתעד את תוצאות הבדיקות ואת הטיפול בפערים שיימצאו.

13.3.6. גיבוי הקלטות שיחות, ככל שנדרש במסגרת הפרויקט, יתבצע בהתאם להוראות פרק "אבטחת מערכות הקלטות שיחות", לרבות דרישות ההצפנה, ההרשאות, תקופות השמירה ובדיקות השחזור.

14. ממשקים אלחוטיים

14.1. הגבלת שימוש ברשתות ובהתקנים אלחוטיים

14.1.1. בסביבת מוקד הספק (Call Center), לא תתאפשר גישה למידע או למערכות הלמ"ס באמצעות רשתות תקשורת אלחוטיות, לרבות Wi-Fi, אלא באישור מראש ובכתב של אגף הגנת הסייבר בלמ"ס.

14.1.2. תחנות העבודה של סוקרי המוקד יעשו שימוש בהתקני קלט, שמע ותקשורת המחוברים בחיבור פיזי חוטי בלבד, לרבות מקלדות, עכברים, אוזניות וטלפוני IP. שימוש בהתקנים אלחוטיים, לרבות Bluetooth, יחייב אישור מראש ובכתב של אגף הגנת הסייבר בלמ"ס.

14.1.3. הוראות פרק זה חלות על סביבת המוקד והתשתיות המשמשות אותה ואינן גורעות מהאפשרות של סוקרי השטח להשתמש בתקשורת אלחוטית מאובטחת שאושרה על ידי הלמ"ס ובהתאם להוראות פרק 8.

15. גישה מרחוק

15.1. גישה מרחוק לרשת המחשוב של הספק

15.1.1. בגישה מרחוק למידע של הלמ"ס הספק יבטיח כי בכל גישה אחרת מרחוק (Remote Access) למערכות המחשוב שלו (עובדים ו/או ספקים צד שלישי) תעשה בתצורה מאובטחת הכוללת:

15.1.1.1. אימות במזהה חזק (Multi / 2 Factor Authentication).

15.1.1.2. הצפנת תווך.

15.1.1.3. ניהול קבוצות הרשאה.

15.1.1.4. בקרה אחר פעולות המשתמשים.

15.1.1.5. זיהוי חד ערכי של ההתקן (מחשב) המבצע את ההתקשרות (Host Check) באמצעות תעודה, בדיקת עדכניות מערכת ההפעלה ותוכנת הגנה (אנטי וירוס או EDR).

15.2. עדכון מערכות מחשוב

15.2.1. גישה מרחוק של עובדי הספק, מנהלי מערכת, קבלני משנה או גורמי צד שלישי למערכות, לרשתות ולתשתיות הספק המשמשות את הפרויקט, לרבות לצורכי ניהול, תחזוקה, תמיכה או טיפול בתקלות, תתאפשר רק לאחר קבלת אישור מראש ובכתב של אגף מערכות המידע ואגף הגנת הסייבר בלמ"ס.

15.2.2. כל גישה מרחוק שאושרה תתבצע באמצעות פתרון גישה מאובטח הכולל לכל הפחות את הבקרות הבאות:

15.2.2.1. הזדהות אישית וחד־ערכית באמצעות אימות רב־שלבי (MFA).

15.2.2.2. הצפנת תווך התקשורת באמצעות פרוטוקולים מאובטחים שאושרו על ידי הלמ"ס.

15.2.2.3. ניהול קבוצות והרשאות גישה בהתאם לתפקיד, לצורך התפעולי ולעקרון ההרשאה המזערית (Least Privilege).

15.2.2.4. תיעוד וניטור פעולות המשתמשים, לרבות התחברות, ניתוק, ניסיונות גישה כושלים ופעולות ניהול רגישות, בהתאם לדרישות פרק הניטור במסמך זה.

15.2.2.5. זיהוי חד־ערכי של התקן הקצה המבצע את ההתקשרות, באמצעות תעודה דיגיטלית או מנגנון מאובטח שווה ערך, ובדיקת עמידתו בדרישות אבטחת המידע (Host Check), לרבות עדכניות מערכת ההפעלה, תקינות פתרון EDR ומצב ההקשחה.

15.2.3. הגישה תוגבל למערכות, לכתובות, לשירותים ולפרקי הזמן הנדרשים לצורך הפעילות שאושרה. לא תתאפשר גישה גורפת לרשתות הספק או למערכות אחרות שאינן נדרשות למתן השירות.

15.2.4. הספק יבטל את הרשאות הגישה מרחוק עם סיום הצורך התפעולי, שינוי תפקיד, סיום העסקה או סיום פעילות של קבלן משנה, בהתאם לדרישות ניהול המשתמשים והרשאות הגישה במסמך זה.

16. ניהול משתמשים במערכות הספק

16.1. ניהול משתמשים

16.1.1. הספק ינהל את המשתמשים וההרשאות במערכות המשמשות את הפרויקט באמצעות מערכת מרכזית לניהול זהויות והרשאות, כגון Active Directory או פתרון IAM שווה ערך, המאפשר אכיפת מדיניות גישה, ניהול חשבונות ותיעוד פעולות.

16.1.2. לכל משתמש יוקצה חשבון אישי וחד־ערכי המאפשר את זיהויו ואת שיוך הפעולות שביצע. חל איסור על שימוש בחשבונות משותפים או כלליים, אלא אם אושר חריג מראש ובכתב על ידי הלמ"ס.

16.1.3. הרשאות הגישה יוקצו בהתאם לתפקיד המשתמש, לצורך העסקי ולעקרון ההרשאה המזערית (Least Privilege). לא יינתנו הרשאות החורגות מהנדרש לביצוע התפקיד.

16.1.4. הספק יקיים תהליך מתועד לניהול מחזור חיי המשתמש, לרבות פתיחת חשבון, הקצאת הרשאות, שינוי תפקיד, סקירת הרשאות תקופתית, השעיה וביטול חשבונות והרשאות עם סיום הצורך או ההעסקה.

16.1.5. חשבונות בעלי הרשאות ניהול יהיו נפרדים מחשבונות המשתמש הרגילים, וישמשו לפעולות ניהול בלבד. הגישה באמצעותם תוגבל למשתמשים מורשים ותחייב הזדהות רב־שלבית (MFA).

16.1.6. חשבונות שירות (Service Accounts), חשבונות אפליקטיביים וחשבונות ממוכנים ינוהלו באופן מבוקר, תוך הגדרת בעל חשבון אחראי, ייעוד, הרשאות מזעריות ומנגנוני הגנה על פרטי ההזדהות. ככל שהדבר נתמך, תיחסם האפשרות להתחברות אינטראקטיבית באמצעות חשבונות אלה.

16.2. ניהול סיסמאות ואמצעי זיהוי

16.2.1. הספק יישם מדיניות סיסמאות ואמצעי הזדהות בכלל מערכות הפרויקט, לרבות חשבונות משתמשים, מנהלי מערכת, חשבונות שירות וחשבונות ממוכנים, בהתאם להנחיות הלמ"ס ולדרישות נספח זה.

16.2.2. סיסמאות ופרטי הזדהות יישמרו ויועברו באמצעים מאובטחים בלבד. סיסמאות משתמשים יאוחסנו באמצעות מנגנוני גיבוב ייעודיים ומאובטחים לסיסמאות, ופרטי הזדהות אחרים, מפתחות ו־Secrets ינוהלו באמצעי אחסון מאובטחים ומתאימים. חל איסור לשמור או להעביר סיסמאות באופן גלוי.

16.2.3. מדיניות הסיסמאות תכלול לכל הפחות את הדרישות הבאות:

16.2.3.1. אורך סיסמה של 8 תווים לפחות למשתמש רגיל ו־16 תווים לפחות לחשבון ניהולי או חשבון שירות, בהתאם לדרישות המקוריות של הלמ"ס.

16.2.3.2. חסימת סיסמאות נפוצות, צפויות, קלות לניחוש או כאלה שידוע כי נחשפו.

16.2.3.3. מנגנון להגבלת ניסיונות הזדהות כושלים ולהגנה מפני מתקפות ניחוש סיסמאות.

16.2.3.4. מניעת שימוש חוזר בסיסמאות בהתאם למדיניות הלמ"ס.

16.2.3.5. החלפת סיסמה בעת חשד או אינדיקציה לחשיפתה.

16.2.4. לא ייעשה שימוש בסיסמאות משותפות, בסיסמאות ברירת מחדל או בשמירה בלתי מאובטחת של פרטי הזדהות. הספק יוודא כי עובדיו אינם מוסרים סיסמאות לאחרים ואינם שומרים אותן במקום גלוי.

16.2.5. הזדהות רב־שלבית (MFA) תהיה חובה בגישה מרחוק, בגישה לחשבונות ניהול ובגישה למערכות או למידע רגיש בהתאם להנחיות הלמ"ס. חריגה מדרישה זו תחייב אישור מראש ובכתב.

16.2.6. סיסמאות של חשבונות שירות וחשבונות ממוכנים ינוהלו באמצעות מנגנון מאובטח, כגון מערכת לניהול Secrets או כספת סיסמאות, תוך הגבלת הרשאות הגישה, ביצוע החלפה מבוקרת ותיעוד השימוש בהן.

16.3. בקרה וניטור הרשאות

16.3.1. הספק יבצע סקירות הרשאות תקופתיות לזיהוי חשבונות שאינם נדרשים, הרשאות עודפות, חשבונות לא פעילים וחשבונות של עובדים או קבלני משנה שסיימו את פעילותם.

16.3.2. פעולות ניהול משתמשים והרשאות, לרבות הקמת חשבונות, שינוי הרשאות, ביטול חשבונות וניסיונות הזדהות, יתועדו וינוטרו בהתאם לדרישות פרק הניטור במסמך זה.

16.3.3. ניהול המשתמשים וההרשאות במערכות הלמ"ס עצמן יתבצע בהתאם למדיניות הלמ"ס ובאחריות הגורמים המוסמכים מטעמה. הוראות פרק זה יחולו על המערכות והחשבונות שבאחריות הספק.

17. הגנה על מידע פיזי

17.1. שירותי הדפסה

17.1.1. בסביבות המחשוב של הספק שבהן נשמר, מעובד או נגיש מידע של הלמ"ס, לא תתאפשר הדפסת מידע, לרבות הדפסה מקומית, הדפסה ברשת, הדפסה לקובץ או למדפסת וירטואלית, אלא באישור מראש ובכתב של אגף הגנת הסייבר בלמ"ס.

17.1.2. הספק יישם בקרות טכנולוגיות לחסימת שירותי הדפסה ויכולות הפקת פלט שאינן מאושרות, בהתאם לדרישות הקשחת תחנות העבודה ומניעת דלף המידע בפרק 10.

17.1.3. ככל שאושר שימוש בהדפסה, הספק יגדיר ויתעד את מטרת ההדפסה, סוג המידע, המשתמשים המורשים, המדפסות המאושרות ואמצעי ההגנה על הפלט. מסמכים מודפסים יישמרו במקום מאובטח ויושמדו באופן מבוקר כאשר אינם נדרשים עוד

17.2. שימוש במדיה נתיקה

17.2.1. חל איסור לעשות שימוש במדיה נתיקה לצורך שמירה, העברה, עיבוד או גישה למידע של הלמ"ס, לרבות כונני USB, דיסקים חיצוניים, כרטיסי זיכרון, CD/DVD ואמצעי אחסון ניידים אחרים, אלא באישור מראש ובכתב של אגף הגנת הסייבר בלמ"ס.

17.2.2. מדיה נתיקה שאושרה לשימוש תהיה ייעודית, מזוהה ומנוהלת, והמידע הנשמר בה יוצפן באמצעות BitLocker או פתרון הצפנה מאושר שווה ערך. אמצעי פתיחת ההצפנה יישמרו באופן מאובטח ובנפרד מהמדיה.

17.2.3. הספק יגן על המדיה הנתיקה מפני אובדן, גניבה וגישה בלתי מורשית, לרבות אחסונה במקום נעול ומבוקר, והחזרתה או מחיקתה באופן מאובטח בתום השימוש, בהתאם להנחיות הלמ"ס.

17.2.4. הספק ינהל תיעוד של שימוש במדיה נתיקה מאושרת, הכולל לכל הפחות את זהות המשתמש, מטרת השימוש, סוג ומזהה ההתקן, סוג המידע, מועד מסירת המדיה, מועד החזרתה או מחיקתה ואמצעי ההגנה שיושמו.

17.2.5. מדיה נתיקה שאושרה לצורך הפרויקט לא תחובר למחשבים, לרשתות או למערכות שאינן מאושרות במסגרת הפרויקט, אלא באישור מראש ובכתב של הלמ"ס.

18. ניטור

18.1. הנחיות כלליות לנושא ניטור

18.1.1. הספק ינטר אירועים תפעוליים ואירועי אבטחת מידע בכלל המערכות, התשתיות, האפליקציות ורכיבי האבטחה המשמשים למתן השירותים ללמ"ס או מחזיקים, מעבדים או מאפשרים גישה למידע של הלמ"ס.

18.1.2. הספק יפעיל מנגנוני איסוף, ניטור וניתוח לוגים לצורך זיהוי פעילות חריגה, ניסיונות גישה בלתי מורשים, פעולות רגישות, שינויים חריגים ואינדיקציות לאירועי אבטחת מידע.

18.1.3. הספק יפעיל מערכת SIEM (מערכת ניטור מרכזית) ויעביר אליה את הלוגים הרלוונטיים לפרויקט, תוך הפרדת הרשאות הגישה למידע של הלמ"ס ממידע של לקוחות אחרים.

18.1.4. הספק יקיים יכולת ניטור ותגובה (SOC) לאורך כל תקופת ההתקשרות ובהתאם לרמת השירות שנקבעה בהסכם. ככל שנדרש ניטור רציף, תופעל יכולת ניטור ותגובה 24 שעות ביממה, שבעה ימים בשבוע.

18.2. איסוף ושמירת לוגים

18.2.1. בכלל המערכות המשמשות את הפרויקט יישמרו לוגים מקומיים למשך חודש לפחות, ככל שהמערכת תומכת בכך. הלוגים הרלוונטיים יועברו למערכת SIEM מרכזית ויישמרו בה למשך 24 חודשים לפחות.

18.2.2. ככל שמערכת או רכיב אינם מאפשרים העברת לוגים למערכת המרכזית, הספק יציג לאישור אגף הגנת הסייבר בלמ"ס פתרון חלופי לאיסוף הלוגים ולשמירתם למשך 24 חודשים לפחות, תוך הבטחת שלמותם, זמינותם והגנה מפני שינוי או מחיקה בלתי מורשים.

18.2.3. לוגים אפליקטיביים יישמרו במנגנון ייעודי ונפרד מנתוני הייצור, כגון שרת לוגים או בסיס נתונים ייעודי, אלא אם אושר אחרת על ידי הלמ"ס.

18.2.4. הלוגים יוגנו מפני שינוי, מחיקה, גישה בלתי מורשית או פגיעה בשלמותם, לרבות על ידי משתמשים בעלי הרשאות ניהול.

18.2.5. כלל המערכות יסונכרנו לשעון אחיד באמצעות NTP. בחצר הספק יבוצע הסנכרון מול שרתי זמן פנימיים של הספק ולא ישירות מול שירותי NTP חיצוניים.

18.3. תוכן הלוגים ואירועים לתיעוד

18.3.1. כל לוג יכלול, בהתאם לסוג הפעולה ויכולות המערכת, את הפרטים הבאים:

18.3.1.1. זהות המשתמש או חשבון השירות שביצע את הפעולה.

18.3.1.2. תאריך ושעה, לרבות דקות ושניות.

18.3.1.3. כתובת IP ומזהה מערכת או רכיב.

18.3.1.4. מזהה יישום, משאב או אובייקט רלוונטי.

18.3.1.5. סוג הפעולה, יעד הפעולה ותוצאתה (הצלחה או כישלון).

18.3.1.6. פרטי השינוי שבוצע, לרבות ערך קודם וערך חדש, ככל שניתן וללא חשיפת מידע רגיש בלוגים.

18.3.2. הספק יתעד לכל הפחות את האירועים הבאים:

18.3.2.1. כניסה, יציאה, ניסיונות הזדהות כושלים ואימות באמצעות OTP.

18.3.2.2. גישה למידע רגיש, שליפת מידע, שינוי, העתקה ומחיקה.

18.3.2.3. פעולות ניהול, שינויי תצורה והרשאות במערכות ובתשתיות.

18.3.2.4. גישה למסדי נתונים, לקבצים רגישים וללוגים.

18.3.2.5. פעילות חשבונות שירות (Service Accounts) וחשבונות בעלי הרשאות גבוהות.

18.3.2.6. אירועי אבטחה, תקלות וזמינות במערכות ההגנה.

18.3.2.7. תעבורה חריגה, ניסיונות גישה חסומים ועומסים חריגים

18.4. ניטור משתמשים וחשבונות שירות

18.4.1. הספק ינטר פעילות משתמשים במערכות הפרויקט, לרבות משתמשים מזוהים, אנונימיים, מנהלנים, משתמשים אפליקטיביים וחשבונות גישה למסדי נתונים.

18.4.2. הספק ינטר פעילות חשבונות שירות (Service Accounts), לרבות הפעלת שירותים, גישה למשאבים, שינוי הרשאות וניסיונות לביצוע פעולות החורגות מהייעוד שהוגדר לחשבון.

18.4.3. פעולות חריגות של חשבונות בעלי הרשאות גבוהות או חשבונות שירות יפיקו התראה לצורך בדיקה ותחקור.

18.5. ניטור מערכות תקשורת ואבטחת מידע

18.5.1. הספק יאסוף וינטר לוגים מרכיבי Firewall, IPS/IDS, EDR, מערכות ניהול, שרתים, תשתיות תקשורת ומערכות הגנה נוספות המשמשות את הפרויקט.

18.5.2. הלוגים יכללו, בהתאם לרכיב, כתובות IP מקור ויעד, פורטים, פרוטוקולים, מזהי רכיבים, זהות משתמש, סוג הפעולה, כמות פניות ותוצאתן.

18.5.3. הספק ינטר שינויים בהגדרות רכיבי תקשורת ואבטחה, תקלות במערכות ובסוכני הגנה, ניסיונות עקיפת בקרות ותעבורה חריגה או בלתי מורשית.

18.5.4. בממשקים אפליקטיביים וחיצוניים ינוטרו פניות חריגות, כמות בקשות, ניסיונות גישה בלתי מורשים, תקלות זמינות ועומסים חריגים, תוך תיעוד זהות הפונה וסוג הבקשה ככל שניתן.

18.5.5. הספק יגדיר ויפעיל חוקי ניטור והתראות לזיהוי אירועים חריגים, לרבות:

18.5.5.1. שליפה או ייצוא מידע בכמות חריגה.

18.5.5.2. מחיקה המונית או בלתי מורשית של מידע.

18.5.5.3. גישה חריגה למאגרי מידע ולהקלטות שיחות.

18.5.5.4. ניסיונות הזדהות כושלים חוזרים.

18.5.5.5. שימוש חריג בהרשאות ניהול ובחשבונות שירות.

18.5.5.6. שינוי או מחיקה של לוגים והשבתת מנגנוני ניטור.

18.5.5.7. ושינויי תצורה רגישים וכשל במערכות הגנה

18.5.6. אירועים חריגים בהתאם לחוקי הניטור שהוגדרו יפיקו התראה לגורמי אבטחת המידע והתפעול המורשים של הספק, באמצעות מערכת הניטור, דוא"ל, SMS או ערוץ התראה מאובטח אחר.

18.5.7. הספק יבחן באופן תקופתי מגמות אבטחת מידע שליליות, ניסיונות תקיפה חוזרים, שינויים בדפוסי פעילות ואפקטיביות חוקי הניטור, ויעדכן את הבקרות בהתאם.

18.5.8. הספק יבטיח כי אירועים והתראות אבטחת מידע שזוהו במסגרת הניטור ייבדקו ויתוחקרו בהתאם לחומרתם ולרמת הסיכון הנשקפת מהם. אירועים או חשדות לאירועים העלולים להשפיע על מידע הלמ"ס, מערכותיה או השירות הניתן לה, יטופלו וידווחו בהתאם להוראות סעיף "אירועי בטחון וסייבר".

18.6. הרשאות גישה וניהול לוגים

18.6.1. הגישה ללוגים תוגבל לגורמי ניהול, ניטור ואבטחת מידע מורשים בלבד, בהתאם לתפקידם ולעקרון ההרשאה המזערית.

18.6.2. צפייה, חיפוש ושליפת לוגים יתבצעו באמצעות ממשק ניהול מאובטח וייעודי, מרשת הניהול של הספק או מסביבה אחרת שאושרה על ידי הלמ"ס.

18.6.3. לא תתאפשר גישה ישירה לבסיסי הנתונים לצורך צפייה שוטפת בלוגים, אלא באמצעות ממשקים ייעודיים ומבוקרים.

18.6.4. פעולות גישה, חיפוש, ייצוא, שינוי הגדרות וניהול מערכת הלוגים יתועדו ויהיו נתונות לבקרה.

18.7. ניטור פעילות משתמשים

18.7.1. הספק יפעיל מנגנוני תיעוד וניטור פעילות משתמשים (Audit Log) בתחנות סוקרי המוקד ובסביבות VDI, ככל שניתן בהתאם ליכולות המערכות, לרבות התחברות וניתוק, הפעלת יישומים, ניסיונות גישה בלתי מורשים, פעולות רגישות וניסיונות לעקיפת בקרות אבטחת מידע. התיעוד יאפשר שיוך פעולות למשתמש מזוהה וישמש לצורכי בקרה ותחקור.

18.7.2. התיעוד יישמר באופן מאובטח, והגישה אליו תוגבל לגורמים מורשים בלבד ותתועד.

18.7.3. הספק יידע את עובדיו על ניטור פעילותם, בהתאם להוראות הדין ולמדיניות הפרויקט.

18.8. בקרה וביקורת מטעם הלמ"ס

18.8.1. הספק יאפשר ללמ"ס לקבל לוגים, דוחות ניטור, התראות ותיעוד טיפול באירועים, לצורכי ביקורת, בקרה ותחקור אירועי אבטחת מידע, בהתאם לדרישתה.

18.8.2. הספק יאפשר ללמ"ס לבחון את מערך הניטור, חוקי ההתראה ויישום בקרות האבטחה בסביבת הפרויקט, בהתאם להוראות ההתקשרות.

18.9. מודיעין סייבר - אופציונלי

18.9.1. הספק יפעיל ו/או יעזר בשירותי מודיעין סייבר לקבלת התראות על איומי סייבר.

18.9.2. ספק המודיעין ידווח לממונה אבטחת המידע של הספק על כל התראה אשר עלולה להשפיע על הספק או על השירות הניתן ללמ"ס במסגרת הסכם זה.

18.9.3. ככל שיתקבל מידע מודיעיני או תזוהה התרעה המעידים על איום העלול להשפיע על מידע הלמ"ס, מערכותיה או השירות הניתן לה, הספק יבחן את השלכות האיום ויפעל לדיווח ולנקיטת אמצעי הגנה בהתאם להוראות סעיף "אירועי בטחון וסייבר".

19. פניות ציבור

19.1. מענה לפניות ציבור

19.1.1. הלמ"ס מפעילה מוקד פניות הציבור, אשר יספק מענה לתלונות ובעיות שיוצגו במהלך ביצוע הסקר. על הספק להפנות פניות שמגיעות אליו, למוקד פניות הציבור של הלמ"ס.

19.1.2. חל איסור מוחלט לספק או לעובדיו, לתת מענה בשם הלמ"ס וללא אישורה.

20. מודעות אבטחת מידע לעובדי הספק

20.1. חובת הספק

20.1.1. הנחיות פרק זה מהוות חלק בלתי נפרד מנהלי העבודה והתחייבויות הסודיות של עובדי הספק וקבלני המשנה המועסקים בפרויקט.

20.1.2. הספק אחראי להביא את ההנחיות לידיעת כל עובד, להדריכו בנושאים הרלוונטיים לתפקידו, לוודא כי הבין אותן ולהחתימו על התחייבות לעמידה בהן לפני תחילת עבודתו בפרויקט.

20.1.3. ההנחיות וההדרכות יימסרו בשפה המובנת לעובד, לרבות באמצעות תרגום לשפת אמו ככל שנדרש להבנתן. הספק יבצע רענון תקופתי של ההנחיות וכן רענון בעקבות שינוי מהותי בדרישות או באיומים הרלוונטיים.

20.2. הוראות כלליות

20.2.1. הוראות פרק זה יחולו על כלל עובדי הספק וקבלני המשנה המועסקים במסגרת הפרויקט, לרבות סוקרי המוקד (Call Center), סוקרי שטח, מנהלים ועובדי תמיכה בעלי גישה למידע, למערכות או לתשתיות המשמשות את הלמ"ס.

20.2.2. כל עובד יחויב לקבל הדרכת אבטחת מידע וסודיות המתאימה לתפקידו ולחתום על התחייבות לעמידה בהנחיות, טרם תחילת פעילותו בפרויקט. הספק ישמור תיעוד של ביצוע ההדרכה ושל חתימת העובד.

20.2.3. הפעילות במסגרת הפרויקט תתבצע בשעות ובמסגרות הפעילות שנקבעו במכרז ובהנחיות הלמ"ס. פעילות החורגת משעות אלו, לרבות פעילות בחצרות הלמ"ס ושלוחותיה, תחייב אישור מראש ובכתב של הלמ"ס.

20.2.4. עובד הספק לא יבצע שינויים בתצורת מערכות, בתשתיות, בהרשאות או באמצעי אבטחת מידע שלא במסגרת סמכותו. שינויים תפעוליים העלולים להשפיע על השירות או על אבטחת המידע יבוצעו בהתאם לדרישות ניהול השינויים בפרק רציפות תפעולית.

20.3. שימוש באמצעי מחשוב וחשבונות משתמש

20.3.1. השימוש באמצעי המחשוב, במערכות ובחשבונות המשתמש שהועמדו לרשות העובד ייעשה לצורכי הפרויקט בלבד ובהתאם להרשאות שניתנו לו.

20.3.2. חשבונות המשתמש, הסיסמאות ואמצעי ההזדהות הם אישיים. חל איסור למסור אותם לאחרים, לשתף סיסמאות, לאפשר לאחר להשתמש בחשבון או לשמור פרטי הזדהות במקום גלוי או בלתי מאובטח.

20.3.3. חל איסור לחבר למערכות הפרויקט מחשבים, התקני אחסון, כונני USB, טלפונים ניידים, מדפסות, התקנים אלחוטיים או ציוד אחר שלא אושר מראש.

20.3.4. חל איסור להתקין תוכנות, תוספים או שירותים שלא אושרו, לשנות הגדרות אבטחה, להשבית אמצעי הגנה או לנסות לעקוף את מגבלות השימוש שהוגדרו במערכות.

20.3.5. העובד ישמור על אמצעי המחשוב שנמסרו לו, ימנע גישה אליהם מצד גורמים בלתי מורשים וינעל את תחנת העבודה בכל הפסקת פעילות או עזיבת העמדה.

20.3.6. עם סיום פעילותו בפרויקט, שינוי תפקידו או לפי דרישת הגורם המוסמך, יחזיר העובד את כלל אמצעי המחשוב, המסמכים, הציוד ואמצעי הגישה שנמסרו לו, ללא שמירת עותקים של מידע הלמ"ס. החזרת הציוד וביטול הגישה יתועדו על ידי הספק.

20.4. שמירת מידע, סודיות ומניעת דלף מידע

20.4.1. מידע של הלמ"ס יישמר ויעובד במערכות ובאמצעי מחשוב שאושרו בלבד. חל איסור לשמור מידע במחשבים פרטיים, באמצעי אחסון חיצוניים או בשירותים שאינם מאושרים.

20.4.2. חל איסור להעתיק, לצלם, להדפיס, להקליט, להעביר, לפרסם או להוציא מידע של הלמ"ס, לרבות מידע דיגיטלי, מסמכים מודפסים ומידע הנמסר בעל פה, אלא במסגרת פעילות שאושרה ובהתאם להרשאות שניתנו לעובד.

20.4.3. חל איסור להעביר מידע של הלמ"ס באמצעות דוא"ל פרטי או ארגוני, שירותי ענן, רשתות חברתיות, יישומי מסרים או שירותי שיתוף קבצים, אלא באמצעות ערוץ העברה ייעודי ומאובטח שאושר במפורש על ידי הלמ"ס.

20.4.4. שימוש בשירותי דוא"ל וענן ארגוניים של הספק, לרבות Microsoft 365 ו־Google Workspace, יתאפשר רק לצרכים שהותרו בהתאם להוראות פרק 7, ולא יהווה היתר לשמירת מידע הסקרים או מידע אחר של הלמ"ס בשירותים אלה.

20.4.5. מסמכים ומידע פיזי יישמרו במקום מאובטח ולא יושארו ללא השגחה. בתום השימוש יוחזרו או יושמדו באופן מאובטח בהתאם להנחיות הלמ"ס.

20.4.6. חל איסור למסור מידע על פעילות הלמ"ס, מערכותיה, תשתיותיה, זהויות משתמשים, חשבונות ניהול, אמצעי אבטחה או מידע שהתקבל במסגרת הסקרים לגורמים שלא אושרו לכך, לרבות עובדים אחרים שאינם זקוקים למידע, חברים ובני משפחה.

20.4.7. עובד שקיבל או נחשף למידע שאינו נדרש לתפקידו יימנע משימוש בו או מהעברתו וידווח על כך מיידית לממונה עליו.

20.4.8. חל איסור להזין, להעלות, להעתיק או להעביר מידע של הלמ"ס לשירותי בינה מלאכותית, לרבות כלי AI ציבוריים או ארגוניים, אלא בהתאם לאישורים המפורשים ולהגבלות שנקבעו בפרק 6.

20.5. אבטחה פיזית וסביבת העבודה

20.5.1. הכניסה לאזורי העבודה של הפרויקט תותר לעובדים ולגורמים שאושרו בלבד. חל איסור להכניס אורחים או גורמים בלתי מורשים לאזורים אלה ללא אישור הגורם המוסמך.

20.5.2. חל איסור לצלם או להקליט בסביבות עבודה שבהן מצוי מידע של הלמ"ס, לרבות בחצרות הלמ"ס, אלא באישור מראש של הגורם המוסמך.

20.5.3. חל איסור לחבר ציוד חשמלי או ציוד מחשוב שאינו מאושר לתשתיות הפרויקט, למעט ציוד שהותר בהתאם לנהלי הבטיחות והתפעול.

20.5.4. העובד יוודא כי מסמכים, מסכים ושיחות הנוגעים למידע של הלמ"ס אינם חשופים לצפייה או להאזנה של גורמים שאינם מורשים.

20.6. ניטור, בקרה ודיווח אירועים חריגים

20.6.1. העובד מאשר כי הובא לידיעתו שבסביבת הפרויקט מופעלים אמצעי ניטור ותיעוד פעילות לצורכי אבטחת מידע, בקרה ותחקור, בהתאם להוראות הדין ולמדיניות הפרויקט. ככל שמופעלים אמצעי הקלטה נוספים, יימסר לעובד מידע מתאים על הפעלתם בהתאם לדין.

20.6.2. חל איסור לשבש, להשבית או לעקוף אמצעי ניטור, תיעוד ואבטחת מידע המופעלים בסביבת העבודה.

20.6.3. בכל אירוע אבטחת מידע או חשד לאירוע, לרבות אובדן או גניבת ציוד או מידע, חשיפת סיסמאות, גישה בלתי מורשית, קבלת מידע שלא במסגרת התפקיד או פעילות חריגה במחשב, העובד ידווח מיידית לממונה עליו ולמוקד הסייבר של הלמ"ס בטלפון 02-6593124, להוראות סעיף "אירועי בטחון וסייבר".

20.6.4. העובד ישתף פעולה עם בירור האירוע, יימנע ממחיקת מידע, לוגים או ראיות ויפעל בהתאם להנחיות הגורמים המוסמכים.

20.7. הנחיות לעובדי המוקד Call Center

20.7.1. העבודה תתבצע באמצעות תחנות העבודה והמערכות שהוקצו לפרויקט בלבד. חל איסור להשתמש במחשבים פרטיים או להתחבר לרשתות אחרות במהלך ביצוע הסקרים.

20.7.2. חל איסור לבצע שימוש אישי בתחנות הסוקרים, לרבות גלישה לאתרים שאינם קשורים לפרויקט, שימוש בדוא"ל חיצוני או הפעלת תוכנות שאינן מאושרות.

20.7.3. חל איסור לשמור מידע סקרים בתחנות העבודה, להעתיקו, להדפיסו, לצלמו או להעבירו מחוץ למערכת המאושרת.

20.7.4. חל איסור לבצע הקלטה עצמאית של שיחות, להאזין לשיחות שאינן במסגרת התפקיד או לגשת להקלטות ללא הרשאה. הקלטת שיחות במסגרת הפרויקט תתבצע באמצעות המערכת המאושרת בלבד.

20.7.5. העובד יוודא כי סביבת העבודה אינה מאפשרת צפייה או האזנה למידע מצד עובדים אחרים, מבקרים או גורמים שאינם מורשים.

20.8. הנחיות לסוקרי השטח

20.8.1. סוקר השטח יעשה שימוש במחשבים ובאמצעי מחשוב שסופקו או אושרו על ידי הלמ"ס בלבד לצורך ביצוע הסקרים, בהתאם להוראות פרק 8. חל איסור להשתמש במחשב פרטי, ציבורי או במחשב שלא אושר.

20.8.2. הסוקר ישמור את המחשב והציוד שנמסרו לו במקום מאובטח וימנע גישה אליהם מצד גורמים בלתי מורשים. חל איסור להשאיר ציוד ללא השגחה ברכב, במקום ציבורי או בבית אזרח.

20.8.3. הגישה למערכות הלמ"ס תתבצע באמצעות אמצעי ההזדהות והתקשורת המאובטחים שהוגדרו לפרויקט בלבד. חל איסור למסור סיסמאות או אמצעי הזדהות לאחרים או לשמור אותם באופן גלוי או בלתי מאובטח.

20.8.4. חיבור לרשתות אלחוטיות יתבצע בהתאם למדיניות הלמ"ס ובאמצעות רשתות שאושרו לשימוש. בחיבור לרשת Wi-Fi ייעשה שימוש בהצפנת WPA2-AES לפחות, תוך העדפת WPA3, ככל שהחיבור הותר. חל איסור להתחבר לרשתות פתוחות או בלתי מאובטחות.

20.8.5. השימוש במחשב יוגבל למערכות, לאתרים וליישומים שאושרו לצורך ביצוע הסקרים. חל איסור לגלוש לאתרים שאינם נדרשים, להוריד קבצים או להתקין תוכנות ותוספים בלתי מורשים.

20.8.6. חל איסור להשתמש בשירותי שיתוף קבצים, אחסון בענן, סנכרון אוטומטי או תוכנות להעברת קבצים, לרבות Google Drive, OneDrive ו־BitTorrent, לצורך שמירה או העברה של מידע הלמ"ס, אלא באישור מפורש.

20.8.7. מידע הסקרים יישמר ויעובד במערכות שאושרו בלבד. חל איסור לשמור מידע רגיש באופן מקומי, להעתיקו, לצלמו, להדפיסו או להעבירו לגורמים בלתי מורשים.

20.8.8. בעת ביצוע סקרים בבית אזרח או במרחב ציבורי, הסוקר ינקוט אמצעים למניעת צפייה במסך, האזנה לשיחות או חשיפת מידע לגורמים שאינם מורשים, ולא יותיר מחשב או מסמכים ללא השגחה.

20.8.9. הסוקר ינעל את המחשב בכל הפסקת עבודה או עזיבת העמדה ויוודא כי לא מתאפשרת גישה למידע או למערכות מצד גורמים אחרים.

20.8.10. במקרה של אובדן או גניבת ציוד, חשד לגישה בלתי מורשית, חשיפת מידע או פעילות חריגה במחשב, ידווח הסוקר מיידית לממונה עליו ולמוקד הסייבר של הלמ"ס בטלפון 02-6593124.

20.9. הצהרת העובד והתחייבות לסודיות

20.9.1. אני החתום מטה מאשר כי קראתי והבנתי את הנחיות אבטחת המידע החלות עליי במסגרת פעילותי עבור הלמ"ס, כי ההנחיות נמסרו לי בשפה המובנת לי וכי קיבלתי הדרכה מתאימה לתפקידי.

20.9.2. אני מתחייב לפעול בהתאם להנחיות, לשמור בסודיות כל מידע שאליו איחשף במסגרת עבודתי, לא לעשות בו שימוש שלא לצורכי התפקיד, לא להעבירו לגורמים בלתי מורשים ולדווח מיידית על אירועי אבטחת מידע או חשד לאירועים בהתאם להנחיות.

20.9.3. ידוע לי כי חובות הסודיות החלות עליי ימשיכו לחול גם לאחר סיום פעילותי בפרויקט, בהתאם להתחייבויותיי ולהוראות הדין.

שם העובד/הסוקר	שם החברה	ת.ז	טלפון נייד – עובד

כתובת העובד	תפקיד	שם המנהל הישיר	טלפון נייד – מנהל ישיר

21. הנחיות פיתוח מאובטח לספק

21.1. הנחיות פיתוח מאובטח ואחריות הספק לקבלתן

21.1.1. הנחיות הפיתוח המאובטח של הלמ"ס יחולו על כל מערכת, יישום או רכיב תוכנה המפותחים, מותאמים או מורחבים במסגרת הפרויקט, לרבות שימוש בקוד פתוח (Open Source), רכיבי צד שלישי ופתרונות המבוססים על בינה מלאכותית (AI).

21.1.2. ההנחיות אינן חלות על מוצר מדף מוגמר שלא מבוצעים בו פיתוחים או שינויי קוד, מבלי לגרוע מיתר דרישות אבטחת המידע החלות על המוצר ועל שילובו בפרויקט.

21.1.3. ככל שהספק צופה, במסגרת הצעתו או במהלך ביצוע הפרויקט, צורך בפיתוח תוכנה, בהתאמת קוד קיים או בביצוע שינויים במוצר שאינו מוצר מדף מוגמר, **תחול עליו החובה לקבל מהלמ"ס, בנוסף להנחיות אלה, את נספח הנחיות הפיתוח המאובטח (שאינו מצורף למכרז) ולעמוד בכל הוראותיו.**

21.1.4. ספק הצופה כי הצעתו תכלול תהליכי פיתוח כאמור מחויב לפנות **<u>מיוזמתו</u>** ללמ"ס, במסגרת שלב שאלות ההבהרה ובטרם הגשת הצעתו למכרז, ולבקש את נספח הנחיות הפיתוח המאובטח. **<u>נדגיש:</u>** האחריות לבקשת הנספח, לקבלתו, לבחינת הוראותיו ולהבאתן בחשבון במסגרת ההצעה, לרבות עלויות, משאבים ולוחות זמנים, מוטלת על הספק בלבד. הנחיות יועברו על ידי אגף הגנת הסייבר.

21.1.5. ספק שקיבל לידיו את נספח הנחיות הפיתוח המאובטח וזכה, מתחייב לעמוד בכל הנחיות הפיתוח במלואן, לרבות דרישות הנוגעות לתכנון, פיתוח, בדיקות, הטמעה, סקר קוד, מבדקי חדירות, תחזוקה וטיפול בחולשות אבטחת מידע, אלא אם אושרה לו חריגה מראש ובכתב בהתאם למנגנון החריגים שנקבע במסמכי המכרז.

21.1.6. ספק שלא פנה לקבלת הנספח בשלב המענה למכרז, ובהמשך ההתקשרות יידרש לבצע פיתוח או יבקש לקבל את הנספח, ייחשב כמי שהסכים מראש לתחולת הנספח ולהוראותיו במלואן, והוא יהיה מחויב לעמוד בהן כתנאי לביצוע הפיתוח, גם אם לא קיבל את הנספח בעת הגשת הצעתו.

21.1.7. **<u>נדגיש:</u>** אי־בקשת הנספח או אי־בחינת דרישותיו במועד לא יהוו עילה לפטור מעמידה בהנחיות, לדחיית מועדים, לתוספת תמורה או להעלאת טענה בדבר אי־ידיעת הדרישות. הספק יישא באחריות להיערכות הנדרשת לעמידה בהוראות הנספח, בכפוף להוראות ההסכם.

21.1.8. הספק לא יחל בביצוע פיתוח, התאמת קוד או שילוב רכיב המחייב עמידה בהנחיות הפיתוח המאובטח, בטרם קיבל את הנספח, בחן את הוראותיו והסדיר את עמידתו בדרישות מול הגורמים המוסמכים בלמ"ס.