נספח ו' - הנחיות אבטחת מידע

מכרז 11/2022 –

מתן שירותי תמיכה במערך התקשוב עבור מפקד האוכלוסין

1

1. הקדמה

1.1. רקע

1.1.1. מסמך הנחיות זה נועד להיות מצורף למכרז תפוקות ל שירותים לליווי ההקמה והתפעול של מערך המחשוב

1.1.2. השירותים שיינתנו על ידי הספק (להלן: "השירותים")הזוכה יכללו, בין השאר:

1.1.2.1. התקנת כ-1,600 מחשבים ניידים.

1.1.2.2. תמיכה טכנית בהפעלת מערך המחשוב להדרכות של כ-2,000 סוקרים.

1.1.2.3. תמיכה (בסיום הדרכה) בקבלת חומר והעברת מתהליך הדרכה לתהליך ייצור עבור 1,600 סוקרים.

1.1.2.4. תמיכה בהפעלת מערך התקשוב בלשכות אזוריות במהלך תקופת המפקד, במשך עד חצי שנה.

1.1.2.5. הפעלת מוקד שו"ב (מערכות מידע) לתמיכה בכ-1,600 סוקרים, במשך 5 חודשים.

1.1.2.6. סגירת ופירוק מערך התקשוב בלשכות אזוריות.

1.1.2.7. איפוס ובדיקת תקינות 1,600 מחשבים.

1.1.2.8. אספקת מומחי System ואבטחת מידע.

1.2. מבנה המסמך

מסמך זה בנוי ממספר חלקים עיקריים לפי המבנה הבא:

1.2.1. הקדמה ורקע כללי

1.2.2. ניהול סיכונים – אינו דרוש בפרסום במכרז.

1.2.3. הנחיות אגף הגנת הסייבר לשירות המוצע – **מחויב בפרסום במכרז**.

1.3. היקף ומגבלות

1.3.1. מסמך זה הינו מסמך הנחיות מנדטוריות וחלק בלתי נפרד מהמכרז.

1.4. אחריות

1.4.1. ראש אגף הגנת הסייבר בלמ"ס – כתיבה ואישור ההנחיות.

1.4.2. מנהלת מערכות מידע (אגף טד"מ) – רכש ויישום השירות.

1.4.3. מחלקה משפטית – קביעת הנחיות משפטיות מול הספק.

1.4.4. מחלקת רכש – פרסום ההנחיות במכרז.

1.4.5. הספק הזוכה – יישום ההנחיות.

2 איומים והערכת סיכונים

2.1. סוגי המידע

הלמ״ס מחויבת בתנאי שמירת סודיות מחמירים על בסיס פקודת הסטטיסטיקה, תקנות הגנת הפרטיות והנחיות מערך הסייבר הלאומי. בין סוגי המידע העשויים להיות חשופים לספק ועובדיו הינו מידע רגיש הכולל מידע טכנולוגי (מבנה הרשת, מערכות הגנה וכיו״ב) אך גם מידע אישי על עובדים ו/או אזרחים. חשיפת המידע לספק ו/או לעובדים מטעמו יוצרים סיכונים לא מעטים בתחומים שונים וברמות סיכון שונות.

2.2. מקורות האיום

גורמים פנימיים (עובדים וספקים), המספקים שירותי לליווי ההקמה והתפעול של מערך המחשוב זוהו בעבר כסיכון עיקרי במודל שרשרת האספקה ויכולים להוות סיכון ללמ״ס בהיבטי: דלף מידע, איתור הספק וניצול חולשות (אנושיות או טכנולוגיות) במטרה לפגוע בלמ״ס, סחיטת הספק וכיו״ב.

2.3. סיכוני אמינות

הלמ״ס רואה במהימנות מידע ככלי מהותי להתמודדות משפטית וחוקית עם פושעי סייבר. לפיכך מהימנות המידע הנאסף ושימוש בו בעת הצורך במסגרת תהליך הוכחות וראיות, הוא נושא קריטי. להלן סיכונים מהותיים שהוגדרו בנושא זה:

האיום	השפעה[1]	פירוט האיום והשלכתו	המענה הנדרש
פגיעה באמינות המידע - בחצרות הלמ״ס	**גבוהה**	שימוש בכוח אדם לא מיומן, אשר במהלך אספקת השירות עלול לפגוע במערכות המידע של הלמ״ס (גם שלא במתכוון) **השלכה: פגיעה בזמינות מידע, מערכות או השירות.**	חבות משפטית של ספק השירותים בהקשר נזק והגדרת אחריות וסעדים בהסכם המשפטי עם הספק.

סיכוני סודיות

השירות יהיה מבוסס בעיקר על פעילות טכנית במערכות החשופות לשירות המפקד ובין היתר סוגי מידע המוגדרים כמידע רגיש על פי תקנות הגנת הפרטיות.

האיום	השפעה	פירוט האיום והשלכתו	המענה הנדרש
חשיפת מידע במהלך השירות	**גבוהה**	גישה לוגית או פיזית למערכות מידע וכן בגישה למתחמים רגישים **השלכה לדוגמה: חשיפת מידע רגיש**	הספק יעמיד כוח אדם מקצועי בעל הכשרה , הסמכה סיווג בטחוני ויחתים את כלל העובדים על הסכם סודיות. הגדרת אחריות וסעדים בהסכם המשפטי עם הספק באי עמידה בהנחיות הלמ״ס.
גישה של עובדי הספק	**גבוהה**	ניצול הרשאות גישה פיזיות או לוגיות למידע רגיש	יישום מדיניות הרשאות למידור גישה למידע אשר יבטיח כי רק ספק שאושר על ידי הלמ״ס יוכל לגשת למידע זה.

[1] הערה סובייקטיבית הנובעת מסוג האיום, מקורו, וקטור התקיפה, קלות/הסתברות המימוש, השפעת הנזק האפשרית וכדומה.

אישור מורשה חתימה: _____ אישור ממונה אבטחת מידע: _____

(לא מורשים) /למידע		**השלכה: דלף מידע רגיש, פרסום המידע ברבים. במקרה קיצון, מסירת המידע לתוקף או גורם זר אשר ישתמש במידע לסחוט את הלמ"ס.**	יצירת מנגנון התראות לאיתור ניסיונות גישה למידע (בקרה פיזית ולוגית). הגדרת אחריות וסעדים בהסכם המשפטי עם הספק.
חריגה מתקנות הגנת הפרטיות	**גבוהה**	חשיפת מידע על עובד או פרט במסגרת אספקת השירות, עלול להיחשב כבלתי מידתית או כבעלת חוסר סבירות קיצונית ותציג את הלמ"ס כמפירת תקנות הגנת הפרטיות לעובד או לפרט. **השלכה: חשיפת הלמ"ס (ויתכן גם את הספק) לתביעות וסעדים.**	הספק בשיתוף המחלקה המשפטית ואגף הגנת הסייבר בלמ"ס יפעלו לכתיבה ועדכון נהלי העבודה הדרושים לשירות ויוודאו כי כלל העובדים של הספק עובדים על בסיס נהלים אלה.

2.4. סיכוני זמינות

האיום	השפעה	פירוט האיום והשלכתו	המענה הנדרש
פעילות עובדי הספק אשר תגרור לפגיעה בזמינות מערכות מידע	**גבוהה**	פעילות במערכות מידע אשר תגרור השבתן.	הספק בשיתוף אגף מערכות מידע יפעלו לכתיבה ועדכון נהלי העבודה הדרושים לשירות ויוודאו כי כלל העובדים של הספק עובדים על בסיס נהלים אלה.

אישור מורשה חתימה: _____ אישור ממונה אבטחת מידע: _____

2.5. סיכונים בשרשרת האספקה

האיום	השפעה	פירוט האיום והשלכתו	המענה הנדרש
חולשות בשרשרת אספקה	גבוהה	השירות הניתן ללמ"ס יינתן על ידי ספק אשר ללמ"ס אין שליטה עליו. השימוש במערכות המחשוב והרשת של הספק עלול לפתוח פתח לסיכונים שונים ואשר יכולים לשמש תשתית תקיפה על הלמ"ס והמידע האגור בה, בין אם המתקפה תעשה באופן ישיר מחצר הספק, או שהספק ישמש תשתית תקיפה לגורם שלישי (הספק כווקטור תקיפה).	בטרם אישור וחתימה על הסכם התקשרות עם הספק יש לבצע סקר בחצרות הספק לאיתור חולשות אבטחה (לוגיות, פיזיות, כוח אדם, מדיניות, נהלים וכדומה) וכן להעביר הנחיות לתיקון הממצאים שיתגלו עד להפעלת השירות. יש לעגן הנחיות אבטחת מידע מחייבות, אשר הספק יידרש להסכים ולחתום עליהם במסגרת הסכם ההתקשרות. יש להבהיר לספק כי במהלך ההתקשרות, הלמ"ס או מי מטעמה יהא רשאי לבצע בקרות פתע לקיום הנחיות אבטחת המידע.

2.6. סיכוני סייבר אחרים

האיום	השפעה	פירוט האיום והשלכתו	המענה הנדרש
תהליך מו"מ עם תוקף אשר יחמיר את השלכות האירוע	גבוהה	מאירועי סייבר וטרור סייבר בעולם ניתן להסיק, כי לעיתים עולה הצורך בצוות מו"מ מיומן, אשר נדרש להתערב ולנהל שיח עם התוקפים. שימוש בצוות מו"מ שאינו מיומן, עלול לפגום באיכות התחקור.	בטרם אישור וחתימה על הסכם התקשרות עם הספק יש לבצע סקר בחצרות הספק לאיתור חולשות אבטחה (לוגיות, פיזיות, כוח אדם, מדיניות, נהלים וכדומה) וכן להעביר הנחיות לתיקון הממצאים שיתגלו עד להפעלת השירות. יש לעגן הנחיות אבטחת מידע מחייבות, אשר הספק יידרש להסכים ולחתום עליהם במסגרת הסכם ההתקשרות. יש להבהיר לספק כי במהלך ההתקשרות, הלמ"ס או מי מטעמה יהא רשאי לבצע בקרות פתע לקיום הנחיות אבטחת המידע.

3 הנחיות התקשרות עם הספק

3.1. כתב הסכמה לאמור בנספח אבטחת המידע

3.1.1. נספח אבטחת המידע המצורף למכרז הוא מנדטורי על כלל סעיפיו.

3.1.2. על נספח הנחיות זה יחתום בנוסף למורשה חתימה מטעם המציע גם ממונה אבטחת המידע מטעם המציע וכן הגורם אשר יספק את השירות בפועל. הנ"ל יחתמו כי הם מתחייבים לפעול ליישום כלל הנחיות אבטחת המידע והגנת הסייבר המפורטות במסמך זה.

3.1.3. יש להבהיר לספק כי בעת מתן השירותים, יתכן כי יועברו לספק המבצע הנחיות נוספות. ככל שיועברו הנחיות נוספות, יידרש הספק לפעול ליישומן. הלמ"ס משאירה לעצמה את הזכות לפסול ספק שלא יענה על קריטריונים אלה במלואם.

3.2. עמידה בהוראות חוק ורגולציה

3.2.1. הספק מסכים כי במידה וייחשף או יימסר לו מידע רגיש (תפעולי או אישי) במסגרת עבודתו, יידרש הספק להצהיר כי הוא עומד בתקנות הגנת הפרטיות לשמירה על מידע אישי וינקוט את מירב האמצעים לשמירה על המידע מפני סיכוני סודיות/דלף מידע וחשיפתו לגורם זר שאינו מורשה לכך.

3.3. סקר חצרות ספקים

3.3.1. הלמ"ס כפופה להנחיות מערך הסייבר הלאומי ולפיכך בטרם כל התקשרות עם ספק, היא מחויבת בביצוע סקר ספק.

3.3.2. מילוי השאלון יעשה במערכת יעדים ובקרות לארגון (יוב"ל) בקישור הבא: (https://www.gov.il/he/departments/news/querysupply).

3.3.3. סוג השאלון שימולא יהיה שאלון ספק ברמה A וימולא על ידי בודק מאושר מערך הסייבר הלאומי.

3.3.4. הספק יעביר לראש אגף הגנת הסייבר בלמ"ס אישור/אסמכתא לביצוע השאלון (ללא הראיות/התעדה), אך יידרש להציגן ללמ"ס במידת הצורך ובמסגרת סקר חצרות ספק שתבצע הלמ"ס.

3.4. רפרנט מטעם הספק

3.4.1. הספק יגדיר איש קשר, אשר יהווה רפרנט/מנהל הפרויקט למול הלמ"ס, שפרטיו והדרכים ליצירת קשר עמו ושזהותו תאושר על ידי הלמ"ס. עדיפות תינתן לגורם טכני.

3.5. גיוס וסיווג עובדי הספק המספקים את השירות

3.5.1. כל העובדים בפרויקט או עובדים המוצעים לפרויקט, יאושרו על ידי קב"ט הלמ"ס. סיווג העובדים יהיה באופן הבא:

3.5.1.1. מנהל הלקוח יהיה ברמת סיווג בטחוני **בתוקף** ברמה 3 לכל הפחות ותצהיר היעדר רישום פלילי.

3.5.1.2. מומחי סיסטם ואבטחת מידע יהיו רמת סיווג בטחוני **בתוקף** ברמה 3 לכל הפחות ותצהיר היעדר רישום פלילי.

3.5.1.3. אנשי תמיכה טכנית ומוקד יהיו רמת סיווג בטחוני **<u>בתוקף</u>** ברמה6 (היעדר רישום פלילי)

3.5.2. כל העובדים ימלאו טופס תצהיר היעדר רישום פלילי.

3.5.3. הספק ועובדיו בפרויקט יחתמו על התחייבות לשמירת סודיות.

3.5.4. הלמ"ס תהא רשאית לדרוש מהעובדים לעבור בדיקות מהימנות אצל בודק מוסמך בלתי תלוי, על חשבון הספק.

3.5.5. עובד שלא יאושר על ידי הלמ"ס, לא יוכל לספק שירותים במסגרת שירות זה והספק יידרש למצוא עובד אחר.

3.5.6. הספק הזוכה יתחייב לקבל מראש ובכתב את הסכמת הלמ"ס וראש אגף הגנת הסייבר בלמ"ס לגבי כל עובד מעובדיו ו/או מי מטעמו, המועסק בביצוע עבודות על פי מכרז זה וראש אגף הגנת הסייבר בלמ"ס יהא רשאי לסרב לתת את הסכמתו להעסקת עובד פלוני של הספק הזוכה מכל טעם שימצא לנכון, ומבלי שיהא עליו לנמקו.

3.5.7. אין באישור הלמ"ס להעסקת עובד כלשהו כדי לפטור את הספק הזוכה מאחריותו לפי הסכם זה או לפי כל דין, ואין בכך מניעה מהלמ"ס לדרוש החלפת עובד כל שהוא, כולל עובדי קבלני המשנה, בכל מקרה שהלמ"ס תאשר הפעלת קבלני משנה, לפי שיקול דעתה.

3.5.8. הספק הזוכה יהיה אחראי כלפי הלמ"ס על כל פעילות עובדיו ו/או מי מטעמו במסגרת ההתקשרות והספק יישא באחריות ישירה לכל פער או סיכון הנובע מכך.

3.5.9. הספק הזוכה מתחייב שכל עובדיו, ו/או מי מטעמו ו/או משתמשי צד שלישי, מבינים את מלוא האחריות המוטלת עליהם בנוגע למידע שהועבר על ידי הלמ"ס לזוכה.

3.6. קבלני משנה

3.6.1. בכל מקרה שהלמ"ס תאשר הפעלת קבלני משנה, לפי שיקול דעתה, יחולו כל החובות וההנחיות המפורטות במכרז ובנספח זה גם על קבלנים וספקי משנה של הספק לרבות הנחיות סיווג הספקים. אולם המחויבות הכוללת למתן השירות היא על הספק הזוכה והספק יישא באחריות ישירה לכל פער או סיכון הנובע משימוש בקבלני משנה.

3.7. אופן השירות

3.7.1. השירות יינתן מחצרות הלמ"ס ושלוחותיה.

3.7.2. לא תתאפשר גישה מרחוק למערכות הלמ"ס בשום אופן.

3.8. מומחיות עובדים

3.8.1. עובדי הספק יהיו בעלי כישורים טכנולוגיים וניסיון מתאים.

3.8.2. עובדי הספק ינוהלו על ידי הלמ"ס.

3.9. בקרה גישה

3.9.1. הספק יגן על סביבות בהם יוחזק ינוהל או יעובד מידע של הלמ"ס.

3.9.2. הספק יפעל למידור גישה פיזית למידע של הלמ"ס (על בסיס הצורך למידע) לגורמים שאושרו על ידי הלמ"ס במסגרת השירות הניתן.

3.10. אירועי בטחון

3.10.1. אירועי בטחון בסביבת הספק, אשר יחולו בסביבה המיועדת לפעילות הספק במסגרת הסכם התקשרות זה, ידווחו גם לאגף הגנת הסייבר בלמ"ס.

3.11. זכויות קניין

3.11.1. כל מידע שייאסף, ינוהל, יתוחקר עבור הלמ"ס במסגרת ההתקשרות – יחשב כקניין רוחני של הלמ"ס ולא יעשה בו כול שימוש אחר שלא באישור בכתב מראש אגף הגנת הסייבר בלמ"ס.

3.12. סיום התקשרות עם ספקים

3.12.1. בסיום התקשרות עם ספק – יחסמו ויוסרו כל הרשאות הגישה אשר נפתחו לספק ולעובדיו במערכות המחזיקות מידע ללמ"ס: חשבונות המשתמשים.

3.12.2. במידה ונמסר לספק או לעובדיו מידע כלשהו דפוס, התקן מחשוב, התקן תקשורת, מודם סלולרי, התקן אימות זיהוי וכדומה – יוודא הגורם הפנימי בלמ"ס האחראי על הספק – השבת החומרים ללמ"ס.

3.12.3. הספק מתחייב להחזיר ללמ"ס כל מידע פיזי או לוגי אשר נמסר לו לצורך עבודתו.

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

3.12.5. בסיום התקשרות עם ספק כול המידע של הלמ"ס ימחק ממחשבי הספק (למעט המחויב לפי החוק).

3.12.6. כול חומרה שניתנה על ידי הלמ"ס תוחזר ללמ"ס.

3.12.7. כל פעילות שבוצעה עבור הלמ"ס לא תיחשף גם לאחר סיום ההתקשרות ולמשך 3 שנים לפחות.

4 הנחיות מודעות אבטחת מידע לעובדי הספק

הנחיות אלה יצורפו **<u>לנהלי העבודה ונספח הסודיות</u>** של עובדי הספק, אשר יחויבו להסכים להם בחתימתם (ללא חריגים):

4.1. בקרות

4.1.1. הלמ"ס מפעילה אמצעי בקרה ומעקב אחר פעילות עובדים בשגרה. לפיכך כל עובד אשר יקבל לידיו חשבון משתמש או גישה למערכות מחשוב של הלמ"ס מסכים לאמור להלן.

4.1.2. אגף הגנת הסייבר יבצע בקרות מדגמיות בתדירות גבוהה. עובד שלא יקיים את הנחיות הלמ"ס – יסיים את עבודתו וינקטו נגדו צעדים משמעתיים.

4.2. שימוש באמצעי מחשוב

4.2.1. השימוש באמצעי המחשוב יעשה רק עבור המטרה שלשמם נועדו ועבור שירותי הלמ"ס בלבד.

4.3. שימוש בחשבון משתמש וניהול סיסמאות

4.3.1. לאור העובדה שהנכם פועלים בשם הלמ"ס יתכן ובמסגרת פעילותכם תהיו חשופים למערכות ולמידע של הלמ"ס, לפיכך חשוב להקפיד בין היתר על ההנחיות הבאות:

4.3.1.1. פרטי הזיהוי (שם המשתמש והסיסמה) למערכות המחשוב של הלמ"ס הינם אישיים וסודיים ואין להעבירם לגורם אחר.

4.3.1.2. יש לוודא כי שם המשתמש הינו נפרד וכי וסיסמתך אינה ידועה לאחרים.

4.3.1.3. יש לעשות שימוש בסיסמא "חזקה" כלומר שילוב של אותיות גדולות וקטנות ומספרים וסימנים באורך של 8 תווים ומעלה.

4.3.1.4. אין לשמור את פרטי הזיהוי במקום שעשוי להיות חשוף לגורמים אחרים מלבדכם כגון על גבי הטלפון הנייד, שולחן העבודה, ליד המחשב, בקבצים שבמחשב האישי, או במקום שיקל על אחרים למצוא אותה.

4.3.1.5. אין להשתמש בסיסמה זו בכל מקום שאינו הלמ"ס, רשתות חברתיות, שימוש פרטי וכיו"ב כיוון הדבר מעלה את הסיכוי לחשיפת הסיסמה ולפריצה לחשבונכם.

4.3.1.6. אין למסור את סיסמתך האישית לאתר לשום גורם, גם אם הוא מזדהה כגורם מטעם הלמ"ס או מטעם הספק ובוודאי שלא לגורם חיצוני. במידה ותתבקש לעשות כן, עליך לפנות למנהלך הישיר ולעדכן את חמ"ל הסייבר בלמ"ס.

4.4. כללי גלישה בטוחה עבור עובד הספק

4.4.1. במידה ותתאפשר לך גלישה באינטרנט במסגרת עבודתך, אין להיכנס לאתרים אחרים מלבד אלא שאושרו לך לצורך עבודתך.

4.4.2. אין לעשות שימוש אישי לרבות: גלישה לאינטרנט, רשתות חברתיות, אפליקציות צ'אט, גישה לדוא"ל פרטי, גלישה לרשתות ופורומים זרים.

4.4.3. אין לעשות שימוש בחשבונות הלמ"ס ברשתות ואתרים זרים.

4.4.4. אין ליצור קשר עם גורמים זרים ללמ"ס, בשם הלמ"ס – אלא במקרים בהם הצורך העסקי מגדיר זאת.

4.4.5. בתום הגלישה חשוב לצאת מהיישומים בדרך מסודרת באמצעות כפתור היציאה. יציאה מהשירות תמנע מאנשים אחרים גישה לחשבונך.

4.5. הנחיות לאבטחת המחשב האישי

4.5.1. קיים איסור להורדה והתקנת קבצים ממקורות בלתי ידועים ומהתקנתם במחשב. כל פעילות כזו מצריכה אישור של אגף הסייבר בלמ"ס.

4.5.2. חל איסור מוחלט להעלות או להוריד קבצים מכל סוג או לשלוח אותם בדוא"ל.

4.5.3. יש לנעול את המחשב בכל פעם בה הנך עוזב אותו, גם אם מדובר לזמן קצר.

4.6. קיום שיח עם מבקשי מידע ומקבלי שירותי תמיכה ובמוקד

4.6.1. כל עובד יעבור הדרכה מסודרת אשר תנחה אותו "מה לענות" ו-"כיצד לענות", ובעיקר "מה לא לענות". כמו כן ההדרכה תעסוק בדרכים "אלגנטיות" ונעימות לסיום ה"השיחה" עם מבקש המידע.

4.7. איסור שימוש באפליקציות זרות: צ'אט, רשתות חברתיות וכיו"ב

4.7.1. אין לעשות שימוש בתוכנות או אמצעי מידע שלא אושרו לצורך עבודתך.

4.8. שימוש באפליקציות מסרים ומשלוח מסרונים

4.8.1. העברת מידע באמצעות מסרונים/מסרים לא תכלול פרטים או מידע רגיש על עובדים, פרט או מידע טכנולוגי אלא מידע אינפורמטיבי בלבד.

4.8.2. העברת מסרונים לא תכלול קישורים והפניות (לינקים) או קבצים.