נספח ב' 1 הנחיות אבטחת מידע לאספקת זכויות שימוש בתשתית CRM עבור הלמ"ס

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

1. הקדמה

1.1. רקע

1.1.1. הלשכה המרכזית לסטטיסטיקה (להלן: "הלמ"ס" ו/או "למ"ס"), מעוניינת ביישום מערכת CRM לצורך ניהול פניות והקשר עם הציבור וכן לניהול תהליכים בין משרדיים פנימיים. השירות כשירות בענן ציבורי.

1.1.2. מערכת ה- CRM ומערכות ההגנה בסביבתה יסופקו על גבי ענן ציבורי השירות יפעל בתצורה אשר תשמור על ריבונות המידע וימנע זליגה של מידע רגיש אל מחוץ לגבולות המדינה. יחד עם זאת, באופן זמני וכדי לא לעקב את שירות, ניתן יהיה להקים את המערכות באזור זמני בחו"ל, בארצות המאושרות על פי הנחיות רשות התקשוב הממשלתית.

1.1.3. התחייבות המציע כי בתוך שנתיים ממועד הפעלת שירות מ-region בתחומי מדינית ישראל, על ידי אחד או יותר משני הספקים הזוכים ברובד I במכרז נימבוס הממשלתי, שירותי תשתית ה-CRM המבוקשים על ידי הלמ"ס יסופקו מתחומי מדינת ישראל באמצעות הנימבוס.

1.2. מטרה

1.2.1. מסמך זה נועד להגדיר את הנחיות אבטחת המידע והגנת הסייבר להקמת מערכת ה- CRM בענן זמני בחו"ל עד להפעלת שירות נימבוס בארץ. מסמך זה מהווה חלק בלתי נפרד מהמכרז.

1.3. מבנה המסמך

מסמך זה בנוי משלושה חלקים לפי הסדר הבא:

1.3.1. רקע כללי.

1.3.2. הערכה וניתוח סיכונים.

1.3.3. הנחיות אבטחת מידע.

1.3.4. נספחים.

1.4. מסמכי רפרנס

ההנחיות המובאות במסמך זה מבוססות בין היתר על הנחיות הבאות:

1.4.1. תורת ההגנה בסייבר - מערך הסייבר הלאומי.

1.4.2. שימוש בשירותי ענן – גרסה 1.0 – מערך הסייבר הלאומי.

1.4.3. הנחיות רשות להגנת פרטיות לשימוש בענן ציבורי והגנה על מידע רגיש ("תקנה 5.5").

1.4.4. אבטחת מידע למעבר לענן ציבורי במסגרת מכרז נימבוס ("תקנה 5.31").

1.4.5. עקרונות פיתוח מערכות להיערכות ענן - ראש רשות התקשוב הממשלתי מספר הנחיה 4.2.4 (טכנולוגיות מחשוב ענן).

1.4.6. מחשוב ענן בממשלה – מרכז המחקר והמידע, כנסת ישראל (מיום 29 בינואר 2020).

1.4.7. שאלון ספקים – יוב"ל (על כלל נושאיו לרבות שירותי ענן).

1.4.8. NIST 800-53r5 להגנה במערכות מידע.

1.4.9. חוזר "שימוש במחשוב ענן במערכת הבריאות" מיום 21 בפברואר 2021 (מס': 2/2021).

1.4.10. מסמכי בקרות CSA לשירותי ענן SAAS, IAAS, PAAS.

1.4.11. דרישות עקרוניות לעבודה עם ספקים בתצורת ענן (XaaS) אפריל 2019 – מערך הסייבר הלאומי.

1.5. היקף ומגבלות

1.5.1. מסמך זה והנחיותיו הינו חלק בלתי נפרד מהמכרז והינו מחייב. ראש אגף הגנת הסייבר הינו הגורם היחיד הרשאי להקל בהנחיות המסמך.

1.5.2. אישור שימוש בשירותי ענן ציבורי, דרוש אישור מערך הסייבר הלאומי ורשות התקשו"ב הממשלתית. על פי כן יתכנו שינויים בהנחיות אבטחת המידע המופיעות בנספח זה.

1.5.3. כתיבת ההנחיות נעשו על בסיס היכרות עם פתרונות CRM מקובלים. מאידך כתיבת הנחיות אבטחת המידע נעשו בטרם הצגת תכנון "על" או תכנון מפורט של המערכת או בחירה בסוג הפתרון. לפיכך יתכן כי יועברו הנחיות פרטיות נוספות במהלך יישום הפתרון.

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

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

1.5.6. המסמך אינו מתייחס לדרישות עיצוב, מבניות, או הנגשה (חוק).

1.6. אחריות

1.6.1. מנהלת הפרויקט[1] בלמ"ס ביחד עם ראש אגף הגנת הסייבר, ומנהל מערכות המידע בלמ"ס יהיו אחראיים לנושאים הבאים:

1.6.1.1. אישור התהליך בוועדת הענן הממשלתית של רשות התקשוב.

1.6.1.2. ביצוע בקרה על הפתרון המוצע, בחינת תקינותו ומעקב אחר תקלות וסיכוני סייבר וכן לנהל מעקב שוטף אחר יישום הפתרון בארגון.

1.6.2. הנחיה וביקורת על יישום אבטחת המידע בפרויקט – ראש אגף הגנת הסייבר בלמ"ס.

1.6.3. אישור ההנחיות המשפטיות בשימוש בשירות מיקור חוץ - מחלקה משפטית בלמ"ס.

1.6.4. פרסום ההנחיות במכרז – באחריות מינהלת הפרויקט בלמ"ס.

2. מונחים

2.1. שירותי ענן

[1] מינהלת הפרויקט הינה הגורם הפנימי בלמ"ס אשר אחראי על הפרויקט, מכיר את התהליכים העסקיים ואת הפתרון המבוקש ליישום

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

2.1.1. בשנים האחרונות גוברת בעולם מגמת המעבר לשימוש בשירותי ענן בתעשיות רבות. טכנולוגיית הענן היא מרכיב חשוב בהכנסת חדשנות לארגון. היא מאפשרת לארגון גמישות תפעולית ואת היכולת לנצל באופן יעיל ומיטבי את משאבי המחשוב העומדים לרשותו, לצד חיסכון בעלויות הפעלת אותם שירותים בתוך הארגון.

2.1.2. בנוסף, טכנולוגיית הענן יכולה לסייע ללמ"ס לארגונים לפתח יכולות מתקדמות ויישומים חדשניים, אשר רבים מהם פועלים כיום בענן בלבד. הפעלת יישומים באמצעות מחשוב ענן צריכה להיעשות באופן מושכל ומאוזן.

2.1.3. ענן ציבורי (Public Cloud) בהגדרתו הוא שירות חיצוני המאחד מספר ארגונים ולקוחות על תשתית מרכזית אחת[2].

2.1.4. מונחי ענן:

2.1.4.1. Infrastructure as a Service – IaaS – הכוונה לשירותי תשתית המסופקים על ידי ספק שירותי הענן, לדוגמא: תשתיות חשמל, אחסון, שרתים פיזיים/וירטואליים, מערכות תקשורת, מערכות אבטחת מידע.

2.1.4.2. Platform as a Service – PaaS - הכוונה לשירותי פלטפורמה המסופקים (בנוסף לשירותי ה- IAAS) על ידי ספק שירותי הענן, לדוגמא: סביבות פיתוח, מערכות הפעלה ושכבת Middleware.

2.1.4.3. Software as a Service – SaaS- הכוונה לשירותי תוכנה המסופקים (בנוסף לשירותי ה- IAAS וה- PAAS) על ידי ספק שירותי הענן, לדוגמא אפליקציית CRM.

2.2. ועדת ענן ומדיניות שימוש בענן בלמ"ס

2.2.1. בהחלטת ממשלה מס' 2443 מיום 15.2.2015 בנושא "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" הונחו המנהלים הכלליים של משרדי הממשלה ויחידות הסמך לפעול לשיפור רמת הגנת הסייבר בתחומי משרדם.

2.2.2. לפיכך בטרם פניה למכרז ויישום תשתית ענן מכל סוג, הלמ"ס תמנה ועדת ענן פנימית אשר תפעל לקידום מדיניות ענן ולהנחות את הגורמים הרלוונטיים בכל הנוגע לשימוש ויישום בשירותי ענן, ניהול סיכונים (תהליכיים, תפעוליים, פרטיות, המשכיות עסקית ורציפות תפעולית, הגנת סייבר), ובכלל זה ליישום בקרות בעת השימוש במחשוב ענן.

2.2.3. הספק יסייע בידי ועדת הענן של הלמ"ס בתהליכי מעבר למחשוב ענן במשרדי ממשלה כאמור בסעיף 7 (ותתי סעיפיו) כמפורט במסמך *"הנחיות ראש רשות התקשוב הממשלתי הנחיות היחידה להגנת הסייבר בממשלה – יה"ב (מספר הנחיה 5.5)"*.

2.2.4. הספק מאשר כי אי עמידה בהנחיות רשות התקשוב הממשלתיות וכן אי אישור ועדת הענן הממשלתית או ועדת הענן של הלמ"ס עלולה למנוע שימוש בשירותי מחשוב ענן לפתרון המוצע על ידו במלואו או בחלקו.

---

[2] מתוך מסמך הנחיות אבטחת מידע למעבר לענן ציבורי ראש רשות התקשוב הממשלתי הנחיות היחידה להגנת הסייבר בממשלה – יה"ב מספר הנחיה 5.5 מיום 04.02.2019.

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

2.3. CRM

2.3.1. Customer Relationship Management - CRM הינה מערכת לניהול תהליכים ושירותים בין לקוחות שונים (פנים וחוץ ארגוניים).

2.3.2. מבקש מידע – אזרח ו/או גורם חיצוני ללמ"ס אשר פונה ללמ"ס באחד מערוצי התקשורת לקבלת מידע.

2.4. מונחי המשכיות עסקית

2.4.1. Recovery Point Objective (RPO) – נקודת הזמן האחרונה אליה ניתן לחזור.

2.4.2. Recovery Time Objective (RTO) – הזמן המקסימלי להחזרת השירות.

2.4.3. Work Recovery Time (WRT) – הזמן שבו לוקח לאושש את המערכת.

2.4.4. Maximum Tolerable Downtime (MTD) – הזמן שבו ניתן לחיות ללא מערכת ה- CRM.

2.5. מונחי הגנה בסייבר

2.5.1. הלבנה – ניקוי והשטחת מידע הנכנס מערוצי מידע חיצוניים.

2.5.2. השחרה – ניקוי מידע רגיש המועבר לערוצי מידע חיצוניים.

2.5.3. DOS – מניעת שירות.

2.5.4. DDOS – מניעת שירות מבוזרת.

2.5.5. End Point Detection and Response – EDR – מערכת הגנה בתחנות קצה ושרתים להתמודדות ומניעת התפרצות קוד עוין.

3. תהליכים עסקיים עיקריים (דוגמה)

המערכת תנהל בין היתר את התהליכים הבאים:

3.1. תהליכים וממשקים בין הלמ"ס לגורמים חיצוניים - לא רגישים (סיווג בלמ"ס)

מערכות או מידע החשוף או ניתן לחשיפה לציבור:

3.1.1. ממשקים רב ערוציים – תחת ממשקים רב ערוציים יתכנו ערוצי צ'אט, אפליקציות מסרים, רשתות חברתיות, דוא"ל, טלפון, אינטרנט, רשתות חברתיות, Mobile.

3.1.2. דוגמת פניות ציבור ליחידת סקרים עבור ניהול תהליכי טיפול בפנייה ע"י יחידת סקרים, ניהול תהליכי טיפול בפנייה ע"י יחידות רוחביות נותנות שירות וניהול תהליכי טיפול בפנייה באמצעות היחידות הרוחביות בפיקוח של יחידת סקרים.

3.1.3. ממשקים למערכות שאינן קריטיות / אינן מנהלות נתונים רגישים או חסויים.

3.1.4. מערכות שפגיעה בהן איננה מהווה פגיעה ביכולת המשילות של ממשלת ישראל ו/או בסמלי שלטון.

3.1.5. קבלת מידע סטטיסטי – עיבודים מיוחדים. עבור ניהול תהליכי פניות ציבור לקבלת מידע סטטיסטי פשוט/בשליפה/מורכב/עיבוד מיוחד.

3.1.6. טיפול בפניית ציבור עפ"י סיווג הפנייה עבור ניהול תהליכי פניות ציבור בנושאי טיפול שונים המנותבות ליחידות העסקיות השונות.

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

3.1.7. פניות של ארגונים בינלאומיים עבור ניהול תהליכי בקשה למילוי סקר / נתונים, שאלוניי ENP /אזוריים, פרסום בקשות חריגות.

3.2. תהליכים פנימיים - לא רגישים (סיווג בלמ"ס)

3.2.1. ניהול ידע.

3.2.2. ניהול תהליכים פנימיים יחידת הוצאה לאור ודוברות עבור ניהול תהליכי טיפול בלוחות שנתיים קיימים וחדשים.

3.2.3. ניהול תהליכים פנימיים רכש עבור ניהול תהליכי דרישות/בקשות חדשות לרכש נושאים כלליים.

3.2.4. ניהול תהליכים פנים ארגוניים (בנא"מ) אגף רכש נכסים ולוגיסטיקה עבור ניהול תהליכי פניות בנוגע לתקלות שבר/ תקלות מונעות / חניון רכבים/ טלפונים ניידים.

3.2.5. ניהול תהליכים פנים ארגוניים הדרכה עבור ניהול תהליכי פניות בנוגע לרישום לקורסים/ימי עיון והכשרות ובנוסף פניות בנוגע לאיכות ומצוינות עובדי הלמ"ס.

3.2.6. ניהול תהליכים פנים ארגוניים תקציבים עבור ניהול תהליכי פניות בנוגע לתכנון תקציב ותוכניות שנתיות - בקשות כלליות.

4. איומים והערכת סיכונים במחשוב ענן

פרק זה מתבסס בין היתר על פרק 6 במסמך אבטחת מידע למעבר לענן ציבורי מספר הנחיה 5.5

4.1. סוג המידע

4.1.1. הפתרון נדרש להתממשק למגוון רחב של שירותים ובין היתר תעביר מידע בין ערוצי תקשורת חיצוניים: אתר אינטרנט, דוא"ל, רשתות חברתיות, אפליקציות מסרים ומערכות ברשת התפעולית של הלמ"ס.

4.1.2. המידע אשר ינוהל בשירות הענן יהא:

4.1.2.1. מידע **<u>ללא סיווג ו/או פתוח לציבור</u>**. או מידע על תהליכי רכש כללי כאמור בפרק 3 תהליכים עסקיים עיקריים.

4.1.2.2. מערכות שאינן קריטיות.

4.1.2.3. מערכות שאינן מנהלות נתונים רגישים או חסויים.

4.1.2.4. מערכות שפגיעה בהן איננה מהווה פגיעה ביכולת המשילות של ממשלת ישראל ו/או בסמלי שלטון.

4.1.3. לא ינוהל מידע ולא יתבצע קישור למערכות קריטיות ו/או מע' ליבה ו/או מע' המספקות תשתיות ליבה עסקית או מערכות המנהלות נתונים רגישים או חסויים.

4.1.4. אך אף על פי כן, מעצם השירות חשוף לציבור ולסביבות מחשוב חיצוניות, הלמ"ס תתייחס למידע ולשירות ברמת רגישות גבוהה.

4.1.5. להלן מספר דוגמאות לסיכונים ותרחישי איום אשר יש לשקול את השפעתם ודומיהם בעת גיבוש החלטה על מעבר לסביבות ענן ובחינת תהליכי הבקרה להפחתת הסיכון. יובהר כי מדובר בדוגמאות בלבד ולא ברשימה ממצה של סיכונים ותרחישי איום, ויש לבחון סיכונים ואיומים נוספים הרלוונטיים לשימוש בענן ציבורי, בהתאם לסוג השירות ומאפייניו וסוג המערכת והמידע המועברים לענן.

4.2. נכסי המידע להגנה

4.2.1. הספק אחראי לספק פתרון העונה באופן מלא על כלל האיומים המפורטים להלן.

4.2.2. **כל** מערכות מידע של הספק ומערכות או טכנולוגיות המוצעות על ידי הספק במסגרת פרויקט זה (לרבות מערכות פנימיות וחיצוניות, תשתית ואפליקציה וכיו"ב) נדרשות לעמוד בהנחיות אבטחת מידע החשופים לרשת האינטרנט וכן לסיכונים אפשריים ממערכות הספק וספקי משנה (סיכונים בשרשרת האספקה).

הערה לספק: פרק אבטחת המידע הינו מנדטורי לספק. הספק המציע נדרש לענות באופן מלא על כלל הסיכונים המפורטים פרק זה וכן על המפורט בפרק 6 "איומים במחשוב ענן" במסמך הנחיות רשות להגנת פרטיות להגנה על מידע רגיש ("תקנה 5.5") : בין אם באמצעות בקרות מונעות, מגלות או בקרות מפצות אחרות. במידה ולא קיימות בקרות, על הספק לפרט ולהציג את הפערים לראש אגף הגנת הסייבר בלמ"ס.

4.3. סיכוני סודיות

איומי חשיפה או זליגת מידע בסביבות מחשוב ענן יכולים להיגרם כתוצאה ממספר תרחישים. להלן דוגמאות לתרחישים נפוצים:

האיום	השפעה[3]	פירוט האיום והשלכתו	המענה הנדרש
דלף מידע ממערכות הענן של הספק וחשיפה לסיכונים רגולטוריים	**גבוהה**	חשיפת מידע כתוצאה מהפרדה לא יעילה בין לקוחות הענן (Tenants) החולקים את משאבי המחשוב. **השלכה: חריגה מהנחיות חוק ורגולציה (רשות התקשוב, מערך הסייבר).**	דרישת הפרויקט הינה לעשות שימוש בענן ציבורי, לפיכך יש לספק מענה למניעת דלף מידע (סינון תוכן יוצא) בשירות זה. היישום יתבצע ביישום בתשתיות הענן הציבורי. הספק יעמוד בתקני הגנה על מידע רגיש: תקנות הגנת הפרטיות, GDPR, תקני ISO27017, ISO27018, ISO2701, ISO27032, SOC 2 וכן בעל תאימות לתקנות הגנת הפרטיות במדיניות אירופה (GDPR) ו-תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 במלואן.

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

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

חשיפת מידע למדינה זרה	**גבוהה**	חשיפת מידע עקב צו בית משפט של ממשלה זרה (או מדינה עוינת). שמירת מידע בתחום שיפוט שאינו מדינת ישראל חושף את המידע לחוקים ותקנות של הממשלות בהם פועל ספק הענן ומאחסן את המידע. **<u>השלכה:</u> חריגה מהנחיות חוק ורגולציה (רשות התקשוב, מערך הסייבר).**	הספק מתחייב שלא למסור מידע לאף גורם זר, ללא רשות בכתב מהלמ"ס (עבור אותו מקרה פרטני) למסירת מידע.
דלף מידע המנוהל בשירותי -ה CRM או מספק הענן	**גבוהה**	זליגת בסיסי נתונים ומידע אשר הועבר או הושאר בסביבת מחשוב הענן בסיום ההתקשרות עם ספק שירותי מחשוב ענן ללא בקרות מספקות אשר נדרשות בכדי להגן על מידע שכזה והותאמו למתאר האיומים הרלוונטיים ודרישות החוק להגנת הפרטיות בישראל. **<u>השלכה:</u> חריגה מהנחיות חוק ורגולציה (רשות התקשוב, מערך הסייבר).**	מערכת ה- CRM נדרשת לתמוך ביכולת חיבור טכנולוגית אפליקטיבית למערכות צד ג' למניעת דלף מידע וכן על ממשקים לערוצי תקשורת חיצוניים מבוססי API שבהם יעשה שימוש במערכת ה- CRM. הספק יפרט את המערכות הנתמכות לנושא זה.
דלף מידע – שרשרת אספקה	**גבוהה**	חשיפת מידע ע"י עובדי ספק שירותי מחשוב הענן או צד שלישי בעל יכולת גישה למידע מחשוב ענן בדומה למיקור חוץ, מערב גורמים נוספים אשר אינם קשורים בקשר ישיר עם לקוח הענן ויתכן כי אינם מחויבים לחיסיון המידע ולבעליו. **<u>השלכה:</u> גישה למידע רגיש עלולה לחשוף את הלמ"ס לאירוע דלף מהותי וכפועל יוצא חריגה מהנחיות חוק ורגולציה (רשות התקשוב, מערך הסייבר).**	על הספק קיימת החובה לשמירה על מידע רגיש גם על ספקי צד ג' של ספק הענן.
גישה של גורמים זרים למידע	**גבוהה**	גישה לא מבוקרת של גורמים זרים (לקוחות הספק, עובדי הספק, גורמים זרים עוינים) **<u>השלכה:</u> גישה למידע רגיש עלולה לחשוף את הלמ"ס לאירוע דלף מהותי.**	על הספק לקבוע מנגנוני הזדהות חזקים בגישה למידע (מכל סוג) שלא מחצרות הלמ"ס וכן בגישה לממשקי ניהול. על הספק שליחת התראות בגישה לממשקי לגורם בקרה (ניהולי ומוקד הניטור SOC בלמ"ס).
דלף מידע – ע"י עובד הלמ"ס בערוצי	**גבוהה**	עובדי הלמ"ס ישיבו מידע על שאילתות שיתקבלו באמצעות ה- CRM. העברת מידע רגיש לשאילתות בשוגג או במכוון	מערכת ה- CRM נדרשת לתמוך ביכולת חיבור טכנולוגית אפליקטיבית למערכות צד ג' למניעת דלף מידע וכן על ממשקים לערוצי תקשורת

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

התקשורת השונים (דוא"ל, צ'אט ומדיה חברתית).		(התחזות לאזרח והטעית העובד, סחיטת עובד, פישינג, עובד ממורמר). **<u>השלכה:</u> גישה למידע רגיש עלולה לחשוף את הלמ"ס לאירוע דלף מהותי. בנוסף פגיעה ברמת האמינות של הלמ"ס וחשיפה לתביעות סעדים בפרסום מידע אישי.**	חיצוניים מבוססי API שבהם יעשה שימוש במערכת ה- CRM. הספק יפרט את המערכות הנתמכות לנושא זה.

4.4. סיכוני זמינות

במחשוב ענן זמינות המידע תלויה במספר גורמים וישנם מספר תרחישים אשר יכולים לגרום לאובדן זמינות השירות. הערכת הסיכונים צריכה לכלול התייחסות לתרחישים אלו והשפעתם על הרציפות התפקודית של הלמ"ס :

האיום	השפעה	פירוט האיום והשלכתו	המענה הנדרש
מניעת שירות	**גבוהה**	מתקפת מניעת שירות, או שיבוש השירות תשפיע על מתן השירות לאזרחים ומבקשי מידע. כמו כן עלולה להשליך על מהימנות (אבטחת השירות) במקרה של מתקפה מכוונת שמטרה להביך את הלמ"ס או את ישראל.	הספק נדרש לספק מענה מפני מתקפות מניעת שירות פנימיים אשר יאפשרו המשכיות עסקית לשירות עבור השירותים הפנימיים של הלמ"ס המנוהלים במערכת. וכן הגנה מפני מתקפות מניעת שירות חיצוניות (DOS, DDOS). על הספק להפעיל אמצעי שרידות ברמת השירות SLA וכן המשכיות עסקית בשירותי הענן הטכנולוגיים המסופקים בפתרון כנדרש במכרז. הספק נדרש לתכנן פתרון המאפשר זמינות שירות גבוהה באמצעות תכנון זמני RPO/RTO ו- WRT על הספק להתייחס לכל הסיכונים המפורטים ולספק להם מענה טכנולוגי או עסקי (לרבות משפטי) מחייב.
מניעת שירות עסקי	**גבוהה**	המערכת מספקת שירותים פנימיים וחיצוניים ללמ"ס. מתקפת מניעת שירות תשבית את שירותי המערכת הן פנימית לעובדי הלמ"ס והן חיצונית לשירותים המנוהלים ב- CRM. ספק מחשוב הענן אינו יכול לאפשר זמינות למערכת כתוצאה מתקלה או התקפה למניעת שירות מוכוונת לספק הענן, DDOS). כתוצאה מכך ספק מחשוב הענן אינו עומד בעומסים או ב- SLA הנדרש למימוש המערכת של הלמ"ס .	הספק נדרש לתכנן פתרון המאפשר זמינות שירות גבוהה באמצעות תכנון זמני RPO/RTO ו- WRT על הספק להתייחס לכל הסיכונים המפורטים ולספק להם מענה טכנולוגי או עסקי (לרבות משפטי) מחייב.

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

		ספק הענן נאלץ להפסיק את השירות כתוצאה מצו בית משפט, הפרה של חוק/תקנות/החלטה עסקית/ פיננסית/ פשיטת רגל/ הפסקת פעילות וכיוצ"ב. **<u>השלכה:</u> עצירת השירות.**	
חדירת קוד עוין בשאילתא או בקובץ המועבר דרך ה- CRM	**גבוהה**	קוד עוין דוגמת כופרה, אשר יצפין או יעמיס את מערכת ה- CRM עד כדי מניעת שירות. **<u>השלכה:</u> עצירת השירות.**	הספק נדרש ליישם אמצעים מתקדמים לניטור קוד עוין והגנה מפני מידע זדוני בכל שרתי ושירותי המערכת (דוגמת EDR או אנטי וירוס מתקדם המכיל מספר מודולי הגנה: HIPS, Antivirus, Antimalware, AntiSpyWare ו- Reputation).

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

4.5. סיכוני אמינות

ספקי שירותי מחשוב הענן אינם חסינים לאובדן או שיבוש המידע כתוצאה מתקלה או מפריצה למערכת. ככלל, יש לבחון את האיום של אובדן מידע או שיבוש תחת התרחישים הבאים:

האיום	השפעה	פירוט האיום והשלכתו	המענה הנדרש
אובדן ושיבוש מידע – כתוצאה מכשל/תקלה	**גבוהה**	אובדן או שיבוש המידע כתוצאה מתקלה אצל ספק מחשוב הענן, לרבות הרס פיזי של תשתיות מחשוב. בין המידע שעלול להיפגע: מידע תפעולי כללי, מידע עסקי, תיעוד פעולות (אישור בקשות שירות/מידע), לוגים וניטור מידע תפעולי או של מערכות הגנת הסייבר **<u>השלכה:</u> מניעת יכולת תחקור לאירוע סייבר.**	הספק נדרש לבצע תהליכי גיבוי מידע במחזוריות גבוהה להקטנת אובדן מידע. הספק נדרש להפעיל אמצעים לאיתור שיבוש מידע. הספק נדרש להפעיל אמצעי שחזור מידע בכל בשירותי הענן הטכנולוגיים (IAAS, SAAS, PAAS) אשר יש להן או עלולות להיות להן השלכות על אופן אחזור המידע של הלמ"ס.
אובדן ושיבוש מידע – כתוצאה מאירוע סייבר	**גבוהה**	אובדן או שיבוש המידע עקב התקפה שחדרה לסביבת מחשוב הענן. יש לזכור כי במחשוב ענן הניהול המרכזי והיכולת לשלוט במגוון רכיבים ממיקום יחיד מגדילים את היכולת לפגוע בכלל המידע והרכיבים. **<u>השלכה:</u> אובדן מידע בתהליכי העבודה.**	הספק נדרש לבצע תהליכי גיבוי מידע במחזוריות גבוהה להקטנת אובדן מידע. הספק נדרש להפעיל אמצעים לאיתור שיבוש מידע. הספק נדרש להפעיל אמצעי שחזור מידע בכל בשירותי הענן הטכנולוגיים (IAAS, SAAS, PAAS) אשר יש להן או עלולות להיות להן השלכות על אופן אחזור המידע של הלמ"ס.
אובדן מידע כתוצאה מהפסקת השירות	**גבוהה**	ספק הענן מפסיק את השירות ולפיכך המידע המוחזק על ידו אינו נגיש עוד ללמ"ס. **<u>השלכה:</u> אובדן מידע בתהליכי העבודה ותיעוד.**	הספק מחויב בהשבה מלאה של המידע כך שיאפשר שימוש (עריכה) וצפייה ויוכל להיקלט למערכות מידע סטנדרטיות.
מסירת מידע לגורם מתחזה	**גבוהה**	מבקשי מידע וגורמים רבים יוכלו לפנות ללמ"ס במגוון ערוצי התקשורת. החשש כי גורם מתחזה יפנה ללמ"ס לצורך קבלת מידע על מבקשי מידע בפעמים בודדו או רבות **<u>השלכות:</u> סיכוני הנדסה חברתית (התחזות למבקש מידע), חשיפת פרטים רגישים, הונאת עובדי הלמ"ס, זליגת מידע.**	מערכת ה- CRM נדרשת לתמוך ביכולת חיבור טכנולוגית אפליקטיבית למערכות צד ג' למניעת דלף מידע וכן על ממשקים לערוצי תקשורת חיצוניים מבוססי API שבהם יעשה שימוש במערכת ה- CRM. הספק יפרט את המערכות הנתמכות לנושא זה.
התחזות לשירותי הלמ"ס	**גבוהה**	הקמת ערוצי תקשורת מתחזים ללמ"ס במטרה להטעות את הציבור למסירת מידע רגיש דוגמת: עמוד מתחזה ברשת חברתית	הספק נדרש בקיומם של שירותי מודיעין לאיתור מתחזים בכל ערוצי התקשורת לרבות מדיה חברתית.

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

		(דוגמת פייסבוק), מסר טלפון המפנה לאפליקציית WhatsApp זדונית, הפניה לדוא"ל זדוני וכיו"ב. **<u>השלכה:</u>** **הונאת אזרחים (מסירת מידע, קבלת נתונים שגויים (בזדון או בשגגה), אישור לביצוע פעולה, התכחשות לביצוע פעולה.** **חדירה למחשב האזרח (גניבת מידע, גרימת נזק תוך פגיעה בשלמות הנתונים ובאמינותם).**	הספק נדרש לקיים אמצעים לאיתור ולמניעת Defacement לשירותי ה- CRM הציבוריים בענן וכן באמצעים אשר ימנעו התחזות (לדוגמה באפליקציית מובייל יוטמעו כלים למניעת Obfuscation – הקמת אפליקציה זדונית מתחזה). הספק נדרש לעשות שימוש רק בערוצי תקשורת חיצוניים מנוהלים על ידו או על ידי הלמ"ס (שירותי דיוור, תקשורת On-Line : משלוח מסרונים SMS , משלוח דוא"ל , תקשורת באמצעות WhatsApp Web ובאמצעות Chat Bot וכיו"ב). הספק נדרש לקיים תהליכים להגברת המודעות למבקשי מידע המבצעים שימוש בערוצי התקשורת של הלמ"ס, לדוגמה באמצעות פרסום ההנחיות בדף נחיתה. הפרסום יתבצע בכל ערוץ כזה.

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

4.6. סיכוני סייבר בשרשרת האספקה (ערוצי תקשורת חיצוניים)

ספקי שירותי מחשוב הענן הינם לרוב ספקים בינלאומיים הכפופים להוראות חוק, רגולציה והנחיות של גופים עסקיים גדולים מאוד אשר ללמ"ס אין שליטה עליהם. כפועל יוצא ללמ"ס אין יכולת בקרה ואכיפה משמעותית עבורם. ולפיכך נתאר את הסיכונים הבאים:

האיום	השפעה	פירוט האיום והשלכתו	המענה הנדרש
חוסר שיתוף פעולה של ספק הענן בעת אירועי סייבר	**גבוהה**	בעת אירוע סייבר או אירוע אשר יצריך מעורבות ושיתוף פעולה של ספק הענן. קיים חשש כי עיכוב ו/או אי מסירת מידע קריטי ללמ"ס יפגום באיכות, מהירות ואפקטיביות הטיפול באירוע. כמו כן קיים חשש כי גוף עסקי אחר או מדינה בה מאוחסנים שירותי הענן ימנעו את שיתוף הפעולה עם הלמ"ס או מי מטעמה (מערך הסייבר הלאומי, משטרת ישראל וכיו"ב). **<u>השלכה:</u> מניעת יכולת תחקור לאירוע סייבר.**	הספק מסכים ומצהיר כי כל שירותי הענן ושירותי הגיבויים אשר יסופקו על ידו (לרבות שירות תמיכה צד ג' ושימוש בקבלני משנה) יעשו בהתאם למפורט בסעיף 8.3 "מיקום גיאוגרפי ותחומי שיפוט" כאמור במסמך הנחיות ראש רשות התקשוב הממשלתי הנחיות היחידה להגנת הסייבר בממשלה – יה"ב (מספר הנחיה 5.5) ומודגש כי רק ממדינות מאושרות (לפי הנחיות של הרשות להגנת הפרטיות). הספק והספקים הפועלים באמצעותו (ספקי צד ג') מסכימים לשיתוף פעולה מלא בעת אירוע לצורך מסירת מידע אשר יכול להיות רלוונטי ללמ"ס או לגורמים מטעמה לרבות גופי ממשלה, משטרה, בטחון, מערך הסייבר הלאומי והיחידה להגנה בסייבר. הנ"ל רלוונטי גם בהיבטי סיום התקשרות ומחיקת מידע הצבור במערכות הספקים. שכן ללמ"ס אין יכולת בקרה אמיתית למחיקת מידע זה.
חטיפת חשבונות (Account or Session Hijacking	**גבוהה**	תרחיש הכולל חטיפת חשבון יכול לגרום התממשות איום זליגת המידע או אובדן המידע, במקביל לסיכונים נוספים. **<u>השלכה:</u>** **פגיעה במוניטין, פגיעה בזמינות פגיעה כלכלית או פגיעה בצד ג' או אדם פרטי וחשיפה לתביעות.**	על הספק המציע ליישם פתרון המספק מענה הולם לסיכון כחלק ממכלול הפתרונות המוצעים בשירות ה- CRM המשולב.
תקיפה וניצול חולשות בממשקי ניהול ו- API	**גבוהה**	טכנולוגיות ענן כוללות לרוב מגוון רב של ממשקי ניהול המתאפיינים במגוון יכולות רחבות ממיקום מרכזי אחד, בדגש על שכבת API[4] המאפשרת מגוון יכולות ניהול וגישה למידע.	על הספק המציע ליישם פתרון המספק מענה הולם לסיכון כחלק ממכלול הפתרונות המוצעים בשירות ה- CRM המשולב.

[4] Interface Programming Application

		<u>השלכה:</u> **אי הגנה על ממשקים אלה עשויה לגרום להתממשות סיכונים כגון חטיפת חשבונות וזליגת מידע ושיבוש נתונים.**

5. הנחיות אבטחת מידע בתהליכי התקשרות עם הספק

5.1. כתב הסכמה

5.1.1. יובהר לספק כי בעת יישום המערכת יועברו לספק המבצע הנחיות נוספות. ככל שיועברו הנחיות נוספות, יידרש הספק המציע לפעול ביחד עם הלמ"ס למציאת הפתרון היעיל והמאובטח ליישומן.

5.1.2. על מסמך הנחיות אבטחת המידע יחתום בנוסף, ממונה אבטחת המידע ו/או ממונה הגנת הסייבר מטעם הספק המציע. בחתימתו הוא מאשר הסכמתו ליישום ועמידה בהנחיות אבטחת המידע והגנת הסייבר המפורטות במסמך זה.

5.2. אישור ועדת הענן הממשלתית ומערך הסייבר הלאומי

5.2.1. הספק מודע כי הפתרון המוצע על ידו מצריך אישור ועדת הענן הממשלתית ומערך הסייבר הלאומי אשר יכולים למנוע מימוש הפתרון במידה ולא יינתן מענה להנחיותיהם – הן בטרם הפעלת השירות (כתנאי מנדטורי מתלה) והן במהלך מתן השירות (כתנאי מנדטורי מפסיק).

5.3. עמידה בהנחיות רשות התקשוב הממשלתי

5.3.1. הספק יעמוד **<u>באופן מלא</u>** בכל ההנחיות המפורטות במסמך "הנחיות ראש רשות התקשוב הממשלתי הנחיות היחידה להגנת הסייבר בממשלה – יה"ב מספר תקנה 5.5. הנחיה זו תצורף כנספח למכרז כחלק בלתי נפרד ממנו.

5.3.2. במהלך כל תקופת ההתקשרות, חלה חובה על הספק לדווח על כל חריגה מהנחיות אלה.

5.4. תקינה והוראות חוק

5.4.1. במידה והמידע המועבר לסביבות הענן מכיל נתונים הכפופים לחקיקה, תקינה או הנחיות אחרות –באחריות הספק להמציא מסמכים המעידים על עמידתו בדרישות וכי אינו כפוף לחוקים ו\או רגולציה אשר יהוו מכשול בהספקת כלל השירותים הנדרשים ע"י המשרד הממשלתי.

5.4.2. ספקי השירות מחויבים בעמידה בתקינה בינלאומית מוכרת ומקובלת ובין היתר: תקני ISO 27001, ISO 27017, ISO 27018, SOC 2 וכן בעל תאימות ל- GDPR (או תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017) במלואן. הספקים ידרשו להעביר אסמכתאות לעמידה בתקנים אלה.

5.5. מתן שירות ממדינות מאושרות

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

5.5.1. הספק מסכים ומצהיר כי כל **שירותי הענן ושירותי הגיבויים** אשר יסופקו על ידו (לרבות שירות תמיכה צד ג' ושימוש בקבלני משנה) יעשו בהתאם למפורט בסעיף 8.3 "מיקום גיאוגרפי ותחומי שיפוט" כאמור במסמך הנחיות ראש רשות התקשוב הממשלתי הנחיות היחידה להגנת הסייבר בממשלה – יה"ב (מספר הנחיה 5.5) ומודגש כי רק ממדינות מאושרות (לפי הנחיות של הרשות להגנת הפרטיות).

5.5.2. לא יעשה שימוש בשירותי ענן המאוחסנים או מנוהלים ממדיניות העוינות לישראל או ממדינות אשר לישראל אין קשרים דיפלומטיים עימן.

5.5.3. הספק לא יחזיק או יעביר מידע **<u>של הלמ"ס</u>** אל ו/בשירותי ענן זרים אחרים.

5.6. המשכיות עסקית

5.6.1. מנהלת הפרויקט בלמ"ס תבחן את התחייבות ספק מחשוב הענן לזמינות האתרים הגאוגרפיים וקביעת מתן SLA מתאים בשלב התקשרות החוזה מולו עפ"י ערכי RPO ו- RTO, WRT ו- MTD של מערכות המידע בארגון, בהתאם למדיניות הענן ולמדיניות ההמשכיות העסקית של הלמ"ס.

5.7. קבלני משנה

5.7.1. הלמ"ס רואה בקבלני משנה של הספק, כזרוע נוספת מטעם הספק. לפיכך יחולו כל החובות וההנחיות המכרז גם על קבלנים וספקי משנה של הספק.

5.7.2. הספק יישא באחריות ישירה לכל פער או סיכון הנובע משימוש בקבלני משנה.

5.7.3. הספק יעביר ללמ"ס את רשימת כל הספקים וספקי המשנה עימם הספק מתכנן לעבוד במסגרת הפעילות או שיש להם קשר ישיר לתפעול ותחזוקת מערכות הענן של הלמ"ס.

5.7.4. ככל שישנו שימוש בקבלני משנה, אלה יאושרו על ידי הלמ"ס ובין היתר על ידי אגף הגנת הסייבר בלמ"ס, לרבות החתמה על טופסי שמירת הסודיות (NDA) כפי המקובל בלמ"ס.

5.7.5. הספק יעדכן את הלמ"ס על כל גישה של קבלן משנה (שאינו הספק הישיר, לדוגמא ספקי תחזוקה) בגישה או ביכולת אפשרית לגישה למידע של הלמ"ס.

5.7.6. הספק יקיים מנגנון בקרת גישה פיזית ולוגית של קבלני משנה, למידע של הלמ"ס למידע כאמור הנמצא במערכות של הספק.

5.7.7. ראש אגף הגנת הסייבר בלמ"ס יהיה הגורם שיאשר מראש כל גישת קבלן משנה למידע של הלמ"ס (פיזי או לוגי) וכן כל מעורבות של קבלן משנה אשר יהא מעורב בפרויקט. האישור יינתן לפני התקשרות עם הספק ו/או קבלן המשנה.

5.7.8. לא תתקיים לגישה למידע של הלמ"ס בגישה של ספקים צד ג' ללא אישור בכתב של הלמ"ס.

5.8. גיוס עובדים לפרויקט

5.8.1. אין באישור הלמ"ס להעסקת עובד כלשהו כדי לפטור את הספק הזוכה ו/או המפעיל את שירותי ה- CRM מאחריותו לפי הסכם זה או לפי כל דין , ואין בכך מניעה מהלמ"ס לדרוש החלפת עובד כל שהוא, כולל עובדי קבלני המשנה.

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

5.8.2. הספק הזוכה ו/או המפעיל את שירותי ה- CRM יהיה אחראי כלפי הלמ"ס על כל פעילות עובדיו ו/או מי מטעמו במסגרת ההתקשרות.

5.8.3. הספק הזוכה ו/או המפעיל את שירותי ה- CRM 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.

5.9. סקרי בטיחות על ידי הספק

5.9.1. האמור לעיל, לא פוטר את הספק מביצוע בדיקות מתודיות וטכנולוגיות בחצרותיו ובמערכות המסופקות על ידו.

5.9.2. הספק יבצע בדיקת שפיות, בדיקת חדירות ובדיקת חולשות ייעודיות ליישום בענן בהתאם למורכבות המערכת ומאפייניה.

5.9.3. הספק יערוך בדיקת אבטחת מידע מקיפה לבחינת הפתרון המוצע. במסגרת התהליך, יתבצעו בדיקות עמידות וחוסן לפתרון המוצע, בתהליכי בדיקות ובסביבות הייצור וכן לרכיבים שעליה מותקן היישום.

5.9.4. ככל שיתגלו ליקויים, הספק מתחייב לטפל בכל הליקויים שימצאו במסגרת בדיקות אלה בתוך זמן סביר.

5.10. טיפול באירועי אבטחת מידע וסייבר במהלך מתן השירות

5.10.1. על הספק להציג ללמ"ס מוכנות לטיפול באירועי אבטחת מידע (Incident Response), בין השאר בקיומם של מסמכי מדיניות ונהלים לטיפול באירועים.

5.10.2. הספק ימנה נציג שיהיה אחראי על טיפול באירועי אבטחת מידע .

5.10.3. הספק נדרש לדווח באופן מידי ללמ"ס במקרה של אירוע או חשש לאירוע אבטחת המידע מכל סוג לרבות, דליפת מידע או שימוש חורג מההרשאה שניתנה לזוכה. הדיווח יעשה בכתב ובטלפון עד 24 שעות מרגע זיהוי האירוע.

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

5.10.5. במקרה של אירוע אבטחת מידע, על הספק הזוכה ו/או המפעיל את שירותי ה- CRM ו/או קבלן המשנה לפעול למניעת דליפת המידע וכל נזק כתוצאה מהתקלה.

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

5.10.7. הספק יפעיל אמצעים למניעת הכחשה וכי כל פעילות המשתמשים מטעמו תנוטר באופן שיהיה ניתן לאתר את המשתמש שגרם ו/או שמעשה ו/או מחדל שלו גרמו ו/או אפשרו את האירוע.

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

5.11. רישום הרישוי

5.11.1. רישוי שירות ה- CRM ירשם על שם הלמ"ס.

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

5.12. סיום התקשרות עם ספקים

5.12.1. במידה ויעלה צורך בסיום ההתקשרות והפסקת השירות, יאפשר הספק לעבור לספק אחר תוך העברת נתוניו הרלבנטיים ממערכות הספק בתוך חצי שנה, מחיקתם ממערכות הספק והתחייבות הספק למחיקה באופן מלא ומקיף ביותר של המידע, מול תאימות לתקנים בינלאומיים מקובלים.

5.12.2. בעת סיום התקשרות עם ספק, באחריות הספק הזוכה ו/או המפעיל את שירותי הענן וה- CRM לחסום ולהסיר את הרשאות הגישה אשר נפתחו לספק, לעובדיו במערכות המחזיקות מידע של הלמ"ס.

5.12.3. באחריות הספק הזוכה ו/או המפעיל את שירותי הענן ושירות ה- CRM להשיב כל מידע שנמסר להם לרבות מידע לוגי, פיזי, התקן מחשוב, התקן תקשורת, מודם סלולרי, התקן אימות זיהוי וכדומה.

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

6. הנחיות רכש טכנולוגי

6.1. רכש טכנולוגיות

6.1.1. למערכת ה- CRM המוצעת יהא אופק תחזוקה (Support) ועדכונים (Life Cycle) לרבות עדכוני חתימות ואבטחת מידע (Patch, Service packs) של לפחות 3 שנים מיום ההטמעה המתוכנן.

7. פתרון משולב למערכת CRM

7.1. גישה לשירותי ניהול השירות

7.1.1. הגישה לשירותי הניהול בענן תתאפשר רק מרשת הספק ומרשתות הלמ"ס מרשת ישראל.

7.2. ניהול תעודות אבטחה עבור ממשקים חיצוניים

7.2.1. עבור כל כתובת חיצונית החשופה לאינטרנט וכן בכל ממשק תקשורת לשירות חיצוני, יעשה שימוש בתעודות אבטחה שירכשו לצורך כך.

7.3. ניהול תעודות אבטחה עבור ממשקים פנימיים

7.3.1. בין שרתים ושירותים אפליקטיביים פנימיים בשירותי הענן (דוגמת ממשקי API) יוגדרו תעודות אבטחה. תעודות אלה יוכלו להיות מונפקות באמצעות שירות חיצוני (הספק ירכוש תעודות) או פנימי (HSM/CA)

7.3.2. ניהול מפתחות ההצפנה יעשה בשרת HSM של ספק שירותי הענן ספק הענן יגן על מפתחות ההצפנה של הלמ"ס ויפעל למניעת דלף או גישה של גורם לא מורשה (גם מחצרות הספק)

7.4. אבטחת ממשקי ניהול

7.4.1. תיושם הפרדת ממשק הניהול של כלל המערכות מממשקי השירות והאפליקציה.

7.4.2. בשירותי ענן, הגישה לממשק הניהול תתאפשר רק מרשתות ישראל ורק מכתובות ה- IP או עובדים פרטניים של הלמ"ס שאושרה להם גישה מרחוק לניהול.

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

7.4.3. גישה לממשק ניהול תעשה בפרוטוקולי ניהול מאובטחים ומוצפנים דוגמת Https.

7.4.4. ככלל בכל ממשק ניהול והעברת מידע, יעשה שימוש בפרוטוקולים מאובטחים ומוצפנים ובעלי מפתחות ההצפנה ארוכים.

7.4.5. במקרים בהם יהא צורך בפענוח הפרוטוקולים לצורך ניטור התעבורה באמצעי אבטחת המידע, יבחנו שיטות לניהול המפתחות במערכות הניטור או יישום טרמינציה לפרוטוקול (לדוגמה: SSL Termination).

7.4.6. הגישה לממשק הניהול של המערכות יתאפשר באמצעות ניהול משתמשים וקבוצות משתמשים על פי קבוצות הרשאה (קריאה בלבד, עריכה חלקית, עריכה מלאה).

7.4.7. אימות משתמשי הניהול יעשה מול שרת ניהול זהויות דוגמת: Active Directory (ADFS).

7.4.8. הזדהות משתמש תוך מתן הזדהות חזקה 2FA או MFA.

7.4.9. כל פעולות הניהול יתועדו במלואן, בין אם הסתיימו בהצלחה או בכישלון.

7.4.10. התראות על גישה לממשקי הניהול יועברו בערוץ מוצפן למערכת ה- SIEM של הלמ"ס. במידה ולא ניתן, יעמיד הספק שירות SIEM עצמי לניטור מערכות הענן ויאפשר למוקד ה- SOC של הלמ"ס גישה לניהול ועדכון החוקה.

8. המשכיות עסקית

8.1. נהלים ומדיניות

8.1.1. הספק יקיים נהלים ומדיניות המשכיות עסקית ושמירה על זמינות השירותים הניתנים ללמ"ס במסגרת פרויקט זה.

8.2. שרידות והמשכיות עסקית

8.2.1. כלל המערכות בסביבת הפתרון יוגדרו כתשתית המחייבת שרידות ויתירות מלאה בתצורת high-Availability או Active-Active , הזמינות תוגדר כ 99.5%.

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

8.2.3. יעשה שימוש בכלים להבטחת זמינות הנתונים של מידע שהוגדר כחיוני בתהליך הערכת הסיכונים למערכות המידע בסביבת ה- CRM.

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

8.3. תמיכה באתר ה- DR

8.3.1. הלמ"ס מתכננת להקים אתר DR. הפתרון המוצע יידרש להתממשק לאתר ה- DR באמצעות הקמת ערוץ תקשורת מאובטח מול אתר ה- DR.

8.4. גיבויים

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

8.4.1. כל מערכות תשתית ואבטחת מידע לרבות חומרה, תוכנה והנתונים השמורים במערכות המחשוב יגובו לאמצעים נפרדים מהציוד בו הם נמצאים באופן מסודר.

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

8.4.3. אחת לשבוע יועברו קבצי הגיבוי וקבצי הלוג לגיבוי בחצרות הלמ"ס.

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

8.5. אחסון הגיבוי

8.5.1. הספק יוודא אחסון של המידע בתצורה בטוחה ויוודא ניהול הרשאות קפדני רק לעובדים אשר אושרו על ידי הלמ"ס בגישה למידע.

8.6. שחזור ובדיקת תקינות הגיבויים

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

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

9. הנחיות אבטחה – מערכות ושירותי הגנה בענן

**הנחיות אלה תיושמנה כחלק מהפתרון המוצע על ידי הספק בשירות הענן המנוהל על ידו.

9.1. מניעת גישה ממדינות זרות

9.1.1. הספק ימנע גישה לשירותי ה- CRM של הלמ"ס ממדינות עוינות.

9.2. מערכות הגנה בענן

9.2.1. הספק מסכים ומתחייב להפעיל מנגנוני ניטור לאבטחת מידע בין הסביבות בהתאם לצורכי הלמ"ס ובכל ממשק רלוונטי, בין היתר:

9.2.1.1. WAF להגנה על ממשקים אפליקטיביים ושירותי אינטרנט.

9.2.1.2. מערכות IPS.

9.2.1.3. שירותי למניעת מתקפות מניעת שירות DoS ו- DDoS.

9.2.1.4. אמצעים לאיתור אנומליה והטעיה (דוגמת מלכודות דבש). הספק יישם מערכת לזיהוי והטעיה (Honey Pot) בסביבות הרשת החשופות למבקשי מידע ובסביבות פנימיות שלו.

9.2.2. הספק יפעיל ניטור גם ממשקים מוצפנים (באמצעות פתיחת ההצפנה וניטור התוכן) לכלל הפרוטוקולים לרבות פרוטוקולים מוצפנים (הפעלת יכולת SSL Decryption).

9.2.3. הספק יעשה שימוש בשתי מערכות נפרדות עבור ממשקים חיצוניים (החשופים לאינטרנט) ופנימיים (החשופים ללמ"ס ולמערכות ה- CRM).

9.2.4. המערכות תמוקמנה באופן המאפשר ניטור לכל תעבורת המידע בין כלל הממשקים והערוצים.

9.2.5. המערכות תוגדרנה באופן המשלב הגדרות Whitelist, Backlist וכן בשילוב חתימות (ככל הניתן ובאופן האפקטיבי ביותר).

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

9.2.6. המערכות הדרושות בעדכוני חתימות תתעדכן בחתימות בתדירות גבוהה מספר פעמים ביום, בהתאם לעדכוני היצרן.

9.2.7. המערכות תופעלה עם יכולות Load Balance להתמודדות עם מתקפות עומס ומתקפות אפליקטיביות.

9.2.8. בעת כשל תפעולי, תאפשר המשכיות תקשורתית באמצעות Failover Bypass. בהינתן מקרה כזה, תשלח הודעה למוקד הניטור של הלמ"ס לצורך בחינת משמעויות הגנת סייבר וכן לדיווח ראש אגף הגנת הסייבר בלמ"ס לצורך בחינת הסיכון והמשכיות השירות בגישה לעדכון נתונים ללא יכולת ההגנה.

9.3. הגנה על בסיסי נתונים

9.3.1. הספק יגן על מערכות Data Base באמצעות טכנולוגיות ותהליכי הקשחה. ב באמצעות פתרון ייעודי, מוצר מדף או שילוב אחר. ובתנאי שימלא אחר כל הנחיות המובאות בסעיף זה.

9.3.2. תשאול בסיס הנתונים יעשה דרך רכיב ההגנה ויספק ניטור מלא על תוכן התשאול, מהותה, מידע טכנולוגי, חשבון משתמש , מועד וכיו"ב.

9.3.3. פתרונות ההגנה על שרתי database ימוקמו בין שרתי האפליקציה לשרתי ה-Database לאיתור פעילות ושאילתות חריגות.

9.3.4. הרכיב ימוקם כך שהוא רואה את כל הרשתות האפליקטיביות והגישות לבסיסי המידע ומגן עליהם מפני איומים בשכבת האפליקציה.

9.3.5. הספק ישלב בקרות המשלבות הגדרות Whitelist, Backlist וכן בשילוב חתימות.

9.3.6. במידה ויעשה שימוש במערכת המבוססת חתימות, המערכת תתעדכן בחתימות בתדירות גבוהה מספר פעמים ביום, בהתאם לעדכוני היצרן.

9.3.7. יש להפעיל יכולת לזיהוי אירועים על פי קריטריונים מובנים וחתימות יצרן.

9.3.8. יש להפעיל יכולת אקטיבית לזהות ולחסום מתקפות ידועות למשל: SQL Injection.

9.3.9. יש להפעיל יכולת לזיהוי אירועים על פי קריטריונים מותאמים (Custom Rules) אישית ללמ"ס בהתאם להערכת הסיכונים (עבור סיכוני סודיות, אמינות, זמינות וסיכוני סייבר) באמצעות חוקים ושילוב חוקים שיכתבו במיוחד. להלן התראות שיתבקשו להתקבל מהמערכת:

9.3.9.1. Unsuccessful login/successful login בכל אחד מבסיסי הנתונים.

9.3.9.2. מועד התנתקות (Logoff) שמתבצע בכל אחד מבסיסי הנתונים

9.3.9.3. המערכת תתריע בכל שינוי בהרשאות משתמש, יצירת משתמשים חדשים ויצירת משתמשים ניהוליים.

9.3.9.3.1. ניטור שינויים:

9.3.9.3.2. שינויים שנעשו בטבלאות רגישות.

9.3.9.3.3. שינויים שנעשו בשרת ה- Database שלא דרך האפליקציה (בכל רמת הרשאה).

9.3.9.3.4. שינויים שנעשו ישירות בשרת ה- Database או בטבלאות בהרשאות מקומיות או ניהוליות.

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

9.3.9.3.5. המערכת תציג את הערכים לפני ואחרי השינוי.

9.3.9.3.6. זיהויי חיבור Administrator מ- IP שונה ממה שאושר לו להתחבר.

9.3.9.3.7. זיהוי חיבור מאפליקציות לא מאושרות.

9.3.9.3.8. זיהויי שימוש בימים ושעות שהוחרגו.

9.3.9.3.9. שמירה ותיעוד כל הנתונים המתקבלים.

9.3.10. תיעוד

9.3.10.1. תמנע יכולת שינוי או מחיקה של התראות, על ידי גורם ניהולי (משתמש ניהולי ב- database)

10. הגנה בתהליכי שמירה, העברה והוצאת מידע

פרק זה מתבסס בין היתר על סעיפים 8.4, 8.5, 8.6 במסמך ההנחיה של היחידה להגנת הסייבר בממשלה – יה"ב (מספר הנחיה 5.5).

10.1. ממשקי תקשורת

10.1.1. הספק יקים ממשק תקשורת מאובטח בין ספק שירותי הענן לרשת הלמ"ס.

10.1.2. הספק יוודא כי ממשקי התקשורת בין ספק שירותי הענן למשתמשי הקצה יהיו מאובטחים.

10.1.3. הספק יקים ממשקי תקשורת מאובטחים בתוך סביבת הענן (בין שרתים או שירותים) המנוהלים על ידו.

10.2. מסירת מידע לספק

10.2.1. העברת מידע (עסקי או תפעולי) בין הספק ללמ"ס תעשה באמצעות ממשק מאובטח אשר יכלול הזדהות בין המערכות של הלמ"ס ומערכות הספק וכן הצפנת תווך התקשורת.

10.3. אחסון מידע בחצרות הספק

10.3.1. הספק יקיים נהלים ומדיניות להגנה מפני דלף מידע ויציג אותם ללמ"ס על פי דרישתה מעת לעת.

10.3.2. הספק לא יאחסן מידע של הלמ"ס באמצעי מדיה נתיקה.

10.3.3. הספק לא יבצע כל פרסום של מידע הקשור ללמ"ס אלא אם ניתן אישור בכתב מראש אגף הגנת הסייבר בלמ"ס ו/או נקבע אחרת בהסכם ההתקשרות.

10.4. הגנה על המידע

10.4.1. על המידע של הלמ"ס להיות מוצפן בעת העברתו בתקשורת וכן כאשר הוא מאוחסן במערכת שאינה לשימושו הבלעדי של הלמ"ס.

10.5. הצפנת מידע במנוחה (אחסון)

10.5.1. הספק יצפין מידע מנוחה באמצעות מפתחות הצפנה.

10.5.2. ההצפנה תתבצע בכל השכבות הרלוונטיות לדוגמה: הצפנת גיבויים, הצפנה ברמת בסיס הנתונים או ברמת שכבת האחסון.

10.5.3. מפתחות ההצפנה למידע ישמרו בחצרות הלמ"ס או במיקום אחר על פי הנחיית ראש אגף הגנת הסייבר בלמ"ס.

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

10.6. הצפנת מידע בתנועה

10.6.1. הספק יעשה שימוש בפרוטוקולי הצפנה מאובטחים עדכניים (נכון לכתיבת הנחיות אלה Https TLS 1.2 או TLS 1.3) להצפנת מידע בתנועה וכן בכל אחד מהממשקים הבאים:

10.6.1.1. תקשורת בין ספק שירותי הענן לרשת המשרד.

10.6.1.2. תקשורת בין ספק שירותי הענן למשתמשי הקצה.

10.6.1.3. תקשורת בתוך סביבת הענן (בין שרתים או שירותים).

10.6.1.4. תקשורת בין סביבת הענן לבין שירותים או ממשקים חיצוניים אחרים (לדוגמה API למערכות צד שלישי, או בין מערכת הענן לשירותים חיצוניים).

10.6.1.5. ממשקי ניהול וממשקי תמיכה ושירות.

10.6.2. מפתחות ההצפנה למידע ישמרו בחצרות הלמ"ס או במיקום אחר על פי הנחיית ראש אגף הגנת הסייבר בלמ"ס.

10.7. התממת מידע

10.7.1. כחלופה לפתרונות ההצפנה, הספק יוכל להציע חלופות נוספות להצפנת המידע כגון מימוש טכנולוגיות .Anonymization או Tokenization, Masking. הלמ"ס אינה מתחייבת לעשות שימוש בפתרונות אלה כחלופה להצפנה.

10.8. חשיפת ממשקי הענן

10.8.1. הגישה לממשקי הניהול וממשקי העבודה של המערכת תתאפשר רק מכתובות הרשת החיצוניות של הלמ"ס.

10.8.2. ממשקים מול מערכות פנימיות של הלמ"ס (דוגמת דוא"ל, אתר אינטרנט, גישת עובדים) ייושמו מול רשתות הלמ"ס ובמקרים מסוימים יוגדר ממשק אפליקטיבי נפרד למשל באמצעות API.

10.8.3. הגישה לשירותי המערכת על ידי גורמים חיצוניים (דוגמת פנית אזרחים לקבלת מידע), תתבצע מול ממשק אפליקטיבי נפרד של המערכת או מול שירות חיצוני. גישה זו תתאפשר רק מכתובות הרשת של מדינת ישראל.

10.8.4. כל ממשק אחר יאושר על ידי ראש אגף הגנת הסייבר בלמ"ס.

10.9. הצפנת ממשקים בין ספק הענן ללמ"ס

10.9.1. ממשקי העבודה בין הלמ"ס לספק הענן, יתבצעו על גבי תשתית VPN Site to Site.

10.10. ניהול מפתחות הצפנה

10.10.1. הספק יאפשר ללמ"ס לנהל מפתחות הצפנה פרטיים (מפתח של הלמ"ס המנוהל בענן). לדוגמה: במערך HSM אשר ינוהל ויוחזק על ידי הלמ"ס.

10.10.2. הלמ"ס תדרג בציון מופחת (באופן מובהק) ספק ענן אשר ינהל באופן עצמאי את המפתחות.

10.11. חריגים להצפנה

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

10.11.1. במקרים בהם יש קושי להצפין את כל המידע כאמור, יש להצפין לפחות את הנתונים שסווגו על ידי הלמ"ס כרגישים ושיש בחשיפתם כדי לפגוע בלמ"ס במקרה כזה יש לבחון יישום המאפשר, ככל שניתן, לאחסן את מפתחות ההצפנה בחצרות הלמ"ס.

10.11.2. יש לעדכן את ראש אגף הגנת הסייבר בכל המקרים בהם לא תתאפשר הצפנה של מידע.

10.12. הגנה על מידע מפני שיבוש

10.12.1. הספק יפעיל מנגנוני הגנה על תשתיות הספק מפני סיכוני שיבוש מידע.

10.12.2. הספק יפעיל מנגנונים לאיתור שיבוש מידע (למשל כתוצאה מקוד עוין, או תקלה).

10.12.3. הספק יספק ללמ"ס כלי אחזור מידע לצורך בדיקות שוטפות לתקינות המידע המגובה.

11. הגנה בערוצי מסירת מידע

11.1. ניטור מידע רגיש

11.1.1. כאופציה לשיקול הלמ"ס, המערכת תתמוך בפתרונות מקובלים למניעת דלף מידע DLP) ואיתור מידע רגיש (מזהה פרט כגון תעודת זהות, מספר טלפון, כתובת דוא"ל) ומניעת דלף מידע רגיש בכל ערוצי התקשורת החיצוניים.

11.1.2. צורך הגדרת מידע רגיש נפנה לדוגמאות הבאות: תעודות זהות, מספרי טלפון, כתובות דוא"ל ועוד. דוגמאות לסוגי מידע רגיש ניתן למצוא בקישורים הבאים:

- https://cloud.google.com/dlp/docs/infotypes-reference#global
- https://cloud.google.com/dlp/docs/infotypes-reference#credentials_and_secrets
- https://cloud.google.com/dlp/docs/infotypes-reference.
- https://cloud.google.com/dlp/docs/infotypes-reference#israel

11.1.3. הספק יאפשר חסימת מידע רגיש או הסרתו מתכתובות בערוצי תקשורת חיצוניים (SMS, דוא"ל, Chat, Chat Bot וכיו"ב).

11.1.4. הספק ידע גם לזהות שינויים מניפולטיביים (זדוניים) במידע רגיש לצורך הסוואתו והוצאתו בערוצים אלה.

11.2. ניקוי והסרת מידע רגיש בשדרים יוצאים

11.2.1. כל מידע מזהה פרט של מבקשי מידע מהלמ"ס: רשת חברתית, טלפון, דוא"ל שיועבר בערוצי המידע) אשר יוסר ככל האפשר מבלי לפגוע בשירות.

11.2.2. הסרת המידע המזהה תתבצע באמצעי השחרת מידע או כלים ייעודיים לזיהוי מידע רגיש, ניקוי הקבצים (השחרה) ומניעת דלף מידע. הכלים ירכשו בהתאם לקריטריונים שיוגדרו למניעת דלף מידע מזוהה או רגיש. הכלים יאפשרו בקרה ועדכון אנושיים בכל אחד מהשלבים: זיהוי, השחרה ומניעת דלף מידע.

11.3. מניעת רישום מידע רגיש בערוץ חיצוני

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

11.3.1. הספק בשילוב עם הגורמים העסקיים ואגף הגנת הסייבר בלמ"ס יגדירו את הערוצים החיצוניים וסוגי המידע הדרושים להימצא בהם.

11.3.2. בערוצים שבהם יועבר מידע ציבורי אנונימי - ימנע רישום מידע רגיש המזהה פרט (תעודות זהות/טלפון וכדומה – גם אם יוזנו בשוגג, אין לשמור אותם במערכת ה-CRM בענן) על ידי מבקשי מידע חיצוניים בכל הערוצים שאינם מצריכים מענה אישי דוגמת:

11.3.2.1. קבלת מידע סטטיסטי.

11.3.2.2. פניות של ארגונים בינלאומיים, שאלוני ENP/אזוריים ופרסום בקשות חריגות.

11.4. **חריגים**

11.4.1. יוחרגו ערוצים חיצוניים בהם התהליך העסקי מצריך השבה אישית לטלפון או לדוא"ל ובתהליכים אחרים שיצריכו זאת. לדוגמה:

11.4.1.1. פניית ציבור אישית.

11.4.1.2. פניה אישית ליחידת סקרים.

11.4.2. בכל המקרים ההשבה תתבצע **<u>רק באותו ערוץ</u>** בה הועברה הבקשה למידע. לדוגמה:

11.4.2.1. בקשות שהוגשו באתר, יקבלו מזהה לתשובה באתר.

11.4.2.2. בקשות שהוגשו במדיה חברתית, יוחזרו לאותה מדיה חברתית ולאותו חשבון משתמש שהגיש את הבקשה.

11.4.2.3. בקשות שהוגשו באפליקציית מסרים -יועברו לאותו משתמש באפליקציית המסרים.

11.4.2.4. בקשות שהוגשו בדוא"ל יוחזרו לאותה כתובת.

12. הגנה בערוצי קבלת מידע

12.1. קבלת תכנים

12.1.1. הספק יפרסם בכל ערוצי המידע, שלא להזין מידע אישי רגיש, למשל באמצעות דף נחיתה או פתרון דומה לכך.

12.1.2. בכל ערוץ נכנס תתבצע הגבלת גודל המידע הנכנס, כמות התווים וסוגי התווים.

12.1.3. יש לבצע בדיקות קלט למניעת הכנסת קלט זדוני, על פי פרק הנחיות פיתוח מאובטח.

12.2. הכנסת מידע וקבצים

12.2.1. המערכת תתמוך בפתרונות מקובלים להלבנת קבצים, Sandbox והשטחת שדרים

12.2.2. הספק יפרט את המערכות הנתמכות לנושא זה.

13. ניהול משתמשים

13.1. עקרונות ניהול המשתמשים

13.1.1. ניהול המשתמשים במערכות הבאות תהא באחריות הלמ"ס:

13.1.1.1. מערכת ה- CRM.

13.1.1.2. Active Directory (ADFS) – על הספק לפרט את השיטה (לדוגמה: ביצוע מהלך Federation מתוך הלמ"ס או סנכרון OU למערכת ניהול המשתמשים של הספק בענן). והסנכרון יהיה מול OU נפרד.

13.2. ניהול הרשאות

13.2.1. ההרשאות למשתמשים אנושיים, מנהלים וחשבונות אפליקטיביים יינתנו על בסיס "פרופילי הרשאות", כאשר לכל בעל תפקיד או משתמש יוגדר פרופיל הרשאות מתאים.

13.2.2. הלמ"ס תוכל לבצע סקירת הרשאות בכל המערכות המסופקות לה במסגרת שירות הענן (CRM, ומערכת ניהול המשתמשים).

13.3. קבוצות משתמשים

13.3.1. על פי הערכתנו, המערכות תנהלנה את קבוצות המשתמשים הבאות:

13.3.1.1. מבקשי מידע חיצוניים/ציבור/ארגונים.

13.3.1.2. עובדי הלמ"ס במחלקות השונות.

13.3.1.3. משתמשי ניהול מערכת ה- CRM (הספק, משתמשים מטעם מע' מידע).

13.3.1.4. משתמשים אפליקטיביים לתהליכי ניהול פנימיים במערכת ה- CRM.

13.3.2. המערכת תתמוך בניהול בקבוצות משתמשים סוג או מחלקה עסקית ובין מחלקות עסקיות (בתהליכי חוצי מחלקות).

13.3.3. המערכת תתמוך בניהול קבוצות משתמשים אפליקטיביים וממוכנים .

13.4. **תמיכה בשירותי** Active Directory **(**ADFS**)**

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

13.4.1. ניהול משתמשי מערכת ה-CRM ומערכות נלוות אליה יעשה במערכת ניהול משתמשים ייעודית Active Directory . כלומר זיהוי אל מול המערכת יבוצע באמצעות חשבון משתמש אישי ייעודי בענן. מערכת זו תנהל רק את משתמשי הלמ"ס.

13.4.2. בנוסף יתאפשר ניהול משתמשים מקומי במערכת ה- CRM ובמערכות הנלוות אליה אשר יתמוך בכל התהליכים הבאים:

13.4.2.1. גישה לתמיכה בחירום.

13.4.2.2. ניהול חשבונות וקבוצות Accounting לצורך הזדהות עבור אוכלוסיות שונות: מנהלים, עובדים פנימיים, ניהול תחזוקה, משתמשים אפליקטיביים (לדוגמה עבור ה- Chat Bot) ותהליכיים (לדוגמה: הלבנה, השחרה, העברת מידע) וכיו"ב.

13.4.2.3. Authentication - ניהול משתמשים וסיסמאות מרכזי, אכיפת סיסמאות.

13.4.2.4. Access Permission/Authorization - ניהול הרשאות מבוסס קבוצות הרשאה לפי צרכי כלל המשתמשים.

13.4.2.5. Monitoring – ניטור הקשר בין המשתמשים למשאבים נדרשים ובין היתר אספקת מידע מהימן למערכות הניטור ולמוקדי הניטור (SIEM) והשו"ב (NOC) המפורטות בפרק "תיעוד ולוגים".

13.4.3. על המערכת לאפשר יישום מדיניות סיסמאות – אורך, מורכבות, נעילה, היסטוריה וכו' בהתאמה לאמור בסעיף ניהול סיסמאות במסמך זה.

13.5. **תמיכה בשירותי** SSO **בשירותי הענן**

13.5.1. המערכת תתמוך בסנכרון וניהול סיסמאות בין המערכות השונות המעורבות בפרויקט לרבות תמיכה בסנכרון סיסמאות מובנות או חיצוניות.

13.5.2. הפתרון יתמוך בתהליכים שאינם דורשים הזדהות חוזרת, אלא חד פעמית Single Sign On, ובתנאי שהזדהות זו מספקת ועונה על הנחיות המופיעות במסמך זה.

14. ניהול מבקשי מידע

14.1. גישה לממשקי מידע/שירות

14.1.1. גישה לממשקי מידע/שירות חיצוניים של משתמשים חיצוניים, ארגונים או מזדמנים תעשה מול ערוץ המידע החשוף להם, כגון: אתר האינטרנט, דוא"ל וכיו"ב.

14.1.2. משתמשים אלה לא ייגשו באופן ישיר למערכות הענן.

14.2. הגנה על ממשקי מידע/שירות

14.2.1. הספק יישם את ההגנות הבאות על כל ממשקי המידע/שירות:

14.2.1.1. הצפנה של תווך התעבורה.

14.2.1.2. שילוב אמצעי זיהוי בין הצדדים.

14.2.1.3. יישום מנגנון לניהול הרשאות.

14.2.1.4. תיעוד מלא ובקרה של בקשות ומעבר המידע.

14.3. ניהול משתמשים

14.3.1. עבור תהליכים לקבלת מידע כללי, אין צורך בתהליך הזדהות.

14.3.2. עבור תהליכים בהם נדרש לשמור על רציפות במסירת מידע. על הספק ליישם הליכי זיהוי נאותים <u>חד ערכיים</u>, למבקשי מידע באמצעות פתרונות 2FA או MFA במטרה להבטיח שלמות התהליכים, מסירת המידע רק עבור אותם גורמים שפנו לקבלת המידע ומניעת התחזות או שליפת מידע באמצעות מתקפת ניחוש משתמשים.

15. ניהול מנהלנים ושירות מוקד Helpdesk מטעם הלמ"ס והספק

15.1. גישה לממשקי ניהול

15.1.1. גישה לממשקי ניהול ופיתוח תתאפשר מחצרות הלמ"ס או חצרות הספק בלבד.

15.1.2. לא תתאפשר גישה לממשקי ניהול מסביבות מרשתות פרטיות (ביתיות), ציבוריות או אלחוטיות.

15.1.3. במקרים חריגים או בתקלות משביתות, ישקול ראש אגף הגנת הסייבר בלמ"ס מתן גישה מרחוק ויעביר מסמך הנחיות פרטניות לספק אשר יתייחס לנושאי גישה מאובטחת מרחוק לצורך זיהוי חד ערכי של עמדות המחשוב מהן מתבצעת הגישה מרחוק וזיכויין (Host Check), זיהוי חד ערכי של משתמשי הגישה מרחוק, הגנה על ממשקי גישה מרחוק, ניהול משתמשים, התקנים ותעודות אבטחה, אמצעי חציצה (Proxy, terminal), אמצעי הלבנה השחרה והפצת עדכונים, ניהול הרשאות, תיעוד והקלטת פעולות, הגבלת שעות הפעילות וניטור חריגים, ניטור הגנה בסייבר ונושאים נוספים.

15.1.4. אימות משתמשים תתבצע באמצעות אמצעי חד ערכי ייעודי עבור כל משתמש.

15.1.5. אימות יעשה באמצעות שם משתמש אישי וכן שימוש באמצעי זיהוי חזק (2Factor Authentication ו/אוMFA וכיו"ב).

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

15.1.6. ניהול משתמשים וקבוצות משתמשים למול מערכות בתוך סביבת הספק תעשה בשירותי Active Directory או מערכת ניהול זהויות אחרת אשר תמצא בלמ"ס ותעדכן את מערכות ניהול המשתמשים של ספק הענן.

15.2. הגנה על ממשקי הניהול

15.2.1. הספק יישם את ההגנות הבאות על כל ממשקי הניהול:

15.2.1.1. הגבלת גישה אל ממשק הניהול מרשתות / ציוד מהימן בלבד.

15.2.1.2. הצפנת התעבורה.

15.2.1.3. הפעלת יכולות זיהוי חזקה והפעלת בקרת גישה בהתאם לעקרון Role Privilege Least.

15.2.1.4. שילוב ניטור ובקרה מובנה הן לממשקים מבוססים GUI או ממשקי מכונה מבוססי API.

15.2.1.5. הפעלת מדיניות סיסמאות בהתאם לנהלי המשרד.

15.2.1.6. יישום נהלים לחילול, שמירה, שימוש נכון והחלפה תקופתית של Keys API ו – Keys Host .

15.2.2. שימוש בתקשורת מוצפנת והגבלת התקשורת במידת האפשר לטווחי כתובות ייחודיים והעדפה של ממשקים חד כיווניים (מכיוון סביבת הניהול לשירות המנוהל).

15.2.3. שימוש במשתמשים עם הרשאות מצומצמות ככל הניתן.

15.2.4. הפעלת שירותי ניטור ובקרה על פעולות הממשק, בין אם ממשק מבוסס GUI או ממשקי מכונה.

15.3. הנפקת סיסמאות חד פעמיות (OTP) למנהלנים

15.3.1. במידה ולא יעשה שימוש בתוכנת MFA, אלא באמצעות שליחת SMS חד פעמי אזי הספק יקים מערכת ניהול סיסמאות חד פעמיות המיועדים למטרה זו.

15.3.2. סיסמאות חד פעמיות יהיו במבנה הבא:

15.3.2.1. אורך 6 ספרות.

15.3.2.2. תוקף למשך 15 דקות בלבד.

15.3.3. סיסמת ה – OTP תישמר ב – Session של המשתמש בזיכרון של ה – process / service.

15.3.4. לאחר אימות זיהוי מוצלח או Timeout (פג תוקף) - יש למחוק את ה – OTP מהזיכרון לאחר זיהוי מוצלח ו\או Timeout.

15.3.5. יש לוודא כי ה – OTP נשלח ללא מספר ת.ז של המשתמשים.

15.3.6. יש לוודא כי לא ישלחו קישורים (Links) בהודעות ה- SMS.

15.3.7. בעת תקלה תתאפשר גישה של מנהלנים באמצעות הזדהות חזקה שתוגדר ביחד עם הספק.

15.4. ניהול סיסמאות למנהלנים

15.4.1. סיסמאות מנהלנים יוגדרו כסיסמאות מורכבות (אותיות, תווים, מספרים) ובאורך מינימלי של 14 תווים לפחות.

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

15.4.2. מורכבות הסיסמאות תהיה מאותיות גדולות, קטנות, ספרות ותווים מיוחדים.

15.4.3. עבור כלל הסיסמאות מספר המחזורים (היסטוריה) שיש לעבור לפני שימוש חוזר בסיסמא הנו לפחות 24 מחזורים ותוקפן יהא 90 יום.

15.4.4. נתוני הזיהוי יישמרו אישיים וחסויים (בתווך התקשורת ובמערכות השונות).

15.4.5. יש לקיים ניטור על משתמשים אלה (ראה הרחבה בפרק ניטור).

15.4.6. לאחר 5 כשלים בהזדהות יתבצע התהליך הבא:

15.4.6.1. חסימת החשבון לפרק זמן שבין 30-15 דקות.

15.4.6.2. שליחת התראה למערכת ה- SIEM , לחמ"ל הסייבר בלמ"ס.

15.4.6.3. הכרח להזדהות נוספת באמצעות Captcha או OTP.

16. ניהול חשבונות עובדי הלמ"ס

16.1. גישה לממשקי עבודה

16.1.1. גישה לממשקי עבודה, תתאפשר מחצרות הלמ"ס לעובדי הלמ"ס בלבד.

16.1.2. לא תתאפשר גישה לממשקי עבודה שלא מחצרות הלמ"ס.

16.2. סנכרון Active Directory (ADFS)

16.2.1. במידה ויידרש לעשות סנכרון בין שרת ה- Active Directory של הלמ"ס לשרת Active Directory בענן, יעשה סנכרון **<u>מוגבל</u>** לחשבונות ייעודיים (השונים מהחשבון בו נעשה שימוש בתוך רשת הלמ"ס) לכמות משתמשים **<u>מוגבלת</u>** ללא משתמשים אפליקטיביים/ניהוליים גבוהים **וללא סינכרון סיסמאות**.

16.3. ניהול משתמשים

16.3.1. ניהול המשתמשים וההרשאות יתבצע באמצעות תכנון פתרון ADFS מול שירות Active Directory פנימי אשר יעדכן את מערכות ניהול המשתמשים בענן.

16.3.2. המערכת צריכה לאפשר אימות משתמשי הלמ"ס יתבצע באמצעות אמצעי זיהוי חזק (2Factor Authentication ו/או MFA) וגם אימות משתמש מול חשבון בדומיין באמצעות פתרון Single Sign On. הלמ"ס תוכל לבחור בדרך העדיפה לה בהתאם לקבוצות המשתמשים וסוגי המידע/התהליכים המנוהלים במערכת. כאשר:

16.3.2.1. תהליכים רגישים: אימות חזק.

16.3.2.2. תהליכים כלליים: שם משתמש וסיסמא.

16.4. ניהול סיסמאות עובדי הלמ"ס

16.4.1. סיסמאות לעובדים פנימיים יהיו מורכבות מ- 8 תווים לפחות.

16.4.2. מורכבות הסיסמאות תהיה מאותיות גדולות, קטנות, ספרות ותווים מיוחדים.

16.4.3. עבור כלל הסיסמאות מספר המחזורים (היסטוריה) שיש לעבור לפני שימוש חוזר בסיסמא הנו לפחות 24 מחזורים ותוקפן יהא 90 יום.

16.4.4. נתוני הזיהוי יישמרו אישיים וחסויים (בתווך התקשורת ובמערכות השונות).

16.4.5. לאחר 5 כשלים בהזדהות יתבצע התהליך הבא:

16.4.5.1. חסימת החשבון לפרק זמן שבין 30-15 דקות.

16.4.5.2. שליחת התראה למערכת ה- SIEM , לחמ"ל הסייבר בלמ"ס.

16.4.5.3. הכרח להזדהות נוספת באמצעות Captcha או OTP.

17. ניהול משתמשי מערכות, אפליקציה ותהליכים (Service Account)

17.1. גישה לממשקי ניהול

17.1.1. הגישה לממשקים המבצעים שימוש בתהליכים אפליקטיביים תנוהל מקומית בחצרות ספק הענן.

17.2. ניהול משתמשים

17.2.1. ניהול החשבונות וההרשאות באמצעות יישום ADFS כאמור לעיל.

17.2.2. יש להגדיר חשבון ייעודי עבור כל Service.

17.2.3. אין לעשות שימוש בחשבונות בערכי ברירת מחדל (admin, monitor וכיו"ב).

17.2.4. בכל חשבון גנרי שלא משויך לעובד ספציפי או מערכת, יש לוודא כי הלוגים מאפשרים זיהוי הגורם המבצע שימשו בחשבונות אלה בפועל.

17.2.5. סיסמאות ניהוליות ישמרו בכספת סיסמאות.

17.2.6. אין לבצע שימוש בחשבון Service אחד, להרצת שירותים אחרים.

17.2.7. יש להגדיר תיאור לחשבונות הניהול בתבנית מוסכמת אשר תאפשר לזהות כי מדובר בחשבון Service ואת שם ה- Service שהוא מריץ.

17.2.8. יש לוודא מינימום הרשאות עבור service users.

17.2.9. יש לוודא כי לא מתאפשר interactive login (הגדרה נדרשת non interactive login).

17.3. ניהול סיסמאות למשתמשים אפליקטיביים

17.3.1. סיסמאות למשתמשים אפליקטיביים יוגדרו כסיסמאות מורכבות (אותיות, תווים, מספרים) ובאורך מינימלי של 14 תווים לפחות.

17.3.2. מורכבות הסיסמאות תהיה מאותיות גדולות, קטנות, ספרות ותווים מיוחדים.

17.3.3. עבור כלל הסיסמאות מספר המחזורים (היסטוריה) שיש לעבור לפני שימוש חוזר בסיסמא הנו לפחות 24 מחזורים ותוקפן יהא 90 יום.

17.3.4. נתוני הזיהוי יישמרו אישיים וחסויים (בתוך התקשורת ובמערכות השונות).

17.3.5. יש לקיים ניטור על משתמשים אלה (ראה הרחבה בפרק ניטור).

18. ממשקים לערוצי תקשורת חיצוניים

18.1. כללי

18.1.1. ערוץ מידע הינו אחד מהבאים: אפליקציות מסרים, שירותי SMS, רשת חברתית, Chat וכדומה.

18.1.2. ערוץ מידע חיצוני הינו ערוץ מידע שאינו מנוהל ו/או מוחזק בחצרות הספק באופן מלא (תשתית, אפליקציה). למשל שירות אפליקציות מסרים או שירות אתר אינטרנט חיצוני. עבור ערוצים אלה, יחולו גם ההנחיות הבאות:

18.1.3. נספח זה מגדיר הנחיות אבטחת מידע לספק בעת שימוש בערוצי מידע וקישורם למערכת ה- CRM לצורך קבלה וניהול פניות ומידע מול גורמים חיצוניים.
לדוגמה: קישור לשירות מאתר הלמ"ס, שירותי דיוור תקשורת On-Line: משלוח מסרונים (SMS) , משלוח דוא"ל, תקשורת באמצעות WhatsApp Web ובאמצעות Chat Bot.

18.2. מדיניות לשימוש בערוצי תקשורת

18.2.1. הספק יגדיר לעובדיו מדיניות שימוש בערוצי תקשורת חיצוניים. המדיניות תתייחס לכל ערוץ תקשורת בנושאים הבאים:

18.2.1.1. הספק ימנה גורם אחראי לנושאי הגנת הסייבר בערוצי התקשורת ובכללם ערוצי מידע המנוהלים באופן מלא ע"י הספק לדוגמה: אתר האינטרנט, Chat, Chat-Bot, SMS, וכן לערוצי מידע שאינם מנוהלים באופן מלא ע"י הספק לדוגמה: אפליקציות מסרים , רשתות חברתיות וכיו"ב.

18.2.1.2. הספק יגדיר את הערוצים אשר נעשה בהם שימוש ואת אוכלוסיית המשתמשים (עובדי הספק) אשר רשאים להשתמש באותם ערוצים בהקשר עם השירותים הניתנים ללמ"ס.

18.2.1.3. הספק יכתוב ויקיים נהלי עבודה בתפעול ערוצי המידע וכן מגבלות ואיסורים בשימוש בערוצים אלה.

18.2.1.4. הספק יכתוב ויקיים נהליי עבודה לטיפול באירוע הקשור לערוצי המידע.

18.2.1.5. הספק יבצע בקרה על תוכן המועבר בערוצי המידע.

18.2.1.6. הספק יבצע בקרה על תגובות של משתמשי האינטרנט בקבוצות / פורומים של הלמ"ס ויכולת הלמ"ס לצמצם נזקים בקרות אירוע.

18.2.1.7. הספק יקיים הדרכות (עשה ואל תעשה) לעובדיו ובפרט לגורמים המעורבים בניהול / תפעול חשבונות הלמ"ס (User Accounts) בערוצי מידע ובערוצי מידע חיצוניים.

18.3. הערכת סיכונים לערוצי מידע

18.3.1. הספק יבצע מיפוי סיכונים ובקרות בתהליכי עבודה בנתיב קריטי המבוססים על ערוצי המידע למתן שירות למבקשי מידע או מידע אישי, פרסומים שונים וכיו"ב.
למשל התייחסות לסיכונים הבאים:

18.3.1.1. סיכוני סייבר, פישינג וסיכוני הנדסה חברתית (Social Engineering).

18.3.1.2. חשיפת פרטי אזרחים (אישי, רגיש, פרטי הלקוח בהקשר של הלמ"ס).

18.3.1.3. גניבת זהויות (כללי, ספציפי לאזרח בהקשר של הלמ"ס), וסיכוני התחזות.

18.3.1.4. הונאת משתמשים (מסירת מידע, קבלת נתונים שגויים (בזדון או בשגגה), אישור לביצוע פעולה (למשל שינוי פרטים לאזרח/מבקש המידע), התכחשות לביצוע פעולה.

18.3.1.5. זליגת מידע או מסירת מידע לא רצויה.

18.3.1.6. העברת מידע שגוי או רגיש ללא מנגנוני בקרה.

18.3.1.7. חשיפת פרטי אימות זיהוי לאזרח/מבקש המידע.

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

18.3.1.8. חדירה למחשב מבקש המידע (גניבת מידע, גרימת נזק תוך פגיעה בשלמות הנתונים ובאמינותם).

18.3.1.9. חשיפה לנוזקות (וירוסים, סוסים טרויאנים) המצויות במרחב ערוצי המידע.

18.3.1.10. חשיפה למתקפות אפליקציה (XSS, CSRF, Click-jacking, Session Hijacking) המצויות במרחב ערוצי המידע.

18.3.1.11. פגיעה בזמינות המערכות והתשתיות אשר אינן נתונות לשליטת הספק (לדוגמה בערוצי מידע חיצוניים).

18.4. מקרים ותגובות

18.4.1. הספק יקים מערך מקרים ותגובות להתמודדות עם מימוש סיכון בכל אחד מערוצי התקשורת החיצוניים (למשל פניה לסחיטה , כופר, איום על הספק/הלמ"ס וכיו"ב).

18.5. בקרות

18.5.1. הספק יתאים את הבקרות להערכת סיכונים ומנגנוני הבקרה בשימוש בערוצים הללו על ידי הספק, מערך מקרים ותגובות להתמודדות עם התממשות של סיכונים בערוצי המידע, ועוד.

18.5.2. הספק יקיים בקרה על אופן השימוש והניהול של חשבונות והרשאות המשמשים לתפעול ערוצי המידע.

18.5.3. הספק יקיים בקרה על תוכן המועבר בערוצי המידע בשם ו/או עבור הלמ"ס.

18.5.4. הספק יקיים בקרה על תגובות של משתמשי האינטרנט בקבוצות / פורומים של ערוצי המידע ויגדיר תהליכים לצמצום נזקים ולבקרות אירוע ברשתות אלה.

18.5.5. קיום מיפוי מתוחזק ומסודר של השימושים בערוצי המידע.

18.5.6. קיום בחינה של אמצעי הבקרה המיושמים אצל הספק לבחינת ניצול תשתית הרשת והמחשוב ופגיעה בהם (למשל החדרת קוד עוין, חדירה לרשת, השבתה וכיו"ב).

18.5.7. קיום הדרכות (עשה ואל תעשה) לעובדים ובפרט לגורמים המעורבים בעבודה מול אזרחים ובתהליכי איסוף ומסירת מידע רגיש.

18.5.8. הספק יפעיל אמצעים לסינון תוכן נכנס ואמצעים למניעת דלף מידע בכל הממשקים בין מערכת ה- CRM לערוץ המידע.

18.6. שירותי דוא"ל פנימי

18.6.1. המערכת תקושר לשירותי דוא"ל לצורך הצגת מידע (פניה התקבלה, סטטוס פניה וכיו"ב) למשתמשי המערכת. שרתי דוא"ל – לצורך קבלת פניות מבקשי מידע בדוא"ל.

18.7. קישור לשירותי דוא"ל חיצוני

18.7.1. קישור זה יעשה לצורך קבלת פניות שישלחו ממבקשי מידע. הפניות ישלחו לכתובת חיצונית אשר תפורסם באתר הלמ"ס. לדוגמה info@cbs.gov.il.

18.7.2. השבת דוא"ל למבקשי מידע תתבצע

18.7.2.1. באופן פרטני מכתובות הדוא"ל של עובדי הלמ"ס

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

18.7.2.2. באופן כללי מכתובת ציבורית של הלמ"ס לדוגמה info@cbs.gov.il

18.7.2.3. לא תתאפשר שליחה ישירה של הודעות דוא"ל חיצוניות ללמ"ס ישירות ממערכת ה- CRM ושלא דרך רכיב מתווך ומנוטר.

18.7.2.4. כל דוא"ל יוצא ינוטר במערכת הלבנה וסינון מידע רגיש.

18.7.2.5. כל דוא"ל נכנס ינוטר במערכת סינון תוכן ו/או השחרה וכן באמצעים לבדיקת קלט.

19. אבטחת שירותי REST API

מערכת ה- CRM שתירכש מחוייבת לאפשר קישור למערכות צד ג' באמצעות ממשקי Rest API. פרק זה נועד להגדיר את דרישות אבטחת המידע הנדרשות ממערכת ה- CRM בתמיכה בממשקי API.

19.1. קישור למערכות צד ג' וערוצי תקשורת חיצוניים מבוססי API

19.1.1. מערכת ה- CRM תידרש להתממשק גם למערכות צד ג' וכן לערוצי התקשורת מסוג זה: אפליקציות מסרים ומובייל- בניהול ערוצי מידע של הלמ"ס (דוגמת WhatsApp או שירותי קבלת מידע ב SMS , ערוץ chat ו-Chat Bot עבור פניות ציבור מתוקשבות ברשתות חברתיות.

19.1.2. מערכת ה- CRM תתמוך באבטחת ממשקים אפליקטיביים בין מערכות הספק לערוצי תקשורת חיצוניים יעשו בממשקים מאובטחים דוגמת: פרוטוקולים מאובטחים, API או Web Services.

19.1.3. מערכת ה- CRM תתמוך בתהליכי הזדהות ואמצעי הגנה בין המערכות המקושרות בממשקים אלה.

19.2. הזדהות בממשקי API

19.2.1. מערכת ה- CRM תאפשר לבצע זיהוי של צרכני השירות באמצעות שימוש ב – Mutual Authentication, ע"י שימוש בשתי תעודות – אחת עבור שרת המערכת (חושף השירות) ושנייה עבור צרכן השירות (לדוגמה באמצעות ייצור תעודה עבור כל צרכן שירות).

19.3. אכיפת הרשאות גישה בממשקי API

19.3.1. מערכת ה- CRM תכיל מנגנון הרשאות. לדוגמה שימוש ב – Attribute: [Authorize], לפני כל End Point שחשוף לצרכני השירות.

19.3.2. מערכת ה- CRM תאפשר לזהות את צורך השירות (הספק) ולוודא כי הוא ניגש למשאבים החשופים עבורו בלבד.

19.4. בדיקות קלטים ופלטים בממשקי API

19.4.1. מערכת ה- CRM תאפשר יישום הבדיקות הבאות:

19.4.1.1. בדיקות אורך – מינימום ומקסימום.

19.4.1.2. בדיקות טווח.

19.4.1.3. סוג הקלט.

19.4.1.4. פורמט הקלט.

19.4.2. מערכת ה- CRM תוכל לאסור כל שימוש שלא במבנה שהוגדר כתקין.

19.4.3. מערכת ה- CRM תתמוך בהגדרת מבנה ה - Input (Request) וגם את מבנה ה - Output (Response) ולבצע וולידציה עפ"י המבנה שהוגדר.

19.4.4. מערכת ה- CRM תאפשר ליישם בדיקות הקלטים עם הגדרת JSON Schema עבור מבנה הקלט עבור כל שירות.

19.4.5. מערכת ה- CRM תאפשר ליישם JSON Schema עבור הפלט שנשלח עבור כל שירות.

20. תמיכה בשירותי דיוור תקשורת On-Line

20.1. כללי

20.1.1. פתרון ה- CRM, יידרש להתממשק גם למערכות עתידיות אשר הלמ"ס מתכננת ליישם. להלן דוגמאות לערוצי התקשורת מסוג זה:

20.1.1.1. אפליקציות מסרים - בניהול ערוצי מידע של הלמ"ס (דוגמתWhatsApp או שירותי קבלת מידע ב SMS .

20.1.1.2. ערוץ chat ו-Chat Bot עבור פניות ציבור מתוקשבות.

20.2. תכנון ויישום

20.2.1. בכל צורך בקישור מערכת ה- CRM לערוץ חיצוני – יעמיד הספק גורם מומחה מטעמו אשר יבחן את המשמעויות ליישום, ביחד עם הגורם העסקי בלמ"ס, אגף מערכות מידע ואגף הגנת הסייבר.

20.2.2. הספק ילווה את יישום הפתרון עד להפעלה מלאה.

20.3. אבטחת ערוצי התקשורת

20.3.1. אבטחת ערוצי התקשורת תתבצע באמצעות ממשקי מאובטחים המאפשרים הצפנת המידע וזיהוי המקורות והיעדים (לדוגמה ממשק Rest API או בשיטה אחרת מאובטחת אשר תוגדר על ידי אגף מערכות מידע ואגף הגנת הסייבר בלמ"ס).

20.4. אימות משתמשים

20.4.1. אימות משתמשי הלמ"ס תתבצע באמצעות אמצעי זיהוי חזק (2Factor Authentication ו/או MFA וכיו"ב). אך בשום אופן לא באמצעות שם משתמש וסיסמא בלבד.

20.4.2. עבור כל התחברות לשירות ניהולי, תועבר הודעה למנהל השירות מטעם הלמ"ס (גורם מבקר נוסף).

21. ניטור, תיעוד ולוגים

הספק יהא אחראי באופן מלא כל הנושאים הבאים:

21.1. כללי

21.1.1. המערכת תאפשר ייצוא הלוגים אחת לשבוע ובמבנה סטנדרטי (Syslog) והעברתם ללמ"ס.

21.1.2. הספק יחד עם הלמ"ס יגדיר את תחומי האחריות לתפעול מנגנוני הגנת הסייבר. בהתאם למודל האחריות המשותפת – ביצוע ניטור ובקרה על השירות מצוי באחריות המשרד ובין היתר האמור בפרק זה המתייחס לתהליכי: זיהוי וניהול אירועים, ניהול תצורה ושינויים וזיהוי וניהול טלאים (Patch's) ופגיעויות (Vulnerabilities).

21.1.3. הספק יפרט ללמ"ס אלו מקורות לוג זמינים לזיהוי אירועים ומהם נהלי הספק בעת זיהוי אירוע, תהליכי תרגול אפשריים לתרחישי האירוע והערכות להתמודדות עם אותם אירועים באמצעות תכנון ותרגול בעלי המקצוע הרלוונטיים הן מצד הלמ"ס והן מצד הספק וכן את תחומי האחריות.

21.2. ניהול תצורה, שינויים, ניהול טלאים (Patch) ופגיעויות (Vulnerabilities)

21.2.1. ככל שיעשה שימוש בשירותי IaaS או PaaS , הספק יאפשר ללמ"ס לתעד ולעקוב אחר כל רכיבי החומרה והתוכנה המעורבים בשירות ע"מ לוודא כי הם נתמכים ומתעדכנים. לחילופין, יוכל הספק להצהיר (באמצעות תצהיר משפטי) כי הוא מחזיק מערכות עדכניות ומתעדכנות. תצהיר זה יוגש אחת לשנה ללמ"ס כשהוא חתום על ידי מנהל בכיר מורשה חתימה ובנוסף על ידי ממונה הגנת הסייבר בפרויקט.

21.2.2. ככל שיימסר תיעוד טכני, על התיעוד אשר יהיה זמין ללמ"ס לכלול את כל הנתונים הקשורים לתצורת הרכיבים השונים ואת הקשרים ביניהם וכמו כן לתעד שינויי תצורה, תיעוד המנגנון לסריקת פגיעויות, תיעדוף תוצאות והתקנת טלאים בהתאם.

21.3. אירועי סייבר

21.3.1. הספק מחויב לעדכן את הלמ"ס בכל אירוע סייבר הנוגע לשירותים או למידע הארגוני המאוחסן אצל ספק.

21.3.2. תפעול מנגנוני הגנת הסייבר ייערך בשיתוף הספק ויתורגל בהתאם לנהלי הלמ"ס.

21.4. שירותי ניטור אבטחת מידע

21.4.1. הספק ישלח את התראות הניטור התראות על גישה לממשקי הניהול יועברו בערוץ מוצפן למערכת ה- SIEM של הלמ"ס. במידה ולא ניתן, יעמיד הספק שירות SIEM מקומי (של יצרן מוביל ב- Gartner) אשר ינטר את מערכות הענן ויאפשר גישה לניהול החוקה למוקד ה- SOC של הלמ"ס. הספק יגדיר ויעדכן את חוקי הניטור ככל שיתבקש על ידי אגף הגנת הסייבר בלמ"ס.

21.5. ניטור אירועי אבטחת מידע ותקלות

21.5.1. הספק יאפשר ללמ"ס לבצע ניטור אירועי אבטחת מידע הקשורים ליישום מחשוב ענן ולשימושו במערכות מחשוב ענן לאורך כל תקופת השימוש בשירותי מחשוב ענן.

21.5.2. הספק יאפשר ללמ"ס להגדיר יעדי ניטור, לרבות סוגי המידע והפעילויות שיש לנטר, סוג הניטור הנדרש, אופן שמירת נתוני הניטור, הגדרת הגורמים המורשים בגישה לנתונים אלו ואופן מתן הגישה אליהם.

21.5.3. הספק יאפשר ללמ"ס לבצע ניטור באמצעות כלים המסופקים ע"י הספק, אולם יש לוודא שהכלים עומדים בסטנדרטים מקובלים ומאפשרים שילוב עם מערכות הניטור הקיימות של הלמ"ס.

21.6. שעון

21.6.1. הספק יעדכן את כל המערכות בשעון אחיד NTP , לצורך אחידות במועדי הלוגים.

21.7. מערכת איסוף מרכזית

21.7.1. הספק יוודא קיום ודיווח לוגים לשרתי איסוף Syslog, NOC ו-SIEM. או בהתאם לפתרון העתידי שיוטמע בלמ"ס.

21.7.2. הספק יעשה שימוש בפרוטוקולי דיווח: SNMP V3 ו- SYSLOG סטנדרטיים.

21.7.3. הספק יתעד שינויי תצורה בכל המערכות והשרתים אשר יוגדרו במערכת. התיעוד יכלול:

21.7.3.1. מהות השינוי (לפני ואחרי).

21.7.3.2. מבצע השינוי (חשבון המשתמש).

21.7.3.3. מועד (תאריך, שעה).

21.7.4. כל המערכות יאפשרו שליפת דוחות על שינויים

21.7.5. במידה והלמ"ס תרכוש ותיישם מערכת SIEM או NOC בחצרותיה, יועברו הלוגים הלוגים למערכות הלמ"ס בערוץ מאובטח שיוקם בין הספק ללמ"ס.

21.7.6. הספק ישמור את הלוגים בבסיס הנתונים או בשרת איסוף לוגים (Collector) לכל הפחות למשך 24 חודשים (או בהתאם למדיניות).

21.8. בקרה אחר פעולות משתמשים

21.8.1. יש לקיים בקרה (לוג) אחר כל פעילות המבוצעת על ידי משתמשים החשופים לסביבת המערכת לרבות משתמשים אנושיים ומשתמשים אפליקטיביים.

21.8.2. רישום הלוגים הבאים:

21.8.2.1. ביצוע Logout במערכת.

21.8.2.2. בעת כל הצלחה או כישלון ירשם לוג.

21.8.2.3. זמני כניסה למערכת.

21.8.2.4. זמני ניתוק מהמערכת.

21.8.2.5. מועדי החלפת סיסמא.

21.9. רישום לוגים

21.9.1. הספק יוודא רישום ללוג את כל הפעולות:

21.9.1.1. פרטים מזהים (חד ערכיים) על מבצע הפעולה.

21.9.1.2. זמן ביצוע הפעולה – תאריך, שעה, דקה ושניה.

21.9.1.3. מהות הפעולה / סוג הפעולה.

21.9.1.4. ערך ישן (לפני שינוי) וערך חדש (אחרי שינוי).

21.9.1.5. סטטוס הפעולה (הצלחה, כישלון).

21.9.2. הספק יתעד מידע תפעולי ואבטחת מידע, אין לתעד מידע רגיש על משתמשי המערכת.

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

21.9.3. הספק יתעד את האירועים הבאים:

21.9.3.1. גישה ללוגים.

21.9.3.2. קריאת מידע של משתמשים.

21.9.3.3. מילוי פרטי הבקשות לרישום מבקש מידע.

21.9.3.4. מחיקת נתונים.

21.9.3.5. ביצוע זיהוי ראשוני וביצוע זיהוי חוזר באמצעות OTP.

21.10. ניטור משתמשי תהליכים (Services)

21.10.1. הספק יפעיל מנגנוני ניטור מלא על כל פעילות משתמשי Services.

21.10.2. הספק יזהה התראות על התנהגות חריגה, למשל חשבון Service המנסה להפעיל Service אחר ממה שהוגדר לו.

21.11. מניעת הכחשה

21.11.1. הספק יישם מנגנוני מניעת הכחשה בכל מקרה של ביצוע פעולות על ידי כלל המשתמשים החשופים לשירות בכל ממשק (פנימי, אינטרנט, ניהול וכדומה) כך שאימות זהות המבצע תובטח באופן חד ערכי.

21.12. תיעוד פעולות חריגות בגישה למידע

21.12.1. הספק יוודא תיעוד הפעולות הבאות:

21.12.1.1. שליפת מספר רב של נתונים.

21.12.1.2. מחיקת מידע.

21.12.1.3. פעולות ניהול במערכת.

21.12.1.4. גישה לבסיס הנתונים.

21.13. תיעוד ולוגים (התראות) ממערכות ההגנה בתקשורת

21.13.1. כל הלוגים יתעדו מועד: שעות, דקות, שניות, ותאריך.

21.13.2. נתוני התיעוד של מנגנון הבקרה יישמרו גם מקומית במערכת למשך 24 חודשים לפחות.

21.13.3. נתוני התיעוד המכילים מידע על פי תקנות הגנת הפרטיות יישמרו מקומית ובמערכת ה- SIEM וה- NOC למשך 24 חודשים לפחות.

21.13.4. תיעוד לוגים עבור ממשקים ומערכות בניהול הלמ"ס:

21.13.4.1. מזהה רשת: כתובת ה- IP, MAC, שם רכיב, פורט תקשורת.

21.13.4.2. מזהה משתמש (אנושי/אפליקטיבי) וסוג ההרשאה (קריאה, כתיבה).

21.13.4.3. מזהה היישום.

21.13.4.4. בעת גישה לקבצים: שם הקובץ והפעולה שנעשתה (שינוי לפני ואחרי).

21.13.4.5. התראות בגין שינויי הגדרות בכל אחד מרכיבי הרשת והשרתים.

21.13.4.6. התראות בגין תקלה או פגיעה במערכת או בסוכן.

21.13.4.7. כמות הפניות.

21.13.4.8. ניהול משתמשים: הצלחה או כישלון אימות משתמש, זמן כניסה למערכת, זמן ניתוק מהמערכת.

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

21.13.5. תיעוד לוגים עבור ממשקים חיצוניים:

21.13.5.1. בפניות תקשורתיות - כתובת IP, פורט תקשורת.

21.13.5.2. בפניות אפליקטיביות - סוג ומבנה השאילתה.

21.13.5.3. בפניות אנונימיות אפליקציה באמצעותה בוצעה הפניה.

21.13.5.4. בפניות מזוהות – חשבון המשתמש באמצעותו בוצעה הפעולה, לרבות חשבון משתמש של גורם אשר נירשם לפורטל הרישום.

21.13.5.5. כמות הפניות.

21.13.5.6. ניהול משתמשים: הצלחה או כישלון אימות משתמש, זמן כניסה למערכת, זמן ניתוק מהמערכת.

21.14. פרק זמן מינימלי לשמירת הלוגים

21.14.1. לוגים תפעוליים, אבטחת מידע ותיעוד פעולות המכילים מידע על פי תקנות הגנת הפרטיות יישמרו מקומית ובמערכת ה- SIEM וה- NOC למשך 24 חודשים לפחות כאשר:

21.14.1.1. **שמירת אירועים לתחקור מיידי** – ישמרו במערכות עצמן או בתהליכי גיבוי חם.

21.14.1.2. שמירת אירועים לתיעוד או תחקור בעת צורך לתקופה של מעל חצי שנה אירועים מתקופה של מעל חצי שנה ישמרו במסגרת תהליכי גיבוי קר.

21.15. ניהול הרשאות גישה ללוגים

21.15.1. יש לצמצם את הרשאות הגישה ללוגים למנהלי המערכת בלבד.

21.15.2. צפייה בלוגים

21.15.2.1. גישה ללוגים תתבצע ע"י גישת UI דרך מסך ייעודי המשמש למטרה זו ונגיש מרשת הלמ"ס בלבד.

21.15.2.2. גישה למסך זו תאופשר למנהל המערכת בלבד.

21.15.2.3. אין לאפשר או להסתמך על גישה ישירה לבסיס הנתונים למטרה זו.

21.15.3. יש למנוע יכולת מחיקה או שינוי לוגים – גם לבעלי הרשאות גבוהות (מנהלי המערכת).

21.16. התראות

21.16.1. בעת אירוע סייבר או בעת כשל תפעולי של מערכת ליבה, ניטור, אבטחת מידע או אפליקציה מהותית באחת המערכות הבאות: IPS, DB Firewall, WAF ו/או מערכות אבטחת מידע בחצרות הלמ"ס ו/או באמצעי המחשוב שנמסרו למבקש המידע. תשלח הודעה מידית לראש תחום יישומי אבטחת מידע ולראש אגף הגנת הסייבר בלמ"ס לצורך בחינת הסיכון והמשכיות השירות בגישה לעדכון נתונים ללא יכולת ההגנה.

21.16.2. עבור כל רישום של לוג של פעולה חריגה במערכת יש לייצר התראה.

21.16.3. ההתראה תישלח לקבוצת אנשים מוגדרים באמצעות אי-מייל או SMS המציין שקיימת פעילות חריגה במערכת.

21.16.4. במידה ותיושם מערכת SIEM, יש להפנות לוגים אליה או אל Collector אשר יותקן בסביבות השונות בפרויקט.

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____

21.16.5. במידה ויבוצע שימוש במוקד ניטור SOC, יועברו התראות למוקד. בהתאם למדיניות וסוגי מידע שיאושרו על ידי ראש אגף הגנת הסייבר בלמ"ס.

21.16.6. צפייה בפעולות החריגות המערכת יתבצעו דרך ממשקי הניהול השונים המאפשרים צפייה בלוגים אפליקטיביים במערכת.

21.17. דוחות

21.17.1. המערכת תדע לייצא דוחות בתדירות יומית, שבועית וחודשית לכל אורך זמן אספקת השירות במטרה לאתר שינויים בהתנהגות.

21.17.2. הדוחות יכללו את נושאים הבאים:

21.17.2.1. דוחות סיכום ומגמות (עומסים, כשלים, תקלות ואירועי אבטחת מידע וסייבר).

21.17.2.2. אירועי מניעת הכחשה

21.17.2.3. תיעוד פעולות חריגות בגישה למידע

21.17.2.4. שליפת מספר רב של נתונים.

21.17.2.5. מחיקת מידע.

21.17.2.6. פעולות ניהול במערכת.

21.17.2.7. גישה לבסיס הנתונים.

21.17.2.8. תיעוד ולוגים (התראות).

21.17.2.9. חוקה: יצירת חוקה חדשה, שינויים בחוקה קיימת, הסרת חוקה, עצירת חוקה (disable).

21.17.2.10. משתמשים: יצירת משתמש חדש, יצירת משתמש ניהולי, שינויים בהרשאות.

21.18. גיבוי לוגים ודוחות

21.18.1. יש לבצע גיבוי תדיר ומסודר באמצעות העברת הלוגים לסביבת רשת פנימית דרך ממשק מאובטח.

21.18.2. יש לבצע בדיקות מדגמיות לבדיקת תקינות גיבוי הלוגים.

חתימה בראשי תיבות של מורשה/י החתימה מטעמו של המציע וחותמת המציע:_____

חתימה בראשי תיבות של ממונה אבטחת המידע או ממונה הגנת הסייבר מטעמו של המציע וחותמת המציע:_____