קובץ מכרז מתוקן מיום 28.4.2022 בהתאם למסמך הבהרות ושינויים מס׳ 3
(השינויים לעומת הנוסח המקורי מסומנים בעקוב אחר שינויים)

נספח 2.11 למפרט הטכני - אבטחת מידע והגנת הפרטיות

מטרת נספח זה שהינו חלק בלתי נפרד מהמכרז ומהמפרט הטכני היא להגדיר, לאפיין ולקבוע את התנהגות נותן השירותים ואת כלל המערכות בהן יעשה שימוש לטובת מתן השירותים נשוא המכרז: בין אם יתפעל אותם ישירות ובין אם באמצעות צדדים נוספים – ככל שלא הוגבלו בגוף המכרז או בנספח זה – בכל הקשור לאבטחת המידע, הגנה בסייבר, חוק הגנת הפרטיות והמסתעף מהם והכל על פי כל דין.

בנספח זה – "המערכת": אוסף פרטי החומרה, התוכנה, היישומון והתקשוב: בין אם הותקנו בחצרות נותן השירותים ובין במקומות אחרים וכן כל שילוב ביניהם, אשר במשותף ו\או בחלקים קבועים או משתנים מתופעלים (ע"י נותן השירותים או קבלני משנה מטעמו או כל גוף או אדם מטעמו) על מנת לספק למשרד את השירותים עליהם התחייב במסגרת המכרז.

1 כללי

1.1 כל המידע הקיים ושיצטבר במערכת לצורך מתן השירותים אותם התחייב נותן השירותים לתת הוא באחריות נותן השירותים – על כל המשתמע מכך ע"פ חוקי מדינת ישראל וע"פ כל דין. במסגרת אחריותו זו, נותן השירותים נחשב "כמחזיק המידע" והוא אחראי על שמירת פרטיות המידע וסודיותו.

1.2 המערכת והפעלתה כפופים להוראות חוק הגנת הפרטיות ולתקנות אבטחת המידע. ההוראות הקבועות בפרק זה לעניין הגנה בסייבר ואבטחת המידע המועבר או השמור אצל נותן השירותים יחולו למעט במקרה של סתירה עם הוראות כל דין.

1.3 באחריות נותן השירותים להשתמש בכל האמצעים הנדרשים על מנת להבטיח את סודיות המידע השמור במערכת, בצינורות המידע ובממשקים מהמערכת ליעדים הלגיטימיים שפורטו במכרז, למנוע זליגת מידע מהמערכות לגורם בלתי מורשה, למנוע כל שימוש לבד מהמטרות עליהן הצהיר על פי כל דין ועל פי תנאי המכרז ולאפשר תפעול המערכת ללא הפרעה ו\או השבתה שמקורם באירועי אבטחת מידע ו\או סייבר.

1.4 על נותן השירותים למלא את הבקרות הנדרשות במערכת יובל של מערך הסייבר, כספק מהותי בדרגה A ולהגיש למשרד את הדוח עד 60 יום ממועד תחילת ההתקשרות לכל המאוחר.

1.5 באחריות נותן השירותים לוודא כי מערכות החומרה והתוכנה המשמשות והשירותים הנוספים – בין אם מסופקים ע"י נותן השירותים ובין באמצעות צד ג' לצורך מתן השירותים - מאפשרות רמה גבוהה של זמינות, מהימנות ואמינות, ומעניקות הגנה נאותה מפני חדירה, שיבוש, הפרעה או גרימת נזק למחשב או לחומר מחשב כהגדרתם בחוק המחשבים, התשנ"ה-1995.

1.6 באחריות הנותן השירותים להבטיח את קיומם של אמצעים לאבטחת המידע במערכת ולניהול סיכונים הקיימים או העלולים להתקיים במערכת, למניעתם, ככל האפשר, או להגבלתם. לשם

כך, נותן השירותים והמערכת יעמדו במבחני הסמכה לפי תקן ישראלי ת״י 27001 המקביל לתקן ISO/IEC 27001 של מכון התקנים או לפי תקן מקביל של מי שאושר לעניין זה לפי סעיף 12 לחוק התקנים, תשי״ג-1953.

1.7 נותן השירותים יקים פונקציות ביקורת פנים ארגוניות שבאחריותן לבקר את הפעילות הנעשית בתחום אבטחת מידע והסייבר ויאפשר ניהול פעילות זו.

1.8 לכל אורך תקופת המכרז, המשרד רשאי לערוך בקורת אצל נותן השירותים, בתיאום מראש, בעצמו או באמצעות מבקר מטעמו, לרבות בחצרות נותן השירותים ו\או צד ג׳ (מהותי) ולבקש מנותן השירותים כל מידע הרלבנטי לפעולות במידע שמבצע נותן השירותים.

1.9 נותן השירותים יעמוד בהוראות החוקים, התקנות וההוראות הרגולטוריות לרבות:

1.9.1 חוק הגנת הפרטיות ותקנותיו.

1.9.2 תקן ISO 27001

1.9.3 תקן SOC2 (לסביבות ענן)

1.9.4 תורת ההגנה של מערך הסייבר הלאומי ומתודולוגית מערך הסייבר הלאומי בנושא שרשרת האספקה.

1.9.5 תקן OpenID Connect/ OAuth2.

2 מדיניות אבטחת מידע

2.1 נותן השירותים יגדיר את מדיניות אבטחת המידע במסמך אשר יתייחס לכל הדרישות המובאות בחוק הגנת הפרטיות ותקנות אבטחת המידע, לסיכוני סייבר, לזיהוי ואימות, לפיתוח מאובטח וכן לעקרון של הפרדת תפקידים בין הגורם המבצע לגורם המאשר, לשמירה על רמת מודעות גבוהה של עובדי נותן השירותים לנושא אבטחת המידע.

2.2 נותן השירותים יעדכן את מסמך מדיניות אבטחת המידע מעת לעת, בהתאם לשינויים במדיניות ובהתאם לשינויים טכנולוגיים או שינויים מהותיים במערכת.

3 מנהל אבטחת מידע (CISO)

3.1 נותן השירותים ימנה מבין עובדיו מנהל אבטחת המידע ויגדיר במסמך מדיניות אבטחת המידע את תפקידיו ותחומי אחריותו, והכל בכפוף להוראות כל דין ודרישות המכרז.

3.2 מנהל אבטחת המידע יהיה בעל כישורים וניסיון מקצועי רציף - בחמש השנים האחרונות בתחום אבטחת המידע.

3.3 מנהל אבטחת המידע יהיה כפוף ישירות למנכ״ל החברה או לחבר הנהלה ולא ימלא תפקיד נוסף שעלול להעמידו בניגוד עניינים עם מילוי תפקידו.

4 נוהל אבטחת המידע

4.1 מנהל אבטחת המידע יערוך נהלי אבטחת מידע מפורטים בהתאם למדיניות אבטחת המידע שנקבעה.

4.2 נהלי אבטחת המידע יתבססו על הליכי מיפוי, סיווג מערכות מידע וסקר סיכונים ויתייחס לכל הפחות לנושאים הכלולים בתקנה 4 לתקנות אבטחת המידע ובכפוף להוראות כל דין, לנושאים הכלולים במדיניות אבטחת המידע ולנושאים הבאים: מתן הרשאות גישה, זיהוי התושבים הזכאיים ואימות זהותם, מיפוי וסיווג מידע, מיפוי וניהול סיכוני סייבר, פיתוח מאובטח, אחריות אישית, אבטחה פיזית, ביצוע בקרות, הכנסה והוצאת מידע, טיפול באירועי אבטחת מידע, תהליכי הפקת לקחים, דיווחים פנימיים ודיווחים למשרד, מודעות והדרכת עובדים, טיפול במצעי מידע ניידים, יישום המלצות ומעקב, התקשרות למערכות חיצוניות וכדומה.

4.3 נותן השירותים יעדכן את נהלי אבטחת המידע לפחות פעם בשנה ובהתאם לשינויים במסמך מדיניות אבטחת המידע, שינויים טכנולוגיים, שינויים מהותיים במערכת ובהתאם לתוצאות ביקורות וסקרי סיכונים תקופתיים.

5 תוכנית עבודה

5.1 נותן השירותים יבנה תכנית עבודה שנתית על בסיס מדיניות ונהלי אבטחת המידע והערכת הסיכונים. התכנית תתייחס לתהליכי העבודה, מערכות המידע והתשתית, טכנולוגיות בשימוש, עובדים וגורמים מעורבים בתהליכים.

5.2 תכנית העבודה תכלול בתוכה: הפחתת סיכוני אבטחת המידע, העלאת מודעות עובדים, זיהוי וטיפול באירועים חריגים, ביצוע סקרי סיכונים, מבדקי חדירה ועוד.

6 הערכת סיכוני סייבר ופרטיות

6.1 נותן השירותים יבצע הערכה של סיכוני הסייבר והפרטיות עמם הוא מתמודד.

6.2 הערכת הסיכונים תכלול, בין היתר, את השלבים הבאים:

6.2.1 זיהוי תהליכים, מערכות, נכסי מידע וגורמים מעורבים.

6.2.2 מיפוי הסיכונים לתהליכים, למערכות, לנכסי מידע ולגורמים המעורבים.

6.2.3 מיפוי סיכונים שורשיים.

6.2.4 מיפוי הבקרות למזעור הסיכון.

6.2.5 הערכת סיכון שיורי (בהתאם להשפעת הבקרות שיושמו).

6.3 לצורך מיפוי הסיכון נותן השירותים יעשה שימוש גם בממצאי ביקורות וסקרים, איסוף וניתוח אירועי סייבר שהתרחשו בעבר וניתוח תרחישים לזיהוי אירועים פוטנציאליים של התממשות הסיכון.

6.4 הערכת הסיכונים תתייחס בין היתר למערכות תשתית (כגון: חשמל, מיזוג אויר, בקרה וכדומה) ולסביבות אחרות לייצור העשויות להכיל מידע רגיש או להשפיע על מערכות המידע.

6.5 הערכת הסיכונים תתייחס למכלול שרשרת האספקה ולסיכונים הנובעים מאופי הפעילות אל מול הגורמים השונים במרחב (מחשוב ענן, מיקור חוץ, נותני שירותים, תושבים זכאיים, וכדומה).

6.6 הערכת הסיכונים תבוקר ותעודכן באופן שוטף עם כל שינוי משמעותי בתהליכים עסקיים, בסביבה הטכנולוגית או במתאר הסיכונים, ולכל הפחות אחת ל-18 חודשים.

7 הגנת הפרטיות

7.1 נותן השירותים יבטיח כי המערך הטכנולוגי שישמש את המערכת ימזער, ככל הניתן ובשים לב לחלופות טכנולוגיות מקובלות, את הסיכון לפגיעה בפרטיות התושבים הזכאיים.

7.2 נותן השירותים יבצע תוכנית אכיפה שנתית לעמידה בדרישות תקנות הגנת הפרטיות - אבטחת מידע תשע״ז-2017, לרבות תיעוד בקרות ובדיקות מיפוי והסרת מידע עודף שלא מבצעים בו שימוש.

8 מיפוי, סיווג וסקרי סיכונים

8.1 נותן השירותים יערוך מיפוי של כל הרכיבים המשמשים את המערכת כולל מערכות המספקות תשתית לרכיבי המערכות.

8.2 נותן השירותים יסווג את רכיבי המערכת שנרשמו במסגרת מיפוי כאמור, על פי רמת הסודיות, הקריטיות התפעולית ונכונות הנתונים בהתאם לרגישות העסקית.

8.3 מיפוי רכיבי המערכות וסיווגם יעודכנו באופן שוטף ולכל הפחות פעם בשנה.

8.4 נותן השירותים יערוך באמצעות גורם חיצוני בלתי תלוי המתמחה בביצוע סקרי סיכוני סייבר, סקר לאיתור סיכוני סייבר (להלן - סקר סיכונים). סקר הסיכונים יכלול, בין השאר, בחינת סיכוני האבטחה בתהליכים תפעוליים, בחינת תהליכי הבקרה, הבקרות המבוצעות ותפעול יחידות הגילוי והטיפול באירוע חריג.

8.5 סקר הסיכונים יערך אחת ל-18 חודשים לפחות וכן לפני הטמעת שינויים טכנולוגיים משמעותיים ו/או הפעלת שרות חדש.

8.6 סקר הסיכונים יתבצע לפי מתודולוגיות מקובלות. המשרד רשאי להעביר טרם ביצוע הסקר דגשים לביצוע הסקר בהתאם למקובל בשוק ולהתפתחויות.

8.7 תכנית העבודה לביצוע הסקרים והמבחנים תיישם את הנושאים הבאים, בהתאם להערכת הסיכונים:

8.7.1 כיסוי של כל רמות האבטחה של התהליכים והמערכות, לרבות הגנות פיזיות וסביבתיות, הגנות ברמת התשתית הטכנולוגית, מערכות הפעלה, מערכות תקשורת, בסיסי נתונים, מערכי אחסון, ממשקים, רכיבי Middleware וכדומה. הגנות אפליקטיביות, הגנות המיושמות ברמת האפליקציה והגנות ברמת הלוגיקה העסקית המיושמת במערכת וכן התהליכים הסובבים את המערכת כגון ניהול משתמשים והרשאות, תהליכי גיבוי, ניטור, ניהול זיהוי ואימות וכדומה.

8.7.2 נוסף על האמור לעיל, טרם הטמעת שינוי משמעותי שהוערך בעל סיכון גבוה במערכת, או בסביבתה הטכנולוגית, יבוצע סקר לבחינת תאימותה למדיניות ולנהלי סיכוני סייבר של נותן השירותים.

8.8 תוצאות סקר הסיכונים יועברו למנהל אבטחת המידע של נותן השירותים, לבחינת הצורך בעדכון מדיניות אבטחת המידע או נוהל אבטחת המידע ולתיקון הליקויים שנתגלו במסגרת הסקר, ככל שנתגלו.

8.9 ליקויים שנתגלו בסקרי הסיכונים, ותכנית העבודה לטיפול בליקויים ידווחו לאגף בטחון, חירום, מידע וסייבר במשרד לשוויון חברתי, בהקדם האפשרי ולא יאוחר מ-30 יום מהמועד שבו נתקבלו אצל נותן השירותים.

8.10 טיפול בליקויים יטופלו על פי רמת סיכון ובהתאם לטבלה הבאה:

רמת סיכון	לו״ז לטיפול	אישור טיפול (בדיקה חוזרת)
קריטית	עד 5 ימים	נדרש
גבוהה	עד 30 יום	נדרש
בינונית	עד 90 יום	לא נדרש
נמוכה	עד 360 יום	לא נדרש

8.11 ליקוי שתידרש דחייה בטיפול, תשלח למשרד בקשת לדחיית הטיפול. המשרד ישקול האם לאשר את הבקשה או לחייב טיפול על פי הלו״ז שנקבע.

9 מבדקי חוסן (חדירה)

9.1 נותן השירותים יערוך מבדקי חוסן על ידי גורם חיצוני בלתי תלוי המתמחה בביצוע מבדקי חוסן, המבדקים יכללו בין השאר, מבחני חדירה ברמה תשתיתית ואפליקטיבית, מבדקים המדמים ניסיון תקיפה מרשתות חיצוניות (כגון רשת האינטרנט, חיבור לספקים או שותפים עסקיים) ורשתות פנימיות, בדיקות הנדסה חברתית, בחינת היכולת להחדרת תוכנות עוינת וגילויה ע״י מערכות הבקרה, התחזות ופישינג, הן על ידי משתמש והן על ידי מי שאינו מזוהה כמשתמש, בשיטות Black Box ו-White Box לפחות.

9.2 המבדקים יבוצעו על פי מתודולוגיות בדיקה נפוצות (OWASP לדוגמא).

9.3 המבדקים יכללו בדיקת קוד מאובטח (Secure Code Review) במטרה לוודא כי לא קיימות ״דלתות אחוריות״ או Debug, כמו כן לוודא כי לא קיימות מתודות במערכת אשר נועדו לעקוף מנגנוני אבטחה (לרבות בשביל ביצוע ניסיונות, שימוש פנימי ועוד).

9.4 כל גרסה חדשה תכלול גם בדיקת קוד מאובטח כתנאי להפעלתה.

9.5 מבחני חדירה מלאים למערכת ייערכו אחת ל-18 חודשים לפחות וכן לפני הטמעת שינויים טכנולוגיים משמעותיים ו/או הפעלת שרות חדש, עם זאת במידה ובוצעו שינויים/פיתוחים נקודתיים במהלך השנה ניתן יהיה לבצע, מבדקי חדירה הרלוונטיים לשינוי בלבד.

9.6 תוצאות המבדק יועברו למנהל אבטחת מידע של נותן השירותים לתיקון הליקויים שנתגלו במסגרת המבדק, ככל שנתגלו.

9.7 ליקויים שנתגלו במבדקי החוסן ותוכנית העבודה לטיפול בליקויים ידווחו לאגף בטחון, חירום, מידע וסייבר במשרד לשוויון חברתי, בהקדם האפשרי ולא יאוחר מ-30 יום מהמועד שבו נתקבלו אצל נותן השירותים. הליקויים יטופלו בהתאם לטבלה בסעיף 8.10.

10 ניטור, בקרה ומוכנות לאירועים

10.1 נותן השירותים יממש מערך ניטור ובקרה לקבלת דיווחים בזמן אמת במערכת והשירות המוצע למשרד (ראה הגדרות לעיל) אודות חשש לאירוע סייבר.

10.2 נותן השירותים יפעל לאיסוף וניתוח מידע רלוונטי, ממקורות פנימיים וחיצוניים לצורך זיהוי וטיפול באיום אבטחת מידע וכבסיס לקבלת החלטות מושכלת, תיעדוף של דרכי פעולה, וקיום הגנה אפקטיבית בזמן אמת.

10.3 כל אירוע משמעותי (שכתוצאה ממנו, באופן ישיר או עקיף, כגון: נפגעו או הושבתו מערכות ייצור למשך של יותר משעתיים, חשש שמידע רגיש נחשף או דלף) ידווח למשרד בפרק הזמן המיידי עליו נודע.

10.4 נותן השירותים יגדיר תכנית היערכות לניהול וטיפול באירועים חריגים, בהתאם להערכת סיכונים ולניתוח תרחישים (כגון: גישה לא מורשית למידע, זליגת מידע, התחזות, נוזקות, הונאה, מניעת שירות וכדומה). התכנית תכלול את כל השלבים: גילוי, ניתוח, דיווח, בלימה, הכרעה וחזרה לשגרה.

11 תצורת אבטחת המידע

11.1 המערכת תאפשר העברת קבצים/מסרים באמצעות תקשורת נתונים מוצפנת ומאובטחת בלבד, כך שלא ניתן יהיה לגשת למידע ללא הרשאת הנמען. בהתאם לכך, המערכת תוכל להשתמש בכל תקשורת נתונים העומדת בהוראות אלה .

11.2 המערכת נדרשת לבצע בקרת איכות המידע, לרבות בדיקות אימות, תקינות, שלמות וסבירות, של כל מידע המועבר אליה ובאמצעותה, לרבות באמצעות "מערכת הלבנה".

11.3 נותן השירותים הינו האחראי הבלעדי לעמידה בכל תנאי מכרז זה ובהוראות כל דין, לרבות דרישות אבטחת המידע. נותן השירותים רשאי להשתמש בתעודת הצפנה המאושרת על ידי כל CA מוכר. על נותן השירותים לוודא שהתקנת והגדרת התעודה תעמוד ברמת A+, בכפוף לעמידה בדרישות המכרז ובהוראות כל דין כאמור.

11.4 כל המערכת, מערכות תשתית, מערכות תומכות, מערכות ההגנה, מערכות תקשורת ואמצעי

אבטחת הגישה למערכת יעודכנו באופן שוטף, בהתאם להתפתחות הסיכונים ולטכנולוגיות מקובלות בתחום וכן בהתאם להתפתחות תקני אבטחת מידע בינלאומיים מקובלים.

11.5 המערכת לא תאפשר שימוש בהתקנים נתיקים/ניידים לשם העברת מידע שהועבר או נשמר במערכת, למעט לצורך גיבוי הנתונים.

11.6 המערכת תקושר לרשת האינטרנט ולמערכות חיצוניות אחרות באופן מאובטח תוך יישום אמצעי הפרדה וסינון מתאימים ורק לשם הפעלת היישומים הנדרשים לתפעול המערכת בלבד.

11.7 נותן השירותים יישם כלי הגנה על המערכת מפני סיכונים מרשת האינטרנט כגון: מערכות IPS, מערכות WAF, הצפנות, מערכות הלבנה/השחרה, API-FW, DB-FW וכדומה.

11.8 נותן השירותים יוודא כי לא נותרו הגדרות ברירת מחדל אותם ניתן לנצל לביצוע פעולות לא מורשות במערכת וכן לא ניתן יהיה לבטל מאפייני אבטחה שנקבעו על ידי המשתמשים.

12 התקשורת בין נותן השירותים למשרד

12.1 נותן השירותים יחבר את המערכת לרשת המשרד באמצעות שדרת המידע או הקמת רשת פרטית מאובטחת ומוצפנת, כגון: תקשורת VPN, בהתאם להחלטת המשרד.

12.2 המידע הנדרש יועבר בין מערכות המשרד למערכות נותן השירותים באמצעות API מאובטח על פי פרוטוקול REST.

12.3 המשרד יעביר לנותן השירותים את המידע המזערי המתחייב לצורך עבודתו.

13 אבטחה פיזית של מתקני המערכת

13.1 נותן השירותים יוודא כי רכיבי המערכת אשר מופו כאמור, יישמרו במקום מוגן, המתאים לאופי פעילות המערכת ולרגישות המידע המועבר בה או נשמר בה ואשר מונע חדירה אליו בלא הרשאה.

13.2 נותן השירותים ינקוט אמצעים סבירים לבקרה על הגישה לאתרי המערכת ולתיעוד גישות שבוצעו, לרבות הכנסה והוצאה של ציוד אל אתרים אלה ומהם.

13.3 נותן השירותים ישתמש באבטחה פיזית המבוססת על מעגלי הגנה, כך שחדרים בהם מאוחסן מידע רגיש או ציוד המאפשר גישה לרכיבים רגישים של המערכת, יהיו במעגל ההגנה האחרון (הפנימי ביותר). מעגל ההגנה הראשון יוצב בכניסה למתקני נותן השירותים, מעגל הגנה שני יוצב בכניסה לכל קומה, מעגל הגנה שלישי יוצב בכניסה לפרוזדורים או מבואות, מעגל הגנה רביעי יוצב בכניסה לאזורים רגישים יותר כגון: חדר המחשב וכדומה.

13.4 כל הכניסות למתקני המערכת, וכן לאזורים רגישים יצולמו באמצעות מצלמות במעגל סגור.

13.5 משרדים/סניפים יאובטחו וימנעו גישה של לא מורשים. הכניסה תכלול בקרת גישה באמצעות התקן פיזי אישי של העובד או באמצעות אמצעי זיהוי ביומטרי.

13.6 הרשאות כניסה לאזורים רגישים יינתנו בהתאם לתפקידי העובד.

14 אבטחת מידע בניהול כוח אדם

קובץ מכרז מתוקן מיום 28.4.2022 בהתאם למסמך הבהרות ושינויים מס׳ 3

(השינויים לעומת הנוסח המקורי מסומנים בעקוב אחר שינויים)

14.1 נותן השירותים יערוך נוהל לגיוס עובדים, תהליכי עבודה וסיום עבודה בהיבט של אבטחת המידע. נוהל זה יכלול התייחסות לנושאים הבאים לפחות:

14.1.1 הליך גיוס עובדים, לרבות עריכת בדיקות מהימנות מועמד לעבודה בשים לב לתפקיד שאותו הוא מיועד למלא והחתמת עובד על התחייבות לשמירה על סודיות ולאחריות העובד בכל הנוגע להיבטי סיכוני אבטחת מידע ופרטיות. ~~מועמד לתפקיד המוגדר כרגיש הכולל הרשאות למידע רגיש המועבר או נשמר במערכת או שיש לו הרשאות העלולות להוות סיכון להשמה יידרש לעמוד גם בבדיקת פוליגרף, כחלק מבדיקת הכשירות.~~

14.1.2 אחריות העובד לשמירה על אבטחת מידע ופעולות שיש לנקוט לשם כך.

14.1.3 תכנית הכשרה והדרכה לפעולות הנדרשות לשמירה על אבטחת המידע והעלאת המודעות לנושא ולסיכונים, בטרם מתן הרשאות גישה, לרבות יידוע העובדים על מערכות אבטחת המידע והבקרות הקיימות והדרכות תקופתיות לעובדים.

14.2 נותן השירותים יערוך נוהל לתהליך סיום עבודה. הנוהל יתייחס לעובדים (לרבות עובדים במיקור חוץ ועובדי קבלן) העוברים תפקיד או מסיימים את העסקתם, לחסימת הרשאות גישה למידע שאינו נדרש עוד, החזרת ציוד ונכסי מידע של נותן השירותים.

14.3 קיום הדרכות לעובדי נותן השירותים ולמורשי הגישה למידע הקיים במערכת או המועבר בהן בנוגע לסיכוני אבטחת מידע ודרך צמצומם, מדיניות אבטחת המידע ונהלי אבטחת, בהיקף הנדרש למילוי תפקידם. הדרכה כאמור תתקיים אחת לשנה ולעובד חדש, סמוך למועד העסקתו ככל שניתן.

14.4 נותן השירותים יבוצע מבדקים (לומדה ושאלונים) לבחינה ושיפור הידע של העובדים בנושאי אבטחת מידע ופרטיות.

15 זיהוי ואימות עובדי נותן השירותים

15.1 נותן השירותים יקבע הוראות לזיהוי המשתמשים הפנימיים במערכת (עובדי נותן השירותים).

15.2 זיהוי עובדי נותן השירותים יעשה תוך שימוש באמצעי זיהוי חזק הכולל אמצעי חומרה המאפשר זיהוי חד-ערכי. לעניין סעיף זה, זיהוי חזק הינו זיהוי המבוסס על שני גורמים לפחות מבין אלה:

15.2.1 תכונה פיזיולוגית ייחודית של המשתמש (Something you are).

15.2.2 פריט הנמצא ברשות המשתמש (Something you have).

15.2.3 פריט מידע הידוע למשתמש (Something you know).

15.3 נותן השירותים יקבע מדיניות ניהול הסיסמאות ותכלול את הכללים הבאים לפחות:

15.3.1 סיסמאות מורכבות ולא טריוויאליות, בהתאם לסטנדרטים מקובלים;

15.3.2 אורך סיסמה מינימלי של 8 תווים לפחות, למנהלי מערכת 14 תווים;

15.3.3 שמירת היסטוריית סיסמאות של 24 הסיסמאות האחרונות לפחות;

15.3.4 הפעלת שומר מסך עם דרישת סיסמה לאחר 15 דקות של אי-פעילות לכל היותר;

15.3.5 החלפת סיסמה למשתמש שאינו מועסק מדי 3 חודשים לפחות;

15.3.6 חסימת משתמש לאחר 5 ניסיונות כושלים לזיהוי לכל היותר.

16 זיהוי ואימות תושבים זכאיים ביישומון

16.1 הרשמה והזדהות ראשונית ליישומון, כחלק מתהליך ההרשמה המזוהה כמפורט במפרט הטכני, תתבצע על ידי שילוב עם רכיבי ההזדהות של מערכת ההזדהות הלאומית.

16.2 לחלופין, ובהתאם להנחיית המשרד, תתבצע ההרשמה וההזדהות הראשונית על פי הדרישות הבאות:

16.2.1 זיהוי המבוסס על סריקת תעודת הזהות, הזנת מספר זהות, צילום עצמי (סלפי), הזנת תאריך הלידה ומספר הטלפון הנייד.

16.2.2 לאחר הזנת הפרטים לעיל, יישלח מסרון לתושב הזכאי עם קוד אישור חד פעמי (OTP) שעליו יהיה להזין ביישומון.

16.2.3 השרת יפיק וישלח Token אישי למשתמש להזדהות ב- Client.

16.2.4 ה-Access Token יישמר באזור המאובטח של המכשיר הנייד. בעת קריאתו יישמר בזיכרון CACHE בלבד ולא יישמר ב-Persistent Storage.

16.2.5 ה- Token ינוקה מזיכרון ה-CACHE בעת סגירת היישומון.

16.2.6 ה-Token יעבור כ- Authorization Header על בסיס OAuth 2.0.

16.2.7 ה-Access Token יחולל בשרת ויהיה בעל תוקף של לא יותר מ- 90 יום. בכל כניסה עם ה-Token תופעל פונקציית Keep Alive. Token שלא נעשה בו שימוש במשך למעלה מ- 90 יום, לא יהיה תקף.

16.2.8 אימות התושב הזכאי ליישומון באופן שוטף יתאפשר באמצעי האימות הקיימים במכשיר הנייד של התושב הזכאי, כגון: קוד, סיסמה, טביעת אצבע, זיהוי פנים וכדומה. אמצעי האימות יבחר על ידי התושב הזכאי.

17 ניהול משתמשים והרשאות

17.1 נותן השירותים יעשה שימוש בממשקי ניהול של המערכת אשר יאפשרו הפרדת סמכויות (מדרג הרשאות) לפי השתייכות לקבוצות, הרשאות נקודתיות וכדומה.

17.2 נותן השירותים יגדיר נהלים המתייחסים לתהליך ניהול המשתמשים וההרשאות במערכת, החל מיצירת חשבון משתמש, מתן הרשאות, נעילת החשבון בתום העסקה ובקרה אחר הביטול. כל התהליך מלווה באישורים המתאימים.

17.3 ממשק הניהול כאמור יהא במודול נפרד אשר אינו נגיש לעובדי נותן השירותים, למעט מנהל אבטחת המידע, מנהלי המערכת ומבקרי ההרשאות, לרבות אחראי על בקרה לאחר ביצוע שינוי

בידי מנהלי המערכת. ככל שלא צוין אחרת במכרז זה, בעלי התפקידים המוזכרים בסעיף זה יקבעו על ידי נותן השירותים.

17.4 הרשאות גישה לעובדי נותן השירותים יינתנו בהתאם להגדרת תפקיד העובד.

17.5 עובדים כגון: מנהלי רשת/אנשי סיסטם של נותן השירותים יקבלו הרשאות אדמיניסטרציה לשרתים של המערכת ככל שנדרש לשם הפעלת המערכת ותחזוקתה בלבד, אך לא יקבלו הרשאות לצפייה במידע המועבר במערכת או הנשמר בה או לעדכון מידע זה.

17.6 הרשאות גישה למשתמשים במערכת יינתנו בהתאם לסוג המשתמש והפעולות שרשאי על פי כל דין לבצע במערכת ובכפוף לאימות זהות המשתמש. ההרשאות יינתנו על בסיס הפרדת תפקידים כך שלא יתאפשר למשתמש בודד לבצע מעגל עבודה שלם.

17.7 מנהל אבטחת המידע ינהל רישום מעודכן בכל עת של סוגי תפקידים וסוגי משתמשים, הרשאות הגישה המתאימות לכל סוג תפקיד ולכל סוג משתמש ושמות בעלי תפקידים או שמות משתמשים אלה. כמו כן יערוך בקרה לפחות פעם ברבעון לגבי חשבונות של עובדים שעזבו, חשבונות שלא נעשה בהם שימוש במשך תקופת הרבעון, שימוש בחשבונות גנריים, שינוי תפקיד המשתמש והרשאותיו.

17.8 הרשאות גישה של עובד, אשר יש לו גישה למערכת כמנהלן, ואשר סיים את עבודתו, יבוטלו מיד עם סיום עבודתו, וכן יוחלפו סיסמאות וקודי גישה למערכת שעשויים היו להיות בידיעת העובד.

17.9 הרשאות הגישה של תושב זכאי יבוטלו במקרה של שינוי במעמדו, מיד עם הבאת המידע על ביצוע השינוי לידי נותן השירותים, כמפורט להלן:

17.9.1 ביטול תוקף אמצעי הזיהוי המשמש לזיהוי המשתמש במערכת.

17.9.2 שינוי במעמד החוקי של התושב הזכאי המחייב שינוי הרשאות הגישה שלו למערכת.

17.9.3 בקשת תושב זכאי להפסיק את פעילותו במערכת, בכפוף להוראות כל דין.

17.10 המשתמשים יקבלו הרשאה במערכת להעלאת קבצי תמונה בפורמטים ספציפיים (JPEG, PNG) בלבד. לא תתאפשר העלאת כלל סוגי הקבצים ובפרט לא קבצי הרצה כגון PS1, BAT, EXE.

17.11 במקרה של הפרה של משתמש את הוראות אבטחת המידע של המערכת, לרבות הוראות תקנות אבטחת המידע ונוהלי המערכת, כפי שפורסמו למשתמשים, נותן השירותים ישעה את הרשאות הגישה של המשתמש בכפוף להוראות כל דין. נותן השירותים יודיע למשרד בכתב בהקדם האפשרי על השעיית הרשאות הגישה של המשתמש, לפי העניין, עד להשלמת בירור הנושא מול המשתמש ובתיאום עם המשרד.

18 ניהול המידע

18.1 העברת מידע אל נמען באמצעות המערכת תיעשה באופן שיבטיח כי הגישה למידע והצפייה בו תתבצע על ידי התושב הזכאי בלבד.

18.2 ניהול המידע המועבר במערכת יבוצע בהתאם להוראות תקנות אבטחת המידע, לרבות מגבלות על

הגישה למידע, מועד מחיקת המידע או פרק הזמן לשמירתו, ואופן שמירת המידע בבסיס הנתונים ובטבלאות המערכת, בהתאם לסוגי המידע השונים הכוללים לפחות את אלה:

18.2.1 פרטי זיהוי של התושב הזכאי - מספר זהות, שם פרטי, שם משפחה, תאריך לידה, מין וכתובת מגורים.

18.2.2 פרטי זיהוי אחרים המתקבלים מהמשרד.

18.3 פרטי הזיהוי של התושבים הזכאיים שהמידע אודותיהם נמצא במערכת יישמרו במאגרים מוצפנים. כל פעולה המבוצעת לגבי מידע המועבר במערכת או השמור בה תיעשה באופן שאינו מאפשר למי שאינו מורשה גישה למידע מסוים לזהות את התושב הזכאי שמידע אודותיו עובר או שמור במערכת, בזמן העברתו או במועד שמירתו.

18.4 הגישה של המערכות הממוכנות של המערכת או של עובדיה אל המידע הקיים במערכות לשם בקרה על פעולותיהן ולשם בירור מחלוקות שנתגלו בין משתמשים במערכת או לשם פיקוח המשרד, תיעשה בהרשאות קריאה בלבד, באופן שלא ניתן יהיה לבצע כל שינוי במידע.

18.5 נותן השירותים יבצע בדיקת תקינות קלט - Input Validation, בכל השדות שתושב הזכאי מתבקש להזין במערכת.

18.6 נותן השירותים יתעד כל ניסיון לפגיעה בשלמות המידע או לשימוש בו ללא הרשאה (להלן - אירוע אבטחה), באופן אוטומטי, לרבות מנגנוני התרעה על אירועי אבטחה והיקף הפגיעה באבטחת המידע השמור במערכת או המועבר בה ובפרטיות התושבים הזכאיים נשואי המידע.

18.7 במקרה של אירוע אבטחה הפוגע בשלמות המידע השמור במערכת או המועבר בה, יבצע נותן השירותים שחזור מידע בהתאם לנהלי הגיבוי וההתאוששות. המערכת תתעד כל פעולה של שחזור מידע כאמור.

18.8 שמירת נתוני תושבים זכאיים ומחיקתם:

18.8.1 כל הנתונים האישיים של התושבים הזכאיים שיתקבלו אצל נותן השירותים במסגרת מתן השירותים, יישמרו אצל נותן השירותים לצורך ההנפקה בלבד.

18.8.2 לאחר ביצוע ההנפקה בצורה מלאה, יימחקו הנתונים האישיים מבסיס הנתונים של כל מערכת שהיא של נותן השירותים.

18.8.3 יובהר כי נותן השירותים לא יותיר ברשותו כל העתק או תעתיק או צילום של נתונים אישיים של התושבים הזכאיים.

18.8.4 נותן השירותים יבער את כל הנתונים אודות התושבים הזכאיים והפרויקט והתחייבותו שלא ניתן לאחזר מידע זה במערכותיו עם סיום ההתקשרות ובהתאם לדרישת המשרד. שמירת נתוני התצלומים של התושבים הזכאיים:

18.8.4.1 התצלומים של התושבים הזכאיים נחשבים כ״מידע אישי רגיש״.

18.8.4.2 יש לשמור את התצלומים בספרית קבצים נפרדת מהנתונים האלפאנומריים

תוך מניעת גישה של משתמשים בלתי מורשים לספריה זאת.

18.8.5 שמות הקבצים שיישמרו על ידי נותן השירותים לא ייכללו את מספרי הזהות של התושבים הזכאיים אלא מספר מזהה אחר שייקבע, כגון – מספר התעודה או מספר פיקטיבי אחר שיקושר בצורה מאובטחת לפרטי בעל התעודה, כפי שייקבע על ידי המשרד בתיאום עם נותן השירותים במסגרת שלב העיצוב. הקבצים המקוריים יגיעו עם מפתח של מספר הזהות. המדובר במענה טכני להגנה על הפרטיות המקובל במאגרים ביומטריים.

18.8.6 התצלומים יימחקו יחד עם יתר נתוני התושבים הזכאיים כאמור לעיל, לאחר קבלת אישור מהממשק על לקליטת הנתונים אודות ההנפקה והמשלוח במשרד.

18.8.7 הנתונים יתקבלו בכל מקרה מהמשרד ויועברו לנותן השירותים בממשק מתאים, בין אם אלו יהיו תמונות ממאגר ממשלתי כלשהו או מצילום עצמי.

18.9 שמירת נתונים מינהליים לצורך בקרה:

מבלי לגרוע מכלליות האמור לעיל, וגם לאחר מחיקת הנתונים האישיים, נותן השירותים ישמור נתוני בקרה כלליים בדבר הנפקת תעודות אזרחים ותיקים במהלך תקופת ההסכם, כמפורט להלן, וזאת עד 90 יום לאחר תום תקופת ההתקשרות:

18.9.1 מועדי קליטת קבצי נתונים מגורמים חיצוניים לרבות המשרד.

18.9.2 נתוני מנות הנפקת תעודות הכוללים את מספרי התעודות, מועד המשלוח וסטטוס התעודות.

18.9.3 נתוני תעודות שבוטלו.

19 אבטחת מידע במערכת

19.1 הגנה על התקשורת

19.1.1 נותן השירותים יישם מידור בין החלקים השונים ברשת באמצעות חלוקה לוגית או פיזית של הרשת והגבלת אפשרות הקישור בין הרשתות השונות. רמת המידור תיקבע בהתאם לרגישות הנתונים המנוהלים במערכות. המידור יתבצע באמצעות Firewall.

19.1.2 נותן השירותים יבצע הפרדה מוחלטת של רשתות אלחוטיות מרשת הייצור שלו. לחלופין וככל שלא מדובר ברשת אלחוטית לשירות אורחיו, נותן השירותים יישם מנגנונים מספקים לאבטחת רשתות אלחוטיות, לרבות הצפנה, הזדהות חזקה, מניעת התקפות על הרשת ומניעה של התחברות גורמים או ציודים בלתי מורשים לרשת האלחוטית.

19.1.3 נותן השירותים ישתמש באמצעי הגנת סייבר המתאימים לסיכוני גישה לאינטרנט מרשת נותן השירותים, כגון אמצעי סינון תקשורת ותוכן, סינון אפליקציות, אנטי וירוס, sandbox, אמצעי ניטור הגנת סייבר ותהליכי בקרה. האמצעים יותאמו לסיכונים ייחודיים לשירותי רשת שונים, כגון DNS, שירותי העברת קבצים, שירותי Web, שירותי דואר אלקטרוני, ועוד.

19.1.4 נותן השירותים יגדיר אמצעי אבטחה מוגברים כגון: שימוש בהזדהות חזקה, הצפנה מקצה לקצה וניטור בגישה מרחוק לרשת נותן השירותים, בדיקת התאמה למדיניות, על גבי תשתית תקשורת ציבורית או מנקודות קצה שאינן מאובטחות דיין.

19.2 **הצפנה וחתימה**

19.2.1 נותן השירותים אחראי להצפנת המידע, הן המידע שבתנועה והן המידע שבמנוחה.

19.2.2 ההצפנה תבוצע בפרוטוקולים סטנדרטיים בלבד. ההצפנה תתבצע על המידע הרגיש הנשמר במערכת או מועבר בין הממשקים החיצוניים והפנימיים, לרבות העברה ברשת תקשורת אלחוטית, רשת ציבורית או באינטרנט.

19.2.3 ההצפנה תתמוך ב- SSL/TLS Public Key Encryption 2048+ Bit SHA2 ובכל סוגי הדפדפנים.

19.2.4 נותן השירותים יגדיר נהלים ומנגנונים מתאימים ליצירה, התקנה, אחסון ושמירה על מפתחות הצפנה הרלוונטיים לפעילות, הנהלים והמנגנונים יתייחסו לרכיבים הבאים:

19.2.4.1 הגנה על המפתחות מפני פעולות או שימוש בלתי מורשים, הכוללים בין היתר: שינוי, החלפה, החדרה ומחיקה של המפתחות.

19.2.4.2 מניעת גילוי בלתי מורשה של התכנים הלא-ציבוריים של המפתחות.

19.2.4.3 לספק אינדיקציות למצב התפעולי של המפתחות כדי להבטיח פעולה תקינה שלהם.

19.2.4.4 איתור שגיאות בתפעול המפתחות ומניעת זליגה של נתונים רגישים ופרמטרי אבטחה קריטיים כתוצאה משגיאות אלה.

19.2.4.5 בקרה בזמן אמת על כל שינוי, פעולה המבוצעת על המפתחות.

19.2.5 המערכת תאפשר בעתיד התממשקות ב- API למנגנון תקני לחתימה אלקטרונית לצורך מניעת התכחשות של פעולות שהתושב הזכאי יוכל לבצע.

19.2.6 ככל שיידרש ביצוע חתימה אלקטרונית על ידי התושב הזכאי, היא תתבסס על התקנים המקובלים בתחום זה. ככל שתידרש חתימה אלקטרונית מאושרת היא תתבצע על ידי גורמים מאשרים לפי סעיף 9(ב) לחוק חתימה אלקטרונית).

19.3 **תיעוד (לוגים)**

19.3.1 המערכת תתעד כל ניסיון גישה אל המערכת ובסיסי הנתונים, גם אם כשל, וכל גישה בפועל באופן אוטומטי, כך שניתן יהיה להתחקות אחר מסלול הגישה, סוג הגישה ורכיבי המערכת והמידע אליהם בוצעה הגישה, לרבות טבלאות בסיס הנתונים.

19.3.2 המערכת תמנע, ככל הניתן, את האפשרות להפסיק את פעילות מנגנון התיעוד כאמור בסעיף זה, או צמצום פעילותו, ולהתריע בפני מנהלי המערכת על הפסקת פעילות או צמצום פעילות מנגנון תיעוד זה.

19.3.3 מנגנון התיעוד (הלוג) יתייחס לכל הפחות למבצע הפעולה, הפעולה שבוצעה, המקום ממנו בוצעה הפעולה, תאריך ושעת ביצוע הפעולה במדויק, האם הגישה אושרה או נדחתה, רכיב המערכת שאליו נעשה ניסיון הגישה וככל שהגישה אושרה גם היקף הפעולה.

19.3.4 נתוני הרישום של מנגנון התיעוד (לוגים) יישמרו למשך שנתיים לפחות ויהיו מוגנים מפני מחיקה או שינוי בלתי מורשה.

19.4 **שמירת עדכניות המערכות**

19.4.1 נותן השירותים יגדיר תהליכי עדכון מבוקרים למערכות ולתשתיות, תוך התייחסות למקוריות קבצי העדכון, בדיקת עדכונים בטרם יישומם ושמירה על יציבות מערכות בתהליך העדכון.

19.4.2 נותן השירותים יישם עדכוני אבטחת מידע שוטפים למערכות ולתשתיות באופן תקופתי, יעקוב באופן תדיר אחר פרסום עדכוני אבטחת מידע למערכותיו ולתשתיותיו ויישם עדכונים קריטיים בהקדם האפשרי.

19.4.3 נותן השירותים יימנע מלהחזיק מערכות אשר סובלות מחוסר עדכניות או היעדר תמיכה ויפעל להחליפם לפני מועד סיום התמיכה.

19.5 **אבטחת מערכות**

19.5.1 נותן השירותים יתקין אמצעי הגנה נאותים מפני חדירה לא מורשית למערכת, הכנסת רכיבים לא מורשים או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב.

19.5.2 נותן השירותים יפריד את המערכת הטכנולוגית המשמשת את המערכת לשם ניהול המידע השמור במערכת או המועבר בה, ממערכות טכנולוגיות אחרות המשמשות אותו.

19.5.3 נותן השירותים יתקין אמצעי הגנה למניעת זליגת מידע (DLP) מהמערכת ובקרה אחר המידע היוצא מהמערכות ומרשת המחשוב.

19.5.4 נותן השירותים יפעל להקשחת המערכות ולהעלאת רמת האבטחה שלהם. המערכת תוכל להתממשק ולפעול עם מוצרי הקשחה חיצוניים.

19.5.5 נותן השירותים יישם אמצעי הגנה על שרתים ומערכות קצה, תוך התחשבות בסיכוני הפעלת קוד עוין, סיכוני Zero day וסיכוני חדירה למערכות.

19.5.6 נותן השירותים יישם הצפנת מידע רגיש במערכות קצה ניידות (כגון מידע הנמצא על מחשבים ניידים, טאבלטים, התקני אחסון ניידים וטלפונים ניידים).

19.5.7 נותן השירותים יטמיע אמצעי אבטחה למניעת חדירה והתפשטות קוד עוין במערכותיו, שייכללו מספר שכבות אבטחה כגון: סינון תקשורת וקבצים נכנסים, סריקת מערכות קבצים, הגנה בזמן אמת על שרתים או תחנות קצה, מערכות אנומליה, מערכת טיפול בסיסמת local administrator ומערכות ניטור ומניעה ייעודיות.

19.5.8 בעת חיבור אמצעי מדיה למערכות מידע יעשה שימוש במנגנוני הגנה אפקטיביים המונעים

חדירת קוד עוין, כגון שימוש במערכות "הלבנת קבצים".

20 פיתוח היישום והיישומון

20.1 נותן השירותים יעשה שימוש במתודולוגיית פיתוח והקמה העומדות בתקני אבטחת מידע מקובלים ובהוראות אבטחת המידע לפי פרק זה.

20.2 על נותן השירותים להבטיח כי הפיתוח יתבצע בהתאם לנוהלי פיתוח מאובטח ובעמידה בבקרות OWASP.

20.3 על נותן השירותים ליישם בתהליכי הפיתוח את עקרונות העיצוב להגנה על הפרטיות.

20.4 אם נותן השירותים משתמש בקוד פתוח, נותן השירותים יתאר את מקור הקוד הפתוח, בדיקות אבטחת המידע שנעשו בקוד הפתוח, העמידה בדרישות המכרז ואי קיום הגבלות לגבי השימוש והרישוי בו.

20.5 על נותן השירותים להתאים את המערכת לשימוש בגרסאות הכי מעודכנות של מערכות ההפעלה הן בשרתים והן בנקודות הקצה. כמו כן נותן השירותים יכפה על נקודות הקצה להוריד את הגרסה העדכנית של המערכת מחנויות היישומונים.

20.6 לא תתאפשר הורדה למכשירים פרוצים, התקנת היישומון תתבצע רק מחנויות היישומונים: Google Play ו-AppStore. ליישומון יתבצע תהליך Obfuscation.

20.7 יש להגדיר ביישומון מנגנון Anti-Hooking.

20.8 בעת סגירת היישומון יתבצע ניקוי מידע רגיש מזיכרון ה- CACHE.

20.9 כל נתון / קובץ רגיש שהועלה / נמצא ביישומון יישמר באזור מאובטח ויהיה נגיש אך ורק באמצעות היישומון.

20.10 לא יוצג מידע רגיש / מידע החושף פרטים על המערכת למשתמש הקצה בהודעות השגיאה.

20.11 פיתוח ממשקים (API)

20.11.1 על נותן השירותים לעמוד בסטנדרטים מקובלים של API (OAuth2) המתייחסים להזדהות, להרשאות, לתקשורת מוצפנת וממשק מאובטח ומאומת.

20.11.2 ההגנה תתבצע הן ברמת ה-Transport והן ברמת ה- Messages.

20.11.3 הצפנת התווך בפרוטוקול TLS1.2 ומעלה.

20.11.4 נותן השירותים יבצע בדיקת מניעת הונאה וזיוף על גבי הממשק.

20.11.5 שליחת מידע רגיש מהיישומון לשרת תבוצע באמצעות הודעות POST ככל הניתן.

21 שימוש בשירותי מיקור חוץ

21.1 נותן השירותים יגדיר נוהל לדרישות הגנת סייבר ביחס לסיכוני מיקור חוץ וביחס לאבטחת שרשרת האספקה. נוהל זה יושם בעת התקשרות עם גורם מיקור חוץ חדש.

21.2 במסגרת הסכם התקשרות עם קבלת שירותי מיקור חוץ:

21.2.1 נותן השירותים יחייב את הצד השלישי לשמירת סודיות מוחלטת.

21.2.2 ייאסר על נותן השירותים להעביר לצד שלישי מידע שקיבל במסגרת ההתקשרות, או להשתמש במידע שאליו נחשף אגב ביצוע ההתקשרות, לכל מטרה אחרת שלא קשורה לביצוע ההתקשרות.

21.2.3 בעת הצורך בהעברת נתונים יבוצע תהליך של גישה מבוקרת לנתונים פרטניים לצורך מתן השירות.

21.2.4 במידת הצורך תידרש עמידה של ספק מיקור החוץ בתקן ת״י ISO 27001 ומילוי הבקרות הנדרשות במערכת יובל של מערך הסייבר.

22 שירותי מחשוב ענן

22.1 בטרם הפעלת שימוש במערכות מבוססות ענן, על נותן השירותים לבצע הערכת סיכונים ייעודית, לדון בנושא עם נציגי המשרד ולקבל את אישורו.

22.2 באם נותן השירותים יבחר להשתמש במחשוב ענן, עליו להשתמש בתשתיות אמזון או גוגל בלבד(תשתיות נימבוס). תחילה המערכת תוצב באזור הזמני בחו״ל – אזור אירלנד עבור אמזון ואזור אמסטרדם (אפשר גם פרנקפורט) עבור גוגל. לאחר שהאזור הישראלי של תשתית נימבוס יוקם נותן השירותים יידרש להעביר את המערכות שהקים לאיזור הישראלי, על חשבונו.

22.3 נותן השירותים לא יאחסן מידע רגיש או נתוני תושבים זכאיים בענן מחוץ לגבולות מדינת ישראל, אלא אם בדק ווידא שספק הענן מקיים את רמת ההגנה בהתאם לתקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס״א-2001 ולדירקטיבה על הגנת המידע במדינות האיחוד האירופי.

22.4 כל התנאים והדרישות הכתובים בנספח זה יחולו גם על מערכת הענן (הצפנות, סיסמאות, MFA, הרשאות, WAF, IPS, Firewall וכו׳.

22.5 הנתונים יאוחסנו במערכת שהינה בשימוש בלעדי של נותן השירותים/המשרד (Single tenant), נותן השירותים יעשה שימוש בטכנולוגיות כגון הצפנה, מיסוך נתונים או טוקניזציה, במטרה למנוע חשיפה של מידע רגיש או נתוני תושבים זכאיים לגורמים שאינם מורשים.

22.6 נותן השירותים יכלול בהסכם ההתקשרות עם ספק מחשוב הענן, יכולת שליטה ובקרה שלו על המידע הנמצא בהחזקת ספק מחשוב הענן וכן אפשרות חד צדדית להפסקת השימוש בשירותי ספק מחשוב הענן תוך מחיקת המידע ממערכותיו והתחייבותו שלא ניתן לאחזר מידע זה במערכותיו.

23 ביטוח סייבר

23.1 נותן השירותים יפעל להקמת פוליסת ביטוח מפני מתקפות ואירועי סייבר בהתאם להיקף העבודה ולכמות המועסקים על ידו.

23.2 הביטוח יכסה מתקפות מסוג מניעת שירות ודלף מידע, כאשר הדגש העיקרי יינתן על מידע מזוהה אישי השייך לתושבים הזכאיים