מדיניות אבטחת מידע והגנת הסייבר ברשות מקרקעי ישראל

תוכן

1. כללי 4
1.1. יעדי הגנת הסייבר ברשות מקרקעי ישראל 4
1.2. מטרת המדיניות 4
1.3. תחולה 4
1.4. המעבר מאבטחת מידע להגנת סייבר 4
1.5. עקרונות אבטחת המידע והגנת הסייבר ברשות מקרקעי ישראל 5
1.6. תהליך ההגבה המחזורי 6
2. התאמה ותאימות 6
2.1. אסדרה (Regulation) ותקנים 6
2.2. המבנה הארגוני של אבטחת המידע והגנת הסייבר ברשות מקרקעי ישראל 6
2.3. תאימות 6
3. מיפוי, ניהול וסיווג נכסי המידע 7
3.1. ניהול המידע 7
3.2. מערך הסיווג 7
3.3. סיווג המערכות הקריטיות 7
3.4. מדידת הבזק 7
3.5. קריטיות המערכות ברשות מקרקעי ישראל 7
4. אבטחה פיזית וסביבתית 7
5. משאבי אנוש 8
6. טיפול באירועי אבטחת המידע והגנת הסייבר 8
7. תשתיות ותקשורת 8
7.1. הגבה לוגית 8
7.2. אמצעי הבקרה 10
7.3. סקרי אבטחת מידע 10
8. פיתוח מאובטח 10
9. המשכיות עסקית 11
10. שינוי המדיניות 11
10.1. חריגה מהמדיניות 11
נספח א' - סוגי תוקפים 12
נספח ב'- שרשרת התקיפה בסייבר (Cyber Kill Chain) 14
נספח ג' – גופים מנחים ותקנים מחייבים 15
נספח ד' – המבנה הארגוני של אבטחת המידע והגנת הסייבר ברשות 17
נספח ה' – פרוט רמות הסיווג 19

נספח ו' – פירוט קריטריונים לסיווג קריטיות של מערכת 19

נספח ז' – קריטריונים למדידת תוחלת הנזק 21

נספח ח' – מערכות קריטיות ברשות מקרקעי ישראל 22

נספח ט' – פירוט תפיסת האבטחה הפיזית והסביבתית 24

נספח י' – תהליכים להגנת הסייבר בהיבט האנושי 26

נספח יא' – הגדרות ומושגים 28

1. כללי

1.1. יעדי הגנת הסייבר ברשות מקרקעי ישראל

רשות מקרקעי ישראל (להלן "הרשות") מנהלת כמות גדולה של מידע בעל רגישות בתחומים שונים: מכרזים, נתונים כספיים, מידע אישי רגיש של עובדים ואזרחים, נתונים טכנולוגיים ועוד. מידע זה חיוני לפעילותה של הרשות כגוף ממשלתי, כאשר פגיעה בשלמות, בזמינות ובסודיות המידע כמו גם במערכות המעבדות ומנהלות אותו, יכולה לפגוע באופן משמעותי ברשות, בממשלת ישראל, בעובדי הרשות ובאזרחי המדינה.

העקרונות המנחים במדיניות להגנת הסייבר ברשות מהווים בסיס לנהלי העבודה בתחום הגנת הסייבר, ונגזרים מחוקים, תקנות, ת"י ISO 27001 ומתורת ההגנה של הרשות הלאומית להגנת הסייבר, תוך שמירה על עקרונות היחידה להגנת הסייבר בממשלה, שימוש במשאבים הקיימים ועמידה בהנחיות.

היעד המרכזי של תחום אבטחת המידע והגנת הסייבר ברשות מקרקעי ישראל הוא הגנה מיטבית על המידע הקיים במאגרי הרשות ומנוהל על ידה, בין אם בעותקים קשיחים ובין אם במערכות המידע (להלן "נכסי מידע") שברשות, וזאת על מנת לאפשר המשכיות עסקית מאובטחת.

1.2. מטרת המדיניות

מסמך מדיניות אבטחת המידע והגנת הסייבר ברשות מקרקעי ישראל יגדיר את:

1.2.1. תפיסת אבטחת המידע ברשות ואת העקרונות והדרכים ליישם אותה.
1.2.2. מסגרת העבודה לתהליכי הגנת הסייבר ברשות ולנהלים לפיהם יתקיימו תהליכים אלה.

1.3. תחולה

מדיניות אבטחת המידע והגנת הסייבר ברשות מקרקעי ישראל תחול על כל אדם ומערכת בעלי גישה לנכסי המידע ברשות: עובדים קבועים, עובדים זמניים, יועצים, עובדי בתי תוכנה, מתנדבים ומנהלים. המדיניות חלה על כל מערכות המידע ברשות, בין שהמידע המעובד מאוחסן בתוכן ובין שהוא עובר דרכן.

1.4. המעבר מאבטחת מידע להגנת סייבר

אבטחת מידע מתייחסת לאיומים סטנדרטיים מגורמים מאיימים כגון עובד פנימי, פצחן (Hacker) רגיל וכו'. לעומת זאת, בעולם הסייבר איום הייחוס שלנו הוא ממשלות, גופי ביון, גופי פשיעה בלוחמת רשת (Cybernetics) (ראה נספח א') – אשר לכולם יכולות טכנולוגיות גבוהות ויכולות מימון גבוהות, מה שמגביר את התחכום וההשקעה במתקפות ודורש במקביל היערכות ברמה אחרת. רשות מקרקעי ישראל, כסמל שלטון של מדינת ישראל, מהווה יעד תקיפה פוטנציאלי ולכן על הרשות להיות מוכנה ככל הניתן לעמוד כנגד ניסיונות אלו, וזאת לאור המגבלות האובייקטיביות הקיימות בממשל זמין.

בניגוד לתפיסת אבטחת המידע המסורתית, תפיסת הגנת הסייבר מתאפיינת בשני היבטים עיקריים:

1.4.1. **התוקף כבר בפנים:** הבנה שהתוקף נמצא כבר בתוך הרשת ותפקיד צוותי הגנת הסייבר הוא להקשות עליו את תהליך התקיפה ככל האפשר, למזער את היכולת שלו לבצע פעולות זדוניות במערכות המידע ולנהל את התוצאות של תקיפה מוצלחת.

1.4.2. **הרחבת תפיסת ההגנה:** הגנת סייבר היא יותר מאבטחת מידע. היא עוסקת בתחום אבטחת המידע אך כוללת גם אבטחה פיזית, המשכיות עסקית ועוד, מכיוון שהתקפת סייבר לא חייבת להגיע דרך האינטרנט (פגיעה במערכת הקירור של חדר השרתים למשל תשבית את מערכות המידע באותו חדר). זאת ועוד, הגנת הסייבר לא מוגבלת לתחום גיאוגרפי מסוים כיוון שמקורות התקיפה מגוונים.

1.5. עקרונות אבטחת המידע והגנת הסייבר ברשות מקרקעי ישראל

1.5.1. הארגון כמכלול

העיקרון הראשי של תפיסת ההגנה הינו "הארגון כמכלול", כלומר ההכרה בכך שנדרש להגן על התפקוד העסקי של רשות מקרקעי ישראל ולתמוך ביעדיה העסקיים. הגנה זו תתבצע על ידי בחינת התהליכים העסקיים והטכנולוגיים לפי שלוש אפשרויות פגיעה בנכסי המידע שברשות (מודל CIA):

א. **חיסיון המידע** (Confidentiality): פגיעה בחיסיון המידע יכולה לחשוף מידע רגיש מבחינה עסקית או מבחינת צנעת הפרט של עובדי הרשות או לקוחותיה.

ב. **אמינות המידע** (Integrity): פגיעה באמינותו של המידע בשימוש הרשות עלולה להוביל לפגיעה משמעותית בתהליכים העסקיים ברשות מקרקעי ישראל.

ג. **זמינות המידע** (Availability): פגיעה בזמינות המידע ומערכות המידע עלולה להשבית חלקים נרחבים מהפעילות של הרשות והשירות שהיא נותנת ללקוחותיה.

1.5.2. אחריות הנהלה

האחריות להגנה על המידע מוטלת על ההנהלה, וזאת על פי עקרונות ומדיניות הרשות להגנת הסייבר בממשלה. האחריות העיקרית למימוש מדיניות זו, תחול על ועדת ההיגוי לנושא הגנת הסייבר. וכמו כן, תחול על מנהלי הנכסים, מנהלי המאגרים ועל כל עובד ברשות.

ועדת ההיגוי תתכנס אחת לשנה בראשות מנהל רשות מקרקעי ישראל ובהשתתפות החברים שנקבעו בכתב המינוי. הועדה תיזום סקרי הנהלה, תוודא ישימות של מסמך המדיניות והנהלים, תגבש מדדים כמותיים לבחינת אפקטיביות נהלי ההגנה בסייבר, תתקצב את כלל הפעילות השוטפת בתחום ההגנה בסייבר ותהווה ממשק בין הנחיות הממשלה ליישומן ברשות ולהפך.

1.5.3. הגנה בהתאם לפוטנציאל הנזק

ההשקעה בהגנה על כל נכס תהיה בהתאם לרמת החשיבות שלו לתפקוד הרשות.

1.5.4. הגנה מבוססת ידע וניסיון

ההשקעה בהגנה מבוססת על בסיס ידע של חברות ייעוץ מתמחות בתחום, רשות התקשוב הממשלתי - היחידה להגנת הסייבר (יה"ב), ה-SOC (Security Operations Center) הממשלתי, אירועי אבטחת מידע שאירעו בעבר באגף ומחוצה לו, ביצוע ביקורות ברשות והערכות מודיעין המתבצעות באופן שוטף ע"י הגופים הממשלתיים, וזאת על מנת ליצור מיקוד ספציפי במעגלי ההגנה השונים.

1.5.5. הגנה פעילה (Proactive)

ההגנה על הרשות מחייבת להשקיע מאמצים בנוסף על ההגנה הסבילה (Passive) המסורתית. הדבר בא לידי ביטוי לדוגמא באמצעות הגדרת בקרות הגנה עבור שלבי המניעה, בדיקות חדירה יזומות, מעבר יזום על לוגים וניטור, זיהוי ותגובה.

1.5.6. הגנה רב שכבתית

העיקרון של הגנה רב שכבתית הוא ליצור מנגנוני אבטחה מרובדים על מנת להגביר את האבטחה של המערכת כולה. כך למשל, אם תקיפה גורמת למנגנון אבטחה אחד להיכשל, מנגנונים אחרים עשויים עדיין לספק את הביטחון הדרוש כדי להגן על המערכת.

הגנה היא תהליך המשלב שלושה מרכיבים עיקריים: אנשים, טכנולוגיה ותהליכים. בקרות ההגנה נדרשות על מנת לספק מענה הגנתי בכל הרבדים הללו.

1.6. תהליך ההגנה המחזורי

תהליך ההגנה הוא תהליך מחזורי הכולל שלושה שלבים עיקריים:

1.6.1. תכנון והערכה

מיפוי יעדי הגנת המידע ברשות, הערכת סיכונים, בחינת אמצעי ההגנה והבקרות הקיימים ובניית תוכנית עבודה לסגירת פערי הגנה.

1.6.2. ביצוע תוכנית העבודה

ביצוע התוכנית על ידי בניית תהליכים ארגוניים, הטמעת כלים והטמעה ארגונית של הגנת המידע לרשות.

1.6.3. שמירה על עדכניות הגנת המידע

התהליכים והטכנולוגיות המוטמעים משתנים כל הזמן: מחשבים ורשתות חדשים מותקנים, תוכנות מתקדמות נרכשות, רכיבים חדשים מקושרים למרחב הסייבר כגון Internet Of Things, מוצעים שירותים חדשים (כגון מחשוב ענן) ועוד. מנגד, גם האיומים ושיטות התקיפה האפשריות משתנים ובהתאמה, גם כלי ההגנה. לכן יש צורך להתעדכן על בסיס שוטף ולהטמיע כלים ושיטות עדכניות להגנה על המידע ברשות.

2. התאמה ותאימות

2.1. אסדרה (Regulation) ותקנים

רשות מקרקעי ישראל כפופה לאסדרה מתוקף חוקים והחלטות ממשלה רלוונטיות. באחריות מנהל הרשות, האגף המשפטי ותחום אבטחת המידע והגנת הסייבר ברשות, לאכוף את האסדרה של הגורמים אליהם כפופה הרשות, לרכז את דרישות ההגנה בסייבר, לעדכן בשינויים חוקתיים, לתת מענה לתביעות, לרכז ולתחקר אירועי אבטחת מידע, לסייע ברמה המשפטית, וכל זאת על מנת לוודא עמידה בהנחיות אותן נדרשת הרשות לקיים (ראו נספח ג' – פירוט אסדרה ותקנים).

2.2. המבנה הארגוני של אבטחת המידע והגנת הסייבר ברשות מקרקעי ישראל

המבנה הארגוני של אבטחת המידע והגנת הסייבר ברשות מקרקעי ישראל מיועד להבטיח ניהול תקין ויעיל של מאמצי אבטחת המידע והגנת הסייבר ברשות מקרקעי ישראל, תוך מתן אפשרות לרציפות הפעילות העסקית של הרשות וקידום השגת היעדים העסקיים (ראו נספח ד' - מבנה ארגוני של הגנת הסייבר ברשות)

2.3. תאימות

נהלי אבטחת המידע ברשות מקרקעי ישראל נכתבו על פי הנחיות ומדיניות יחידת הסייבר בממשלה ועומדים בתאימות לייעוד ולתכנים הנדרשים.

3. מיפוי, ניהול וסיווג נכסי המידע

3.1. ניהול המידע

כלל נכסי המידע של הרשות מנוהלים ומתועדים. רשימת נכסי הארגון כוללת בין השאר את שם "בעל" הנכס ורמת הקריטיות שלו. בעל הנכס יישא באחריות הכוללת להגנה על הנכס ברמה הנדרשת.

3.2. מערך הסיווג

המידע ברשות מקרקעי ישראל מתחלק לארבע קבוצות - כללי, פנימי, חסוי, חסוי ביותר. קבוצות אלו משקפות את רמת הסיכון בפגיעה בכל מערכת מידע / מאגר מידע וכן את המשאבים הנחוצים להגנה על מערכות אלה. רמת הסיווג תיקבע ע"י מפיק המידע או בעלי המידע, וזאת בהתאם לרמת הסיווג הגבוהה הקיימת באותו מסמך/ מאגר, וזאת ע"פ הנחיות היחידה להגנת הסייבר בממשלה (יה"ב) (ראו נספח ה' - פרוט רמות הסיווג)

3.3. סיווג המערכות הקריטיות

רשות מקרקעי ישראל אינה מוגדרת כ"קריטית" על ידי הרשויות הממונות על הגדרות אלה (רשות החירום הלאומית, הרשות הממלכתית לאבטחת מידע בשירות הביטחון הכללי, המטה לביטחון לאומי ורשות הסייבר), והצפי הוא שבזמן חירום / מלחמה, הרשות תשעה את עבודתה עד חלוף זמן החרום. מכאן שחשיבות המערכות נובעת מאחד או יותר מהקריטריונים הבאים: שכיחות השימוש, הרגישות העסקית וצנעת הפרט (לפירוט הקריטריונים, ראו נספח ו' - פירוט קריטריונים לסיווג קריטיות של מערכת)

3.4. מדידת הנזק

מדידת הנזק תתבצע לפי **סוג** הנזק ו**תוחלת** הנזק.
את סוג הנזק הצפוי מפגיעה במערכת מידע אנו מחלקים לשלושה סוגים לפי מודל משולש ה-CIA - חסיון Confidentiality, אמינות Integrity, זמינות Availability, כפי שצוין בסעיפים הקודמים.
תוחלת הנזק היא הערכת הנזק בשקלול הסיכוי להתרחשותו.
הצירוף של סוג הנזק ותוחלת הזנק מהווה במדד להערכת הסיכון הנובע מפגיעה במערכת מידע כלשהי, ומכאן גם שהוא הבסיס לסיווג מידע ומערכות מידע בארגון.
חשוב לציין כי עלות המשאבים המושקעים בהגנה על מערכת מסוימת לא יעלו על תוחלת הנזק שחושבה.
(לקריטריונים למדידת תוחלת הנזק, ראו נספח ז' - קריטריונים למדידת תוחלת הנזק)

3.5. קריטיות המערכות ברשות מקרקעי ישראל

קריטיות המערכות נבחנה על פי כל אחד מהקריטריונים שהוגדרו ולפי רמת הסיכון אליה המערכת חשופה (לרשימת המערכות שזוהו כקריטיות ראו נספח ח' - מערכות קריטיות ברשות מקרקעי ישראל)

4. אבטחה פיזית וסביבתית

אבטחה פיזית וסביבתית נדרשת כאשר הגישה למתחם עלולה לטמון בחובה אפשרות לנזק לרשות מקרקעי ישראל. תפיסת האבטחה מתייחסת לאפשרות של גישה פיזית לסביבת העבודה של בעלי התפקידים בארגון, אל תחנות העבודה או למרכזי התקשורת והמחשוב. (לפירוט ראו נספח ט' - פירוט תפיסת האבטחה הפיזית והסביבתית)

מתחמים רגישים – מעגלי האבטחה מותאמים למתחמים השונים באגף מערכות המידע והמחשוב בפרט ובמתחמי רשות מקרקעי ישראל הפרושים ברחבי הארץ בכלל. מתחמים אלו יוגדרו רגישים, אם מערכות המידע או המידע

(מידע פיזי הכולל מסמכים, התקנים ניידים, דיסקים ועוד) הנמצאים בהם מוגדרים כקריטיים, או שבאמצעותם ניתן להגיע למערכות מידע המוגדרות כקריטיות. לכל מתחם רגיש יותאם מעגל אבטחה בהתאם לרמת הסיכון הנשקפת מחדירה אליו ולגישה של תוקף למידע הנמצא בו.

הממונה על הגנת הסייבר יקבע את מדיניות הרשאות הגישה על פי מעגלי האבטחה השונים, וזאת בשיתוף פעולה עם מנהל אגף הביטחון הארצי (המנב"ט).

5. משאבי אנוש

הגורם האנושי הוא מרכיב קריטי בהגנה על נכסי המידע של רשות מקרקעי ישראל מפני סכנות אבטחת המידע והסייבר. לעובדים ולבעלי התפקידים (להלן המשתמשים) ברשות מקרקעי ישראל נוכחות בתחומי העיסוק של הרשות והם בעלי גישה למערכות המידע. למצב זה יש להתייחס בשני היבטים:

- ✓ העלאת המודעות בקרב המשתמשים ברשות וההסתייעות בגורם האנושי כמכפיל כוח למאמצי אבטחת המידע והגנת הסייבר ברשות.
- ✓ פיקוח ואכיפה על כלל המשתמשים , על מנת לעצור התקפות סייבר פנימיות על ידי גורם פנימי עוין או בעל מודעות נמוכה.

התהליכים המומלצים לצמצום הסיכונים בהיבט האנושי מפורטים בנספח י' - תהליכים להגנת הסייבר בהיבט האנושי.

6. טיפול באירועי אבטחת המידע והגנת הסייבר

- ✓ הטיפול באירועי אבטחת המידע והגנת הסייבר יהיה מהיר, יסודי ומקצועי.
- ✓ האירוע יטופל על ידי הצוות המתאים לחומרת האירוע ולמורכבותו.
- ✓ הטיפול יתועד בתחקירים אשר יכילו את הסעיפים העיקריים הבאים:
  - ממצאים (עובדות לאחר תשאול הגורמים הרלוונטיים)
  - משמעויות ונזקים
  - נזק עתידי/פוטנציאלי נוסף
  - השלכות האירוע (טווח בינוני וארוך)
  - מסקנות והנחיות לסגירת פערים

(לניהול אירוע הגנת סייבר, ראו נוהל א16 בקובץ נוהלי ISO - ניהול אירועי אבטחת מידע והגנת הסייבר, ובהתאמה לסעיף 8.5 בהנחיית יה"ב 5.2)

7. תשתיות ותקשורת

7.1. הגנה לוגית

7.1.1. זיהוי וניהול הרשאות ומשתמשים

מערכת IDM (Identity management) לניהול ההרשאות ולניהול הזהויות תוטמע ותיושם בארגון על מנת לקבע ולבקר את הרשאות התפעול של כל משתמש למינימום ההכרחי לביצוע עבודתו.

יצירת שכבות הגנה אלו עשויה להקשות על חוליות המגע וההתקפה (ראו נספח ב' - שרשרת התקיפה בסייבר) כאשר הטמעה נכונה שלהן תהפוך את התנועה של התוקף ברשת לקשה מאוד ואת פעולותיו למוגבלות ביותר.

נושא ניהול הרשאות הגישה ברשות מפורט בנוהל א9 "נוהל בקרת גישה".

7.1.2. חלוקה למקטעים (סגמנטציה) והצפנה של הרשת

רשת הארגון תחולק למקטעים על פי הצורך העסקי ואבטחתי כגון Network Firewall, Network - NAC Access Control ועוד. כמו-כן תבוצע הצפנה של כל קווי התקשורת בין כל אתרי הרשות. פעילות זו נדרשת בכדי להקשות באופן מהותי על חדירת התוקף לרשת, על ביצוע פעולות בתוך הרשת ועל היכולת של התוקף לנוע בין התחנות. שכבה זו גם היא מגנה על חוליות המגע וההתקפה. (ראו נספח ב' - שרשרת התקיפה בסייבר)

7.1.3. תמיכה בתשתיות ענן

רשות מקרקעי ישראל משתמשת ואף עתידה להרחיב השימוש בתשתיות ענן ציבורי או פרטי/ממשלתי לקידום צרכיה העסקיים ולשיפור מתן השירותים לאזרח. שירותי הענן נוחים וידידותיים למשתמש, ובה בעת עלולים להוות פרצה בהיבטי אבטחת המידע, ולכן השימוש בשירותי ענן יהיה על פי הנחיית יחידת הגנה בסייבר (יה"ב) שמספרה 5.5 - אבטחת מידע למעבר לענן ציבורי.

7.1.4. איחוד קובצי תבניות (Images) והקשחת תחנות קצה

יצירת קובץ תבנית (Image) אחד אחוד לכל אחת מהקבוצות התפעוליות - כללי, מפתחים, ניידים ומפקחים - ויצירת מנגנון מעקב אחר שחרורי גרסאות מערכת הפעלה תקופתיות. מערכת הפעלה מוקשחת ומעודכנת היא אחד הכלים החזקים ביותר לעצירת התקפת סייבר. שכבה זו מסייעת בהגנה על הרשת מפני אפשרויות חימוש, העברה, ניצול, התקנה, תקשורת ועוד.

7.1.5. Bring Your Own Device - BYOD

עובדי רשות מקרקעי ישראל, כמו גם ספקים ואורחים, בכפוף להרשאות, מתחברים לרשתות המחשוב של רשות מקרקעי ישראל באמצעות רשת אלחוטית WiFi, גישה מרחוק, שירותי Exchange סלולריים ועוד. גם בסביבות אלה, שנמצאות מחוץ ובמקביל לרשת ה-LAN הארגונית, קיימות סכנות סייבר לארגון ויש לנהל אותן באמצעות טכנולוגיה מתאימה (AW - AirWatch, ניהול ואבטחת רשתות, Network Access Control - NAC וכו') וזאת על מנת לצמצם את סיכוני אבטחת מידע.

7.1.6. הקשחת שרתים

יש לדאוג להקשחה סטנדרטית בהתאם ל-Best Practices של כל קבוצת שרתים לפי שיוך תפעולי (DC -Domain Controller, חוות גלישה, Exchange וכו'). בדומה להקשחת תחנות הקצה, ההקשחה מגנה גם היא על תחומי התקפה כמו מגע, התקפה (ראו נספח ב' - שרשרת התקיפה בסייבר) ועוד.

7.1.7. הקשחת ציוד תקשורת אקטיבי

יש לדאוג להקשחה סטנדרטית בהתאם ל-Best Practices של ציוד אקטיבי (מתגים, Firewall וכו'). ההקשחה תחזק את עמידותם להתקפות נקודתיות עליהם ותצמצם את היכולת של התוקף לחדור דרכם לתוך הרשת. שכבה זו מגנה על התחומים הבאים: חיצוני, מגע והתקפה (ראו נספח ב' - שרשרת התקיפה בסייבר).

7.1.8. וירטואליזציה

הטעמת כלי וירטואליזציה כגון טכנולוגית VDI - virtual desktop infrastructure על מנת לוודא ולשפר את תהליך עדכוני תוכנה וניהול גרסאות ברשות ברמת תחנות הקצה.

לצד היתרונות בשימוש בכלי וירטואליזציה, קיימות סכנות וחששות בשימוש בכלים אלו שהופכים את המערכות הארגוניות לחשופות יותר בפני מתקפות של האקרים. הסכנה המרכזית הינה לכשל במכונה וירטואלית אשר תשפיע על שאר המכונות הווירטואליות והיישומים הקיימים באותו משאב. משמעות הדבר כי נדרשת אבטחה מחמירה יותר על מכונה וירטואלית.

7.2. אמצעי הבקרה

7.2.1. ניטור הרשת

הטמעת מערכת Security Information and Event Management – SIEM והתחברות ל-SOC – Security Operating Center הממשלתי. התחברות זו תעניק לרשות יכולות איסוף מודיעין חיצוני ופנימי על הנעשה בתוך הרשת ומחוצה לה. כמו כן יש במהלך זה הוספת יכולות ניטור מתמיד (24/7) של רשת המחשוב של הרשות ובכלל – התמודדות עם השלבים הבאים: חיצוני, מגע, התקפה וההוצאה לפועל (ראה נספח ב' - שרשרת התקיפה בסייבר)

7.2.2. זיהוי חריגות וסטיות (אנומליות)

הטמעת כלים והפעלת יכולת ניטור, זיהוי ועצירת חריגות וסטיות (אנומליות) על בסיס Agent בתחנות. וכן הפעלת כלי ניטור מרכזי אשר למעשה מהווים יחד קו הגנה אחרון בפני התקפות לא ידועות.

7.2.3. הונאה ופיתוי

רשות מקרקעי ישראל תשאף לשלב טכנולוגיות קיימות, הטמעת כלים והפעלת יכולות ניטור, זיהוי וחשיפת התוקף תוך כדי תנועה וביסוס שליטה ברשת הרשות. שימוש במנגנון לפיתוי התוקף באמצעות מידע הנראה כחלק מבסיס הנתונים של הרשות ויכול להיות בעל ערך עבורו, אך למעשה מאפשר לבודד, לנטר ולחשוף את התוקף.

7.2.4. מעקב והקלטות

הטמעת כלים למעקב ותיעוד של פעילות ספקים בתוך רשת הרשות. כמו כן, תיעוד של פעילות חשודה או זדונית.

7.2.5. עדכוני תוכנה (מיקרוסופט + צד ג')

הטמעת כלי מעקב מדויק לניטור ומעקב על כלל התחנות והשרתים, על מנת לוודא שמותקנים עליהם עדכוני התוכנה האחרונים (עדכוני מיקרוסופט + עדכוני צד ג').

7.3. סקרי אבטחת מידע

7.3.1. בדיקות חוסן תשתיתיות

ביצוע בדיקות חוסן רוחביות, נקודתיות ותקופתיות בכדי לוודא קיום רמת הגנה טובה של הרשת, בפני פעילות עוינת מבחוץ ומבפנים.

7.3.2. סקרי אבטחת מידע והגנת הסייבר

ביצוע בחינה תקופתית חיצונית ו/או בלתי תלויה, של מערך האבטחה הפיזי והלוגי ברשות על מנת להציג תמונת מצב לחשיפת הארגון לפגיעות חיצוניות ופנים ארגוניות.

7.3.3. אבטחה פיזית

ביצוע סקרים למערך האבטחה הפיזית של מערכות המידע במתקני רמי השונים, סניפים, מרחבים ומוקדי שירות וכו'. בסקרים ייבדקו ארונות וחדרי תקשורת, מתחמים רגישים - והטמעת האמצעים המתאימים באופן אחיד ובהתאמה לרמת הסיכון הנובעת מכל מערכת לפי סיווג המידע.

8. פיתוח מאובטח

ברשות מקרקעי ישראל קיימות ומפותחות אפליקציות רבות על ידי צוותי הפיתוח השונים. תהליכי הפיתוח והתחזוקה של האפליקציות יתבצעו בשילוב מלא ובהנחיית תחום אבטחת מידע. ליווי והנחיה זו יבוצעו במהלך כל שלבי מחזור החיים של הפיתוח והתמיכה (Secure Software Development Life Cycle - SDLC).

הליווי בפיתוח מתבטא כבר משלב התכנון והייזום בו נעשה תכנון של המערכת או האפליקציה, תוך התחשבות בנקודות תורפה אפשריות ומתן מענה על ידי בקרות מתאימות. בסיום שלב הפיתוח ושלב הבדיקות (QA) תתבצע בדיקת חוסן על המערכת או האפליקציה, על מנת לנסות ולאתר בה בעיות אבטחת מידע. רק לאחר שכל השלבים הללו יסתיימו, תעלה המערכת או האפליקציה לאוויר. במהלך פעילות המערכת או האפליקציה, תתבצע בדיקה תקופתית על פי רמת הרגישות שנקבעה למערכת, ובהמשך יתבצעו פעולות לתיקון הליקויים.

התהליך הזה מתקיים בסביבות הפיתוח (Dev) ובסביבת הבדיקה (Test) ויש בו תהליך בקרה ומעקב אחרי שינויים, וזאת ע"מ להפריד בין סביבות אלו ובין סביבת האמת (Prod).

כל שינוי או תוספת מהותית למערכת יקבל את אישור גוף אבטחת המידע בטרם העלאתו לאוויר.

במסגרת תהליך הפיתוח ינחה צוות אבטחת המידע את צוותי הפיתוח ויבצע בדיקות בטרם ההעלאה לאוויר.

לפירוט נוסף ראה נוהל א14- "נוהל פיתוח ורכש מאובטח".

9. המשכיות עסקית

על רשות מקרקעי ישראל להתכונן למצב שבו לא תוכל להמשיך ולהתקיים כסדרה, בין אם בשל גורם חיצוני או אסון טבע, ובין אם בעקבות מתקפה זדונית.

המשכיות עסקית נועדה לאפשר לארגון לסכל הפרעות לפעילות השוטפת של המערכות הפיזיות והלוגיות במצבי חירום וכן לאפשר המשך ניהול רציף של אבטחת מידע במצבים אלו.

בכדי להבטיח את רמת ההמשכיות הנדרשת לאבטחת מידע במצבי אסון, רמ"י תיצור, תתעד, תיישם ותתחזק תהליכים, נהלים ובקרות.

לפירוט אודות נושא ההמשכיות העסקית ברשות מקרקעי ישראל ראה נוהל א17- "נוהל המשכיות עסקית".

10.שינוי המדיניות

- ✓ מדיניות הגנת הסייבר של המשרד תיבדק ותאושרר אחת לשנתיים ע"י ממונה הגנת הסייבר במשרד, או מוקדם יותר בהתאם לצורך מיוחד (על רקע שינויים משמעותיים במערך המחשוב הארגוני של המשרד). במקרה הצורך תעודכן המדיניות.
- ✓ הבדיקה והעדכון של המדיניות הממשלתית תתבצע ע"י היחידה להגנת הסייבר בממשלה (יה"ב).
- ✓ הבדיקה והעדכון של המדיניות המשרדית יתבצעו ע"י ממוני הגנת הסייבר ותאושר ע"י ועדת ההיגוי.

10.1. חריגה מהמדיניות

- בחינה ואישור חריגות ממדיניות המשרד, אם ידרשו, תתבצע ע"י ממונה הגנת הסייבר ובאישור ועדת ההיגוי.
- חריגות מהמדיניות הממשלתית ידווחו ליחידה להגנת הסייבר בממשלה (יה"ב).

נספחים

נספח א' - סוגי תוקפים

1. מעצמה

מעצמות סייבר כמו רוסיה, סין וארצות הברית מהוות גורם משמעותי בשדה הקרב הקיברנטי. יחידות הסייבר שלהן חזקות והוכיחו יכולות בזמן אמת (פלישת רוסיה לחצי האי קרים, ציונר הגז הסיבירי בשנות השמונים, הכור האיראני וכד'). היכולות הטקטיות של יחידות אלה כוללות חדירה למערכות המחשוב הרגישות ביותר בעולם, שליפת מידע נקודתי או מלא והשבתה כללית או חלקית של מערכות מחשוב, עד לכדי גרימת נזקים כבדים בעולם הפיזי. חלק מהיכולות המתקדמות של מעצמות הסייבר הוא לגרום נזק מבלי שיתגלו על ידי הקורבן, או לפחות יתגלו באיחור וזאת על מנת לצמצם את יכולת הקורבן להגיב באופן יעיל. למרות האיום הממשי של מעצמות הסייבר אין לרשות מקרקעי ישראל את היכולת או המשאבים לעצור או אפילו לזהות התקפה מתוחכמת ברמה זו. האחריות על ניטור פעילות עוינת מצד מעצמות הסייבר היא על כוחות הביטחון ברמה הארצית.

2. מדינה

יכולות התקיפה של מדינה בתחום הסייבר דומות לאלה של מעצמה אך ברמה נמוכה יותר באופן משמעותי. עם זאת, יחידות סייבר במדינות שונות עדיין מהוות איום על תשתיות ארגוניות ומדינתיות, ובעלות יכולות פריצה לארגונים.
גם ברמה זו, רשות מקרקעי ישראל אינה מתמודדת בעולם הגנת הסייבר.

3. ארגון טרור

ארגוני טרור מפתחים גם הם יכולות סייבר ובאירועי ציון מזדמנים מנסים להסב נזק לארגונים פרטיים וציבוריים. רשות מקרקעי ישראל, כסמל שלטון של מדינת ישראל מהווה יעד תקיפה פוטנציאלי לארגונים אלו ועליה לוודא מוכנות מול תקיפות שכאלה, באמצעות הכלים הקיימים במערך אבטחת הסייבר הלאומי.

4. אנרכיסטים

ארגונים אנרכיסטים כמו Greenpeace, אירועי OpIsrael וכו' מבצעים תקיפות על ידי יחידים או קבוצות מתוך כוונה להביך, להעביר מסר פוליטי ולשבש את מרקם החיים במדינה שלא למטרה עסקית. תקיפות אלה מאופיינות לרוב בקנה מידה נרחב אך ברמת תחכום נמוכה.

5. גורמים פליליים

בדומה לתקיפות הטרור, הכלים דומים אך המוטיבציה היא בעיקר פלילית–עסקית.

6. גורם פנימי

עובד פנימי (קבוע וזמני), עובד קבלן ועובד מיקור חוץ (Outsourcing) אשר קיבל גישה למערכות המחשוב של רשות מקרקעי ישראל ומבצע פעולות פוגעניות, בין בתמים ובין בזדון, או עובד כלשהו בעל מודעות נמוכה לנושא אבטחת המידע ולנהלים המחייבים.

7. גורמים נוספים

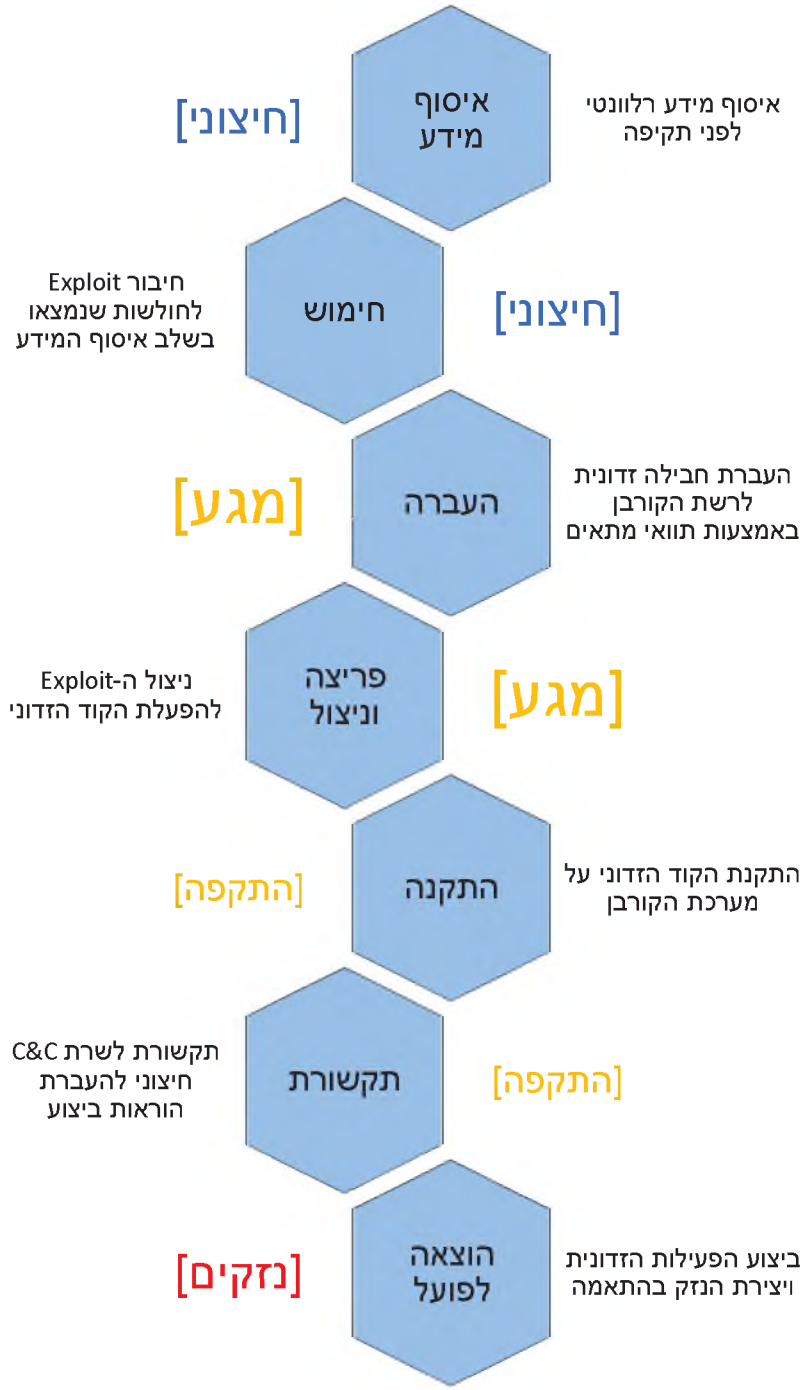
1.1.1 **חולשות טכנולוגיות** – חולשות מובנות במוצרי מדף או חולשות הנובעות מפיתוח פנימי.

1.1.2 **שרשרת אספקה** – צמצום הסיכונים הנובעים מחשיפה של עובדי שרשרת האספקה למידע ולמערכות של המשרד. החשיפה של עובדים אלו תהיה מינימלית ככל הניתן בהתאם לתפקידם, וע"פ עיקרון "הצורך לדעת".
רשות מקרקעי ישראל תיישם אמצעים לפיקוח ולבקרה על פעולות החברות וכן על פרצות אבטחה הקיימות אצל ספקי השירות השונים (חומרה, תוכנה, יועצים חיצוניים, אחזקה, תשתיות וכדו').

1.1.3 **סיכונים כללים** – סיכונים העלולים ליצור פגיעה במידע או במערכות המידע של רשות מקרקעי ישראל וזאת כתוצאה מגורם תוקף מכוון, כשל מבני או אנושי ברשות (תרבות עבודה שגויה, טעות אנוש או כשל תשתיתי במערכות).

נספח ב'- שרשרת התקיפה בסייבר (Cyber Kill Chain)

שרשרת התקיפה בסייבר מתארת את אופן הפעולה האופייני להתקפות סייבר. אמצעי אבטחה מכוונים כלפי אחד או יותר משלבי שרשרת ההתקפה. סגירה של כל חוליה בשרשרת תצמצם משמעותית את היתכנות ההתקפה.



נספח ג' – גופים מנחים ותקנים מחייבים

1. יחידת להגנת הסייבר (יה"ב)

היחידה להגנת הסייבר כחלק מרשות התקשוב הממשלתי במשרד רוה"מ. אחראית על הנחיית היחידות הממשלתיות, משרדים ורשויות - בנושא הגנת הסייבר.

2. רשות הסייבר הלאומית

רשות הסייבר הלאומית הוקמה בעקבות החלטת הממשלה מספר 2444 מיום 15.02.2015 בנושא "קידום היכולת הלאומית במרחב הקיברנטי", במטרה לעצב, ליישם ולהטמיע תורה לאומית להגנת סייבר.

3. רשות להגנת הפרטיות

הרשות להגנת הפרטיות (לשעבר "רמו"ט" – הרשות למשפט מידע וטכנולוגיה) במשרד המשפטים, האחראית על יישום וביקורת של חוק הגנת הפרטיות, התשמ"א – 1981. הרשות להגנת הפרטיות היא הרגולטור של רשות מקרקעי ישראל בכל הנוגע לשמירה על מידע רגיש מבחינת צנעת הפרט.

4. תקני International Organization for Standardization - ISO

בעקבות החלטת הממשלה מספר 2443 מיום 15.02.2015 נדרשים הגופים הממשלתיים לעמוד בתקן ISO27001 – תקן אבטחת מידע בארגון ובהמשך נבצע התעדה לתקן ISO 27032 – תקן להגנת הסייבר.

5. חוק הגנת הפרטיות (תקנות רמו"ט)

עוסק בהגנת פרטיותו של אדם לרבות בהגנת הפרטיות במאגרי מידע ממוחשבים. החוק מחייב רישומו של כל מאגר מידע המכיל מידע אישי אצל רשם מאגרי המידע במשרד המשפטים. בעליו של מאגר המידע נדרש להגן עליו לבל יועבר ממנו מידע למי שאינו מורשה לכך, ובפרט נדרשת הגנה למידע רגיש, המוגדר כ"נתונים על אישיותו של אדם, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו".

6. חוק חתימה אלקטרונית

החוק עוסק בהגדרה והסדרה של חתימה אלקטרונית על מסמכים, ומתן תוקף ואימות למסמך זה כאשר הוא חתום אלקטרונית (חתימה אלקטרונית מאובטחת או חתימה אלקטרונית מאושרת). החוק קובע את הכללים לפיהם חתימה אלקטרונית על מסר אלקטרוני (כגון הודעת דואר אלקטרוני) תהיה שקולה לחתימה על מסמך מודפס.

7. חוק הגנה על זכויות יוצרים

יצירה הינה קניין רוחני של היוצר ונדרשת התייחסות לקניין זה כאל שאר קניינים ונכסים ממשיים. מטרת החוק להגן על היוצרים ועל נכסיהם הרוחניים, וכן להסדיר את הזכויות של קניינים אלו, לרבות שימוש, העתקה וכד', ואת אמצעי האכיפה במקרה של פגיעה בזכויות היוצרים.

8. חוק המחשבים

החוק קובע עניינה פלילית לאדם העושה אחת מהפעולות הבאות הפוגעות בחיסיון, אמינות או זמינות המידע: יוצר וירוס מחשב או מפיץ אותו בזדון, חודר שלא כדין לחומר מחשב הנמצא במחשב, מוחק חומר מחשב, גורם לשינוי בו, משבשו בכל דרך אחרת או מפריע לשימוש בו, עושה פעולה לגבי מידע כדי שתוצאתה תהיה מידע

כוזב או פלט כוזב, משבש את פעולתו התקינה של מחשב או מפריע לשימוש בו. כמו"כ, החוק מגדיר כי מידע ממוחשב דינו כראיה לכל דבר ועניין וכי נדרש לשמור את המידע כמו כל ראיה אחרת.

נספח ד' – המבנה הארגוני של אבטחת המידע והגנת הסייבר ברשות

1. ועדת היגוי להגנת סייבר

ועדת ההיגוי מתכנסת אחת לשנה בראשות מנהל רשות מקרקעי ישראל ובהשתתפות מנהליה. מטרת הוועדה לאשרר ולתקף את רמת הגנת הסייבר של הרשות ואת מדיניות הרשות בתחום ההגנה על הסייבר, להתוות אסטרטגיות לפעילות, לפקח אחר יישום תכניות העבודה השנתיות, לקיים הערכת נזקים בעקבות תקלות ולגבש המלצות לטיפול.

- מנהל הרשות – יו"ר הועדה
- ממונה על הגנת הסייבר – אחראי על כלל היבטי אבטחת המידע והגנת הסייבר ברשות
- מנהל אגף משאבי אנוש –אחראי על כלל היבטי משאבי אנוש וזכויות העובדים
- נציג יה"ב – גורם מנחה ומייעץ להנחיות היחידה והגנה בסייבר במשרדי הממשלה
- יועץ המשפטי או נציג מטעמו – אחראי לכלל ההיבטים המשפטיים ולעמידה בהנחיות משפטיות
- חשב או נציג מטעמו – אחראי לצד הפיננסי והכלכלי
- מנהל חטיבת השמירה – אחראי לשמירה על הקרקעות, מניעת פלישה ואכיפה בהתאם
- מנהל חטיבת השירות – אחראי לתהליכי השירות והנגישות לאזרחי ישראל
- מנהל אגף בכיר עסקות – אחראי לתהליך העסקי ברשות
- מנהל אגף בכיר מידע ומחשוב – אחראי לכל מערכות התקשוב ברשות
- מנהל אגף ביטחון – אחראי לנושאי האבטחה הפיזיים
- ראש תחום בכיר תכנון ותקצוב – אחראי ליישום ולעמידה במסגרת התקציבית הכוללת
- מבקר הפנימי – אחראי לייעץ ולוודא התנהלות תקינה על פי התקנון

פירוט הגדרת תפקידים ובעלי עניין ניתן למצוא במסמך "הגדרת תפקידים ובעלי עניין"

2. ממונה הגנת סייבר

מנהל בכיר ברשות מקרקעי ישראל המשמש בתפקיד ממונה הגנת סייבר, ואחראי להבטיח את הטיפול והבקרה (וסקרים) על נושאי הגנת הסייבר מטעם מנהל הרשות.

3. מנהל מערכות מידע

אחראי על אסטרטגיית מערכות המידע ברשות מקרקעי ישראל ועל ניהול ויישום הגנת סיכוני הסייבר בארגון.

4. מנהל הגנת סייבר

גורם מנחה ומבקר של כלל היבטי הגנת הסייבר הנוגעים לתחומי המחשוב והתקשורת. באחריותו להגדיר ולקדם תוכניות עבודה בנושא הגנת הסייבר ברשות, וכן להיות אחראי לגיוס והעמדת תקציבים בהתאם.

כמו כן, מהווה גורם מנחה לגבי צרכי ההגנה הפיזית של מערכות המידע הנדרשים ברשות.

5. צוות הגנת סייבר

צוות הגנת סייבר באגף מערכות מידע מוגדר כגורם המנחה והמבקר. הצוות אחראי על הנחיות הגנת סייבר לאגף מערכות מידע ולכלל רשות מקרקעי ישראל. בנוסף יקיים הצוות פעילות הדרכה ובקרה בתחומי מערכות המידע השונים, במתחמי הרשות ברחבי הארץ ובתהליכים העסקיים של הרשות, וזאת על מנת לוודא רמת הגנת סייבר נאותה ברשות מקרקעי ישראל.

צוות הגנת הסייבר עוסק בשלושה תחומים עיקריים:

- תשתיות ותקשורת
- פיתוח מאובטח
- נהלים, רגולציה וביקורת (GRC)

6. מטמיעי הגנת סייבר

מנהלי הטכנולוגיה והתשתיות האחראים על הטמעה ויישום ההנחיות המועברות מתחום אבטחת מידע.

7. מנהלי מאגרי מידע

עם התרבות מקרי הפגיעה בזכויות הפרט והשימוש הלא מפוקח בפרטים האישיים של אזרחי העולם, הוטעמה באירופה רגולציה בנושא – GDPR. בעקבות זאת, גם בישראל הורחב ועודכן החוק להגנת הפרטיות, והוא מתייחס בהרחבה לכל נושא מאגרי המידע.

כחלק מכך, הוחלט כי לכל מאגר מידע ימונה מנהל ועליו יהיה לוודא כי המאגר עומד ברגולציה ובהנחיות השמירה על המידע האגור בו.

8. ועדת הרשאות

ועדת הרשאות תגדיר את סיווג המשרות ואת רמת ההרשאות הנדרשת לכל משרה, תוך התייחסות לקריטריונים ספציפיים הנוגעים לרגישות המידע אליו יחשפו. הרשימה תאושר על ידי מנהל משאבי אנוש.

9. תחולה

האחריות לכתיבת, הפצת והטמעת נהלי אבטחת המידע ברשות היא של מנהל הגנת הסייבר ברשות. במסגרת זאת, עליו להגדיר מה המחויבות והאחריות של כל עובד בשמירה ויישום נהלים אלו. לאחר מכן, עליו להציג את התוצר לרמה הממונה ולקבל את אישורה ליישום הנחיותיו.

נספח ה' – פרוט רמות הסיווג

1. כללי (ניתן לשיתוף ציבורי)
מידע פתוח לעיון הציבור. מידע שבחשיפתו לציבור לא יגרום נזק, מידע שיש לפרסמו על פי דין או מידע שפורסם.

2. פנימי (תפוצה פנימית וגורמי חוץ הקשורים לנושא)
מידע שבחשיפתו לגורמים שאינם מורשים, פגיעה בזמינותו או שיבושו עשויים לגרום נזק לרשות, לגופים ממשלתיים אחרים או לאינטרס הציבורי.

3. חסוי (תפוצה פנימית מוגבלת)
מידע אשר פגיעה בחסיונו, שלמותו, מהימנותו, זמינותו או שרידותו עלולה לגרום לפגיעה בניהולה התקין של הרשות, במשרדי ממשלה אחרים, במדינה או בגופים ציבוריים אחרים, או לפגוע בפרטיות על פי הגדרת החוק.

4. חסוי ביותר (תפוצה פנימית מצומצמת)
מידע אשר פגיעה בחסיונו, שלמותו, מהימנותו, זמינותו ושרידותו עלולה לגרום לפגיעה קשה ומתמשכת בניהולה התקין של הרשות, במשרדי ממשלה אחרים, במדינה או בגופים ציבוריים אחרים.

רמת סיווג	כללי (1)	פנימי (2)	חסוי (3)	חסוי ביותר (4)
	ניתן לשיתוף ציבורי	תפוצה פנימית וגורמי חוץ הקשורים לנושא	תפוצה פנימית מוגבלת	תפוצה פנימית מצומצמת
	מידע פתוח לעיון הציבור. מידע שחשיפתו לציבור לא יגרום נזק, מידע שיש לפרסמו על פי דין או מידע שפורסם.	מידע שחשיפתו לגורמים שאינם מורשים, פגיעה בזמינותו או שיבושו עשויים לגרום נזק לרשות, לגופים ממשלתיים אחרים או לאינטרס הציבורי.	מידע אשר פגיעה בחסיונו, שלמותו, מהימנותו, זמינותו או שרידותו עלולה לגרום לפגיעה בניהולה התקין של הרשות, במשרדי ממשלה אחרים, במדינה או בגופים ציבוריים אחרים, או לפגוע בפרטיות על פי הגדרת החוק	מידע אשר פגיעה בחסיונו, שלמותו, מהימנותו, זמינותו ושרידותו עלולה לגרום לפגיעה קשה ומתמשכת בניהולה התקין של הרשות, במשרדי ממשלה אחרים, במדינה או בגופים ציבוריים אחרים.
ישימות הסיווגים	√	√	√	√
מידע עסקי	√	√	√	√
מידע עסקי קריטי				√
נהלים פנימיים		√		
מידע על לקוחות			√	√
מידע פרטי או אישי של עובדים בודדים			√	√
מאגר מידע פרטים אישיים				√
תהליכי אבטחה והגנת סייבר			√	√
תיעוד תשתיות מחשוב			√	√
			ביחס זה פגיעות ניתן לכלול משרדי ממשלה אחרים, ההתעכרה התבצע עלפי תקנות העברת מידע שכחוק הגנת הפרטיות	

נספח ו' – פירוט קריטריונים לסיווג קריטיות של מערכת

ניתן להתאים את הקריטריונים המשמשים לזיהוי רמת הסיכון הכללית של כל מערכת לסוגי איומי הייחוס המוזכרים בסעיף 1.5.1 "הארגון כמכלול" (פגיעה בחיסיון, באמינות ובזמינות):

1. שכיחות השימוש

המערכת נמצאת בשימוש של יחידות רבות ברשות מקרקעי ישראל או בשימוש של עובדים ואזרחים רבים. השבתה של מערכת כזו תגרום לשיבושים משמעותיים ברצף העבודה ברשות ובשירות לאזרח. מערכת הנמצאת בשימוש נרחב ברשות חשופה בעיקר לאיומים של פגיעה בזמינות (Availability) ופגיעה באמינות (Integrity).

2. רגישות עסקית

במערכת קיים מידע בעל רגישות עסקית גבוהה. פגיעה במערכות כאלה ודליפת מידע מהן יכול להביא להפסד כספי, עצירה או ביטול של תהליכים עסקיים. מערכת המכילה מידע בעל רגישות עסקית גבוהה לתהליכים ברשות חשופה בעיקר לאיומים של פגיעה בחיסיון (Confidentiality) ופגיעה באמינות (Integrity).

3. צנעת הפרט

במערכת קיים מידע אישי על עובדים, אזרחים או מידע אחר. לפי חוק הגנת הפרטיות התשמ"א – 1981 ותחת הנחית הרשות להגנת הפרטיות (לשעבר רמו"ט) מערכת המטפלת במידע המאופיין כרגיש מבחינת צנעת הפרט חשופה בעיקר לאיומים של פגיעה בחיסיון (Confidentiality).

נספח ז' – קריטריונים למדידת תוחלת הנזק

קריטריון למדידה	רמת סיכון		
	נמוכה	בינונית	גבוהה
שימוש נרחב (משתמשים)	עד 100	עד 500	מעל 500
רגישות עסקית (₪)	עד 100K	100K-5M	מעל 5M
צנעת הפרט - עובד	עד 3	עד 50	מעל 50
צנעת הפרט - אזרח	עד 1K	עד 50K	מעל 50K

נספח ח' – מערכות קריטיות ברשות מקרקעי ישראל

מצורפת רשימה מערכות שזוהו כקריטיות. בכל מערכת קיימות תת-מערכות ולכל תת-מערכת שכזו סיכון משלה. הרשימה תתעדכן מידי תקופה כחלק מתהליך של סקר סיכונים שיתקיים ברשות אחת לתקופה לפי הנחיות יה"ב:

	שם המערכת	תת מערכת	רמת סיכון כללית	שימוש נרחב	רגישות עסקית	צנעת הפרט
1	System / תקשורת	תקשורת, טופולוגיה ומבנה הרשת	גבוהה	X	X	X
		Active Directory + Exchange	גבוהה	X	X	X
		Storage + Backup	גבוהה	X	X	X
2	כוכב / עכ"א	כוכב	גבוהה	X	X	X
3	הדמיה	ECM	גבוהה	X	X	X
		DRIVE U	גבוהה	X	X	X
		WINS	בינוני	X	X	X
4	SAP		גבוהה	X	X	X
5	GIS	GIS- Desktop (קליטת עסקאות)	גבוהה	X	X	
		GIS- web רמפ"ה (רמ"י על המפה)	גבוהה	X	X	
		GIS- מחשבים ניידים מערכת פיקוח, ArcPad, הדמיה, Email	גבוהה	X	X	
		GIS- מחשבים מובייל פורטל גאוגרפי בסמארטפון	בינונית	X	X	
6	בקרת פעילויות	בקרת פעילויות- כלל המערכות	גבוהה	X	X	X
7	פניות הציבור	כל פניות הציבור לרמ"י	גבוהה			X
8	מכרזים	מערכת מכרזים	בינונית	X	X	X
		מכרזים אינטרנט	גבוהה	X	X	X
		תוצאות	בינונית	X	X	X
		תשלום עבור השתתפות במכרז	בינונית	X	X	X
9	הערכת עובדים	הערכת עובדים (נמלה)	גבוהה	X		X
10	איתורמי	איתורמי – נכסים, בעלי זכויות, פרטים על הכירות	גבוהה			X
11	אתר האינטרנט	אתרי מידע של רמ"י לאזרח, מחשבון אתר לשמאים, מרכזים...		X	X	

פירוט המערכות הקריטיות

System / תקשורת

תשתיות המחשוב והתקשורת ברשות מקרקעי ישראל מהוות את הבסיס עליו מתקיימים כל התהליכים העסקיים והטכנולוגיים ברשות. פגיעה בתשתיות אלה תוביל לפגיעה פוטנציאלית בכל אחת מהמערכות הקריטיות, בנפרד או ביחד, בכל אחד מהקריטריונים שצוינו.

מערכת כוכב/ עכ"א כמרכז העשייה ברשות

מערכת כוכב היא מערכת קריטית ברשות. רוב רובן של המערכות מתממשקות למערכת זו כאשר רוב התהליכים העסקיים מתבססים עליה.

המערכת כוללת ניהול מידע לשני תהליכים מרכזיים של הקצאות קרקע בפטור, קרקעות במכרז ומחזור החיים של עסקה.

המערכת כוללת מידע אישי (שם, ת.ז, כתובת וכו'), מידע עסקי (העברת בעלות מעל דונם, הזנה של עסקה, אישור עסקה וכו') וספר הנכסים, כחלק ממערכת עכ"א שלא דרך כוכב.

מערכת הדמיה

מערכת ההדמיה ותת-מערכותיה העיקריות (ECM ,Drive U ,WINS) מכילות מידע רגיש ותומכות בתהליכים עסקיים מהותיים ברשות. פגיעה במערכות אלו עלולה לגרור פגיעה מהותית בעשייה המרכזית ברשות.

גם אם מערכת כוכב/עכ"א נופלות, ניתן לבצע פעולות (קבלת קהל, מתן מידע וכו') באמצעות איתורון או איתורמ"י (במידה ומערכת הדמיה עובדת).

מערכת SAP

מערכת ERP אשר תקלוט אליה את מרבית מערכות המידע המסורתיות שברשות. מדובר במערכת שתכלול את רוב התהליכים המהותיים ותקיים חלק גדול מהתהליכים העסקיים ברשות.

מערכת GIS

מערכת ה-GIS מכילה את שכבות המידע הגאוגרפי המהווה בסיס למערכות מידע רבות ברשות מקרקעי ישראל. רבים מתהליכי העבודה ברשות מסתמכים על מערכת זו, החל מהמפקחים בחטיבת השמירה, דרך קליטת עסקאות, הממשק האינטרנטי ועוד.

מערכות נוספות

מערכות מידע נוספות (כמו אתר האינטרנט של הרשות, איתורמ"י ועוד) המכילות, מעבדות או מעבירות מידע רגיש, אשר פגיעה בהן תגרום נזק משמעותי לרשות.

נספח ט' – פירוט תפיסת האבטחה הפיזית והסביבתית

אבטחת מתחם

בתכנון אבטחה של מתחם יש לשקול את הגורמים הבאים:

1. מידור

מטרת המידור היא הכנסת העובדים המורשים להיכנס תוך חסימה של גורמים אשר אינם מורשי כניסה. יש לשקול גם מידור ראיה וצילום במידת הצורך.

דוגמאות לאמצעי מידור:

- ✓ מעגלי אבטחה ע"פ הנחיות הקב"ט
- ✓ בקרת כניסה
- ✓ נעילת המתחם במפתח ייעודי
- ✓ וילונות

2. מיגון

מטרת המיגון היא העלאת רמת הקושי של תוקף לחדור למתחם תוך שימוש באמצעי פריצה קרים או חמים.

דוגמאות לאמצעי מיגון:

- ✓ סורגים על חלון
- ✓ הקשחת קירות המתחם
- ✓ דלת מחוזקת

3. תיעוד מבקרים

רישום ותיעוד של כל מבקר במתחם, שעת הביקור ופרטים חיוניים נוספים.

דוגמאות לאמצעי תיעוד:

- ✓ יומן מבקרים
- ✓ מצלמות מעגל סגור
- ✓ רישום כניסות במערכת בקרת כניסה

אבטחת ציוד

ברשות מקרקעי ישראל קיים ציוד מחשוב רב ומגוון המשמש את העובדים לצורך מילוי תפקידם. נזק, אובדן או גניבה של ציוד זה יגרום לנזק כספי לרשות אך מעבר לכך, סכנות דליפת מידע חיוני ומתן כניסה לא רצויה של תוקף לתוך רשת המחשוב של הרשות.
ניתן לחלק את הציוד הקיים ברשות מקרקעי ישראל לפי אזור השימוש:

1. ציוד נייח

ציוד נייח מוגן על ידי מעגלי האבטחה של מתקני הרשות בהם הוא נמצא (שרתים, מדפסות, מחשבים נייחים וכו'). הסיכון הנשקף לציוד זה הוא גניבה או גרימת נזק על ידי גורם עוין הנכנס למתחם הרשות במסווה או עובד (זדוני או תמים).

שיטות האבטחה של ציוד נייח יכללו אך לא יוגבלו ל:

- ✓ מיגון פיזי של המתחם

- ✓ ביקורת של מאבטחי המתחם בכניסה וביציאה
- ✓ מידור, בקרת כניסה ונעילת חדרים בתוך המתחם הראשי
- ✓ מודעות עובדים להתנהגות חריגה של עובדים ומלווים
- ✓ גריסת דפים וגריטת התקני אחסון המכילים מידע פנימי / חסוי / חסוי ביותר

2. ציוד נייד

ציוד נייד הוא ציוד היוצא מתחומי מתקני רשות מקרקעי ישראל לשימוש עובדי הרשות במשימות שונות, מחוץ למתחמי ושעות העבודה (מחשבים ניידים, מצלמות, טלפונים סלולריים, מצעים פיזיים וכו'). מלבד הסיכונים הקיימים לציוד זה בהיותו נמצא במתחמי הרשות, קיימים סיכונים רבים נוספים לציוד נייד (גלישה ברשתות לא מאובטחות, שימוש של גורמים לא מורשים בציוד, גניבה של הציוד וכו'). גורם סיכון נוסף הוא העובדה שרוב מעגלי האבטחה הקיימים סביב הציוד הקבוע חסרים במקרה זה.

למען הסר ספר, ציוד נייד כולל בתוכו גם רשומות ומידע מודפס, או כל מידע אחר שניתן לשנע אותו אל מחוץ למתחמי הרשות.

שיטות האבטחה של ציוד נייד יכללו אך לא יוגבלו ל:

- ✓ נהלי שמירה ושימוש קפדניים של העובד על הציוד
- ✓ הקשחת הציוד באופן שיקשה על תוקף או גנב לגשת למידע או לרשת רשות מקרקעי ישראל
- ✓ מנגנוני הגנה בפני גלישה לאתרים לא רצויים והחדרת מפגעים לציוד שיצא מחוץ לחצרות הרשות

נספח י' – תהליכים להגנת הסייבר בהיבט האנושי

1. אבטחת מידע והגנת סייבר בתהליכי גיוס, ניוד ועזיבת עובדים

צמצום הסיכונים להגנת הסייבר, הנובעים מגיוס עובדים העלולים להיות בעלי רמה נמוכה של מהימנות ומחויבות אישית, וצמצום הסיכונים הכרוכים בעזיבת עובדים.

1.1. פעילות נדרשת - גיוס עובדים

- ✓ כל העובדים הנקלטים ברשות מקרקעי ישראל יעברו בדיקת מהימנות בהתאם להחלטת הגורם המוסמך ברשות ובהתאם לצורך, על פי הנחיות הגופים המנחים.
- ✓ חוזים והתקשרויות של הרשות עם חברות וספקים יכללו התייחסות למחויבות של החברות והספקים בכל הנוגע לבדיקות המבוצעות בתהליכי גיוס העובדים.
- ✓ רשות מקרקעי ישראל תיצור רשימת סיווג משרות באמצעות ועדת הרשאות, תוך התייחסות לקריטריונים ספציפיים הנוגעים לרגישות המידע אליו יחשפו. הרשימה תאושר על ידי מנהל משאבי אנוש. למידע נוסף ראה נוהל א.9-"נוהל בקרת גישה".
- ✓ כל עובד חדש יקבל את רמת ההרשאות הנדרשת לפי הגדרת תפקידו.
- ✓ חוזה שייחתם עם עובדים חדשים יכלול התייחסות לאחריות של העובד בכל הנוגע להיבטי אבטחת מידע והגנת הסייבר, וילווה בהצהרת סודיות, עליה יהיו מחויבים לחתום כל עובדי רשות מקרקעי ישראל וזאת על פי התקשי"ר.

1.2. פעילות נדרשת - ניוד עובדים

- ✓ כל החלפת תפקיד במהלך פעילותו של עובד ברשות או עבורה, תגרור בקרה על ההרשאות החדשות הניתנות לו וההרשאות הישנות שיש לבטלן.
- ✓ במסגרת שינוי תפקיד יוסרו באופן מיידי כלל ההרשאות אשר ניתנו למשתמש במסגרת תפקידו הקודם, ויוגדרו הרשאות מתאימות המשקפות את דרישות התפקיד הנוכחי.
- ✓ במידה ויתקבל אישור מנהל בכיר, ניתן יהיה להשאיר את ההרשאות הקודמות לתקופה מוגבלת.

1.3. פעילות נדרשת - סיום העסקת עובדים

- ✓ עובדים העוזבים את רשות מקרקעי ישראל יחזירו את כרטיס העובד שהונפק להם, את כל המידע הפיזי (מסמכים, מצעי זיכרון נתיק וכד'), וכן את כל ציוד המחשוב (חומרה ותוכנה) שהונפק להם על ידי הרשות.
- ✓ הרשאות העובדים במערכות הרשות יבוטלו מייד עם עזיבת העובד, ובמקרה של פיטורים – בהתאם להמלצתו של מנהלו הישיר ויועמ"ש.
- ✓ מנהל העובד יגדיר את הגורמים הרשאים לגשת לקבצים שהיו בשימוש העובד. גישה לקבצים שהיו בשימוש העובד תיפתח רק לאחר קבלת אישור בכתב מהגורם המוסמך.

2. עקרון האחריות האישית

מטרת עקרון האחריות האישית להבטיח את מחויבות העובדים לאבטחת מידע והגנת הסייבר ולמידע המצוי ברשותם.

- ✓ כל עובד ברשות יהיה אחראי באופן אישי להגנה על המידע אליו הוא נחשף במהלך עבודתו ולכלל המידע המצוי בחזקתו, כולל מידע אשר נשלח או הועבר אליו על ידי גורם אחר.
- ✓ במסגרת אחריות זו, על העובד לנקוט בכל האמצעים העומדים לרשותו על מנת להגן על המידע. בין אמצעים אלה ניתן למנות:
  - שימוש אישי בזיהוי המשתמש.
  - שמירה על חיסיון ההזדהות.

- דיווח על חריגות בהגנת הסייבר.
- הגנה על מסמכים ורשומות.
- הגנת סביבת העבודה.
- מדיניות "שולחן נקי"
- מדיניות "מסך נקי"

✓ כל עובד ברשות יהיה אחראי לדווח לממונה על הגנת הסייבר ולמנהל מערכות המידע על כל פעילות העלולה להשפיע על הגנת הסייבר ברשות.
✓ כל פגיעה במידע עקב רשלנות של העובד או אי עמידה בנהלים היא באחריות העובד.
✓ מנהלים יישאו באחריות כוללת ליישום נהלים להגנת הסייבר בתחום סמכותם.
✓ טיפול באירועי חריגים יתבצע בשיתוף פעולה של המנהל, מנהל הגנת הסייבר ואגף מערכות מידע.
✓ עיקרון האחריות האישית יוטמע ברשות באמצעים הבאים:
- החתמת העובדים על הצהרת סודיות ואחריות.
- העלאת מודעות העובדים לנושאי הגנת הסייבר באמצעות הדרכות והפצת חוזרים בנושא.
- טיפול משמעתי בחריגות מנהלי הגנת הסייבר.
- שימוש בכלים טכניים, המאפשרים בקרה על יישום האחריות האישית.

למידע נוסף אודות נהלים והנחיות לעובד ברשות מקרקעי ישראל, ראה מסמך "כללי הגנת הסייבר לבעל תפקיד ברשות מקרקעי ישראל".

3. מודעות להגנת סייבר

על מנת להביא למודעות גבוהה בקרב עובדי הרשות לסיכונים בכל הקשור לאבטחת מידע והגנת הסייבר, ולספק להם את הכלים ליישום מדיניות ונהלי להגנת הסייבר, יש לבצע את הפעולות הבאות:

✓ כל עובד חדש יעבור הדרכה בנושאי הגנת הסייבר במסגרת ההכשרה הראשונית ברשות מקרקעי ישראל.
✓ כל עובדי הרשות יחויבו להשתתף בהדרכות תקופתיות להגנת הסייבר, בהתאם למידת הידע הנחוצה לכל בעל תפקיד.
✓ עובדי הרשות ישתתפו בפרויקטים לשיפור המודעות להגנת הסייבר, כמו למשל מתקפות דיוג (פישינג), זאת במטרה לשפר ולחדד את המודעות לנושא אבטחת המידע והגנת הסייבר.

נספח יא' – הגדרות ומושגים

4. **רשות** - רשות התקשוב הממשלתי.

5. **יה"ב** – היחידה להגנת הסייבר בממשלה.

6. **הנחיה** - הנחיית יה"ב במסגרת הנחיות ראש רשות התקשוב הממשלתי.

7. **משרד** - משרד ממשלתי או יחידת סמך ממשלתית או יחידה משרדית.

8. **נכסי המידע** – המידע, מערכות המחשוב המעבדות ומאכסנות אותו והתקשורת, האמצעים והציוד עליו הוא מושתת.

9. **יחידה מובחית רשות התקשוב**- יחידה בארגון המונחית על ידי רשות התקשוב הממשלתי בהתאם להחלטות הממשלה: אגף מערכות מידע, אגף הגנת סייבר, וכדומה.

10. **מנמ"ר** - מנהל מידע ראשי / (Chief Information Officer) (CIO) מנהל אגף מערכות מידע.

11. **ממונה הגנת הסייבר במשרד** - אדם שמונה לתפקיד זה מטעם מנכ"ל המשרד ואשר אחראי על הגנת הסייבר במשרד.

12. **מאגר מידע** - אוסף נתוני מידע המוחזק באמצעי מגנטי או אופטי(ובכלל זה מחשב)ומיועד לעיבוד ממוחשב.

13. **מנהל המאגר** - מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לעניין זה;

14. **סיווג מידע** - מדד המגדיר את רמת רגישות המידע והמערכות התומכות בו ,בהתבסס על העקרונות שהוגדרו על ידי היחידה להגנת הסייבר בממשלה(יה"ב.)

15. **נזק למידע** - פגיעה בסודיות ,בשלמות וזמינות המידע בבעלותו של המשרד.

16. **סודיות המידע** - חשיפת המידע לגורמים לא מורשים.

17. **שלמות מידע** - זהות הנתונים במאגר מידע למקור שממנו נשאבו, בלא ששונו, נמסרו או הושמדו ללא רשות כדין.

18. **זמינות המידע** - הבטחת נגישות למידע באופן רציף.

19. **מידע רגיש** - מידע אשר פגיעה בזמינותו ,סודיותו או שלמותו עלולה לפגוע בניהולו התקין של המשרד הממשלתי או גופים אחרים.

20. **מידע פרטי** - מידע אודות עניניו הפרטיים של אדם בהתאם לחוק הגנת חוק הגנת הפרטיות ,תשמ"א 1981 –

21. **סייבר – מרחב הסייבר** - מרחב וירטואלי ופיזי המורכב משלושה רבדים מרכזיים:
רובד פיזי :כלל רכיבי המחשוב והתקשורת.
רובד לוגי :הקוד המפעיל את רכיבי המחשוב וקובע כיצד יפעלו.
רובד אנושי /נוהלי :כלל האנשים המשתמשים ברשת.

22. **הגנת סייבר** - תחום שעניינו להגן על נכסים ברובד הפיזי ו/או ברובד הלוגי מפני תקיפות סייבר המכוונות לגרום לדלף מידע, שיבושו והשחתתו, במקביל לפגיעה מכוונת במערכות התקשוב התומכות, תוך שיבוש מערכתי חלקי עד כדי שיתוק מוחלט ומלא של יכולת המערכות לתפקד, כלומר למלא את משימתה.
הגנת סייבר כוללת איסוף מודיעין על יריבים פוטנציאליים, שימוש בכלי סייבר כדי לאתר "פוגענים" ו"נוזקות" שכבר נכנסו למערכת ונמצאים בתוכה, ניטור של המידע העובר ברשת וחיפוש אחרי אנומליות ו/או תקשורת בין "סוסים טרויאניים" למרכיב ה "פיקוד ושליטה" שלהם וכדומה.
תחום זה כולל גם" הגנה אקטיבית ,"כלומר פעילות שתכליתה לזהות ולחסום תוקפים, תקיפות וזליגת מידע על ידי ניטור והפעלת אמצעי הגנה פרו-אקטיביים על מערכות שעליהם מתכוונים להגן.

23. **מדיניות להגנת הסייבר בממשלה** - עקרונות המפורטים במסמך מטעם רשות התקשוב הממשלתי/היחידה להגנת הסייבר בממשלה - יה"ב, המגדיר את מחויבות המשרדים והעובדים בהם לעמידה בחוק, בתקנות ובהנחיות הגופים הרגולטוריים ועל פי תורת ההגנה הלאומית בסייבר לארגונים בהיבטי סיכול איומי סייבר והגנת המידע בממשלה.

24. **מידע** - כל נתון הנוגע ו/או הקשור לפעילותם, תפעולם או תפקודם של המשרדים, לרבות מידע הנוגע לצנעת הפרט ומידע ממשלתי רגיש, הקיים על-גבי אמצעי אחסון ממוחשבים, מגנטיים או אלקטרוניים, מצעי מידע פיזיים וכן מידע המועבר בעל-פה.

25. **ועדת היגוי משרדית לנושא הגנת הסייבר** - פורום ניהולי שממונה ע"י מנכ"ל משרד ובראשו יושב מנכ"ל המשרד .חברים בוועדה :נציגים בכירים במשרד בעלי אחריות לתחום הגנת הסייבר, לרבות אחריות בהיבטים טכנולוגיים, אבטחתיים ותפעוליים, מנהל התקציבים, מנהל משאבי אנוש, יועץ משפטי, נציג יה"ב ונציגים נוספים לפי שיקול דעתו של המנכ"ל. הוועדה נועדה לאשרר ולתקף את רמת הגנת הסייבר של המשרד ואת מדיניות המשרד בתחום ההגנה על הסייבר, להתוות אסטרטגיות לפעילות, לפקח אחר תכניות העבודה השנתיות, לקיים הערכת נזקים בעקבות תקלות ולגבש המלצות לטיפול.

26. **רשומות מידע** - כוללות מצעי פיזיים נושאי מידע, כגון מסמכים, תדפיסים, דיסקים, קלטות, אוגרי מידע ניידים.