תוכן עניינים

אישורים

מהדורה	שם	תפקיד	סימוכין	תאריך
1.1				

שינויים בנוהל

מהדורה	תאריך	מאשר	מהות השינוי
1.1	9/09/14		שדרוג כל הנוהל

1. רקע

1.1. כללי

1.1.1. עקרונות אבטחת המידע יתבססו על מערכת ניהול סיכונים המזהה, מבקרת ממזערת או מונעת את סיכוני האבטחה העלולים להשפיע על המידע, מאגריו או מערכותיו.

1.1.2. ניהול הסיכונים יהיה מושתת על הערכת סיכונים המשקפת את מידת פגיעותם של המידע, מאגריו ומערכותיו, הערכת האיומים, השלכותיהם ומידת התכנות התממשותם.

1.1.3. ניהול הסיכונים יוביל לקבלת החלטות באשר לפעילויות אבטחת המידע הנדרשות במשרד האוצר, סדרי עדיפותם (לרבות משאבי כ"א ותקציבים) ואופן קיומם (החלטה בנושאי תהליכים, שיטות, כלים וכיוצא באלו).

2. מטרה

2.1. מטרת הנוהל

2.1.1. צמצום נזקים פוטנציאליים למידע, מערכותיו ומאגריו, כתוצאה מניהול לוקה של סיכוני אבטחת המידע במשרד האוצר.

2.1.2. השגת תוצאות מתוכננות למערכת ניהול אבטחת המידע וזיהוי פעולות לשיפור.

2.1.3. הגדרת עקרונות ניהול הסיכונים במשרד.

3. הגדרות

3.1. **פגיעה במידע -** שיבוש, שינוי, מחיקה, העתקה או חשיפה של מידע רגיש בפני גורמים בלתי מורשים. פגיעה במידע יכולה להתרחש בשוגג, במתכוון או ע"י כוח עליון.

3.2. **סיכון (בהיבט אבטחתי) -** מצב הנגרם מפעילות הנובעת מיישום תהליכים ו/או מהפעלת כלים או מוצרים, העלולים להזיק לתפקודו התקין של הארגון, בהיבטי אבטחת המידע. הסיכונים עלולים להביא לדליפת מידע רגיש ו/או לפגיעה במידע, מאגריו או מערכותיו.

3.3. **הערכת סיכונים -** הגדרת האיומים השונים על נכסי משרד האוצר בכלל ועל המידע בפרט

- פנימי-

וכן הערכת פגיעותו של המשרד ביחס לאיומים אלו, סבירות התרחשותם והשפעתם על המשרד.

3.4. **ניהול סיכונים -** תהליך זיהוי, בקרה, מזעור או סילוק של אותם גורמי המהווים איום על נכסי משרד האוצר והמידע בפרט.

3.5. **מידע -** כל הנתונים הקשורים לפעילותו של משרד האוצר, הקיימים על-גבי אמצעי אחסון ממוחשבים, מגנטיים או אלקטרונים, ועל-גבי מצעים פיזיים.

3.6. **מידע רגיש** - נתונים אשר שיבושם, מחיקתם, חשיפתם או הגעתם לידי גורמים בלתי מורשים, עלולים להוביל לפגיעה במשרד האוצר. כמו כן, נתונים המחויבים בהגנה מתוקף חוק.

3.7. **אבטחת מידע** - מכלול הפעילויות והאמצעים הננקטים במטרה להבטיח את שלמות, סודיות, אמינות, זמינות ושרידות המידע.

4. אחריות

4.1. באחריות ועדת ההיגוי לנושאי אבטחת מידע לגבש ולהתוות את מדיניות ועקרונות הטיפול בניהול הסיכונים במשרד האוצר.

4.2. באחריות מנהל תחום אבטחת מידע וסייבר לספק כלים ותהליכים ליישום הנחיות נוהל זה.

4.3. באחריות ועדת ההיגוי לנושאי אבטחת מידע לבקר ולאכוף יישום הנחיות נוהל זה.

4.4. באחריות המנהלים במשרד האוצר לבקר ולאכוף יישום הנחיות אבטחת המידע על-ידי עובדיהם, בכל הקשור להיבטים הפיזיים.

4.5. באחריות מנהל תחום אבטחת מידע וסייבר לעדכן נוהל זה לפי מידת הצורך והעניין.

5. תוקף ומסמכים

5.1. תוקף הנוהל

5.1.1. תוקף הנוהל-מפרסומו.

5.2. מסמכים מתייחסים

5.2.1. תקן ת"י ISO 27001: 2013, פרק 6.

5.2.2. פורמט טבלה לניהול סיכונים (נספח א').

5.2.3. תוכנית לביצוע סקרי סיכונים (נספח ב').

6. השיטה

6.1. כללי

6.1.1. הסיכונים מבוססים על האיומים הרלוונטיים לרכיבי ולתהליכי כל מערכת, בהתאם לניתוח הסיכונים שבוצע על-ידי מנהל תחום אבטחת מידע וסייבר.

6.2. הסיכונים במשרד האוצר

6.2.1. <u>סיכונים כלכליים:</u>

סיכונים בהיבטים כלכליים, כדוגמת פגיעה או חשיפה של מידע כלכלי רגיש כגון ספר התקציב לפני פרסומו או היערכות כלכלית טרם פרסומה.

6.2.2. <u>סיכונים תפעוליים:</u>

סיכונים בהיבטי היישום, כדוגמת ניצול הרשאות קיימות לגישה למידע בלתי מורשה או חדירה דרך האפליקציות.

6.2.3. <u>סיכונים טכנולוגיים:</u>

סיכונים בהיבטים טכנולוגיים, כדוגמת גניבת מידע מבסיס הנתונים לאחר השגת גישה, ניצול מערכת דואר אלקטרוני לגניבת מידע, חדירה למערכת באמצעות כלים ממוכנים או חדירה לשרתים ולמערכות ההפעלה.

6.2.4. <u>סיכונים בהיבטי צנעת הפרט:</u>

סיכונים הקשורים לצנעת הפרט של עובדי משרד האוצר, אזרחי ותושבי המדינה.

6.2.5. <u>סיכונים תדמיתיים:</u>

סיכונים העלולים לנבוע מהגעתם של מחדלים, כשלים, ליקויים או חשדות לגבי קיומם

של אלו, אל אמצעי התקשורת, אל ספקים, אל הציבור וכיוצא באלו. מלבד הפגיעה התדמיתית הישירה, עלולה התממשותם של סיכונים אלו להוביל לפגיעה בכושרו התפעולי של משרד האוצר.

6.3. יישום

על מנת לבדוק את מידת ההתאמה בין רמת האבטחה המוגדרת, המושתת על ניהול סיכונים, לבין רמת האבטחה המיושמת בפועל, תבוצענה הפעילויות הבאות:

6.3.1. ביקורות טכניות - לוגיות:

- מנהל תחום אבטחת מידע וסייבר יכין בראשית השנה תוכנית ביקורות שוטפות / תקופתיות, אשר תתייחס לנושאים המבוקרים, לתדירות או העיתוי של הביקורת המתוכננת, לאתרים המיועדים לביקורת (מלא או מדגמי), לפורמט התיעוד של הביקורת, לגורמים נוספים האמורים להיות מעורבים ותפקידם באירוע, וכדומה.
- נכסים שיבדקו:
  - ציוד תקשוב (מחשוב ותקשורת).
  - מערכות מידע.
  - מידע השמור במדיה מגנטית אופטית ו/או בכל צורה אחרת.
  - מסדי נתונים, נהלים ותקנים, מדריכים והוראות תפעול תהליכי עבודה עסקיים וקבצי נתונים.
  - מערכות יישומיות, מערכות הפעלה, כלי פיתוח ותוכנות שונות.
  - הון אנושי (עובדים).
  - מערכות בקרה.
  - תהליכי העבודה של המחלקות השונות במשרד.
- התוכנית תכלול ביקורות לצורך בדיקת היישום הטכני של הכלים והתהליכים המוגדרים בדרישות אבטחת המידע במערכות השונות וכן איתור פרצות ברשת, תוך שימוש בכלים ייעודיים, הבודקים את הגדרות המשתמשים,

הסיסמאות, ההרשאות, הגדרות המערכת וכיו"ב.

תדירות ומסגרת: אחת לשנה במסגרת מבדקים פנימיים (לפי הגדרות תוכנית מבדקים פנימיים) ו/או במסגרת סקרי סיכונים חיצוניים שיבוצעו על-ידי גורמים חיצוניים (הערה: בכל מקרה, יש לבצע סקר על-ידי גורם חיצוני אחת לשנתיים, לכל הפחות).

- מבדקי חוסן (penetration tests) לאפליקציות ובמערכות ההפעלה.

תדירות ומסגרת: אחת לשנתיים, על-ידי גורם חיצוני המתמחה בביצוע מבדקי חדירה.

- מבדקי חוסן (penetration tests) לאתרים המונגשים לקהל מחוץ לרשת המשרד .

תדירות ומסגרת: לפני העלייה לאוויר ולאחר כל שינוי מהותי האתר, על-ידי גורם חיצוני המתמחה בביצוע מבדקי חדירה.

6.3.2. ביקורות אבטחה פיזית – ביצוע ביקורות שוטפות / תקופתיות לבחינת התהליכים והכלים המיושמים במשרד בהיבטי האבטחה הפיזית, לבדיקת מידת היישום של דרישות תשתית האבטחה הפיזית.

תדירות ומסגרת: אחת לחציון במסגרת מבדקים פנימיים (לפי הגדרות תוכנית מבדקים פנימיים) ו/או במסגרת סקרי סיכונים חיצוניים שיבוצעו על-ידי גורמים חיצוניים (הערה: בכל מקרה, יש לבצע סקר על-ידי גורם חיצוני אחת לשנתיים, לכל הפחות).

6.3.3. סקר סיכונים תהליכי – מעת לעת, יבוצע סקר סיכונים תהליכי על-ידי גורם שלישי בלתי תלוי אשר יסקור את הפרצות וההונאות הפוטנציאליות האפשריות בתהליכי העבודה הרלוונטיים למערכות הארגון השונות.

6.3.4. ביקורות נוהליות – כל מנהל במשרד אחראי לוודא כי עובדיו פועלים בהתאם לנהלי אבטחת המידע של המשרד. בנוסף, מכילים הנהלים עצמם מנגנוני בקרה פנימיים, אשר ייושמו על-ידי הגורמים הרלוונטיים לכל נוהל.

6.3.5. הביקורות / הסקרים יוגדרו במסגרת תוכנית דו-שנתית מפורטת, אשר:

- התוכנית תפרט את כל סוגי הסקרים והבדיקות (ביקורות טכניות – לוגיות וביקורות נוהליות), בהתאם לפריסת ביצועם על פני השנתיים (ראה נספח ב').

- פנימי-

באופן זה, ניתן יהיה לוודא כי בוצעו כלל סוגי הסקרים.

- התוכנית תיכתב על-ידי מנהל תחום אבטחת מידע וסייבר ומנהל מערך סייבר חרום וביטחון ותאושר על-ידי ועדת ההיגוי לנושאי אבטחת מידע .
- התוכנית תכלול פירוט של התחומים הנבדקים, הגורם המבצע ולוחות הזמנים. יוקצו משאבים תקציביים לצורך יישום התוכנית (ראה פירוט בפרק "ניהול משאבים", בהמשך).
- תוצאות הביקורת יתועדו על פי פורמט שנקבע ויכללו תיעוד תמציתי של הביקורת (תאריך, מבצע, נושא ורכיבים שנבדקו, אתרים/גורמים מבוקרים, הערכת ממצאים, נושאים/נקודות לתשומת לב וטיפול שוטף, ו/או לביקורת חוזרת בעתיד – קבועה או אד-הוק, ועוד).
- מנהל תחום אבטחת מידע ומנהל מערך סייבר חרום וביטחון, כל אחד בתחומו, יפיצו את התוכנית לגורמי הארגון הרלוונטיים עם אישורה של התוכנית וכן יתזכרו את הגורמים הללו בטווח של כחודש טרם מועד הביקורת.

6.3.6. ממצאי הביקורות, הסקרים ומבדקי החדירה יוגשו למנהל תחום אבטחת מידע וסייבר ולמנהל מערך סייבר חרום וביטחון וכן לוועדת ההיגוי לנושא אבטחת מידע. מנהל תחום אבטחת מידע וסייבר ומנהל מערך סייבר חרום וביטחון, כל אחד בתחומו, יגבשו תוכנית ליישום ההמלצות, תוך ציון הגורמים האחראים, לוחות הזמנים ודרכי הטיפול (לרבות פעילות בהתאם לנוהל "דרישה לפעולה מתקנת והזדמנויות לשיפור"). במידת הצורך, יוקצו לצורך היישום משאבי תקציב, כ"א וזמן. התוכנית תאושר על-ידי ועדת ההיגוי לנושא אבטחת מידע.

6.3.7. חריגות או ממצאים משמעותיים או המצריכים דיווח וטיפול משלים מידי ידווחו מידית למנהל תחום אבטחת מידע וסייבר אשר יתאם פעילויות מתקנות מידיות, בהתאם לנוהל "פעולה מתקנת והזדמנויות לשיפור".

6.3.8. מנהל תחום אבטחת מידע וסייבר ינהל טבלה (ראה נספח א', "פורמט טבלה לניהול סיכונים") בה יפורטו הסיכונים הלוגיים (בהיבטי המחשוב והתקשורת), המערכת / מיקום, מידת הנזק, פוטנציאל התרחשות הנזק, דרגת החומרה, המלצות / הפתרונות לטיפול, אחריות, לו"ז לטיפול, אופן בדיקת אפקטיביות הטיפול (פירוט שיטת הבדיקה), הסיכונים השיוריים, דרגת חומרת כל סיכון, שם הגורם הבודק או המאשר (את בדיקת אפקטיביות הטיפול או את הסיכונים השיוריים), חתימה ותאריך (נספח

- פנימי-

א' מהווה דוגמא לטבלה לניהול סיכונים. ניתן לעשות שימוש בטבלאות אחרות, המכילות את השדות המופיעים בנספח א').

6.3.9. במקרה בו יהיו קיימים סיכונים שלא ניתן לתת להם מענה תהליכי ו/או טכנולוגי ו/או אשר הוחלט שלא לטפל בהם, תאשר ועדת ההיגוי הותרת הסיכונים כ"סיכונים שיוריים". עבור כל סיכון שיורי תוגדר גם רמת החומרה שלו. נציג ועדת ההיגוי יאשר קיומו של כל סיכון, באמצעות חתימתו בטבלה.

6.3.10. באחריות מנהל מערכות מידע לעדכן את מנהל תחום אבטחת מידע וסייבר בתהליכי הטמעה של חידושים טכנולוגיים עוד בשלבי טרום POC

6.3.11. ניהול הסיכונים בהיבטי האבטחה הפיזיים יבוצע באחריותו של המנהל אגף חרום וביטחון.

6.3.12. תוכן הטבלה יתבסס על ממצאי מבדקי התאמה, סקרי ועדת ההיגוי, סקרי סיכונים, מבדקי חדירה, פעולות מתקנות וכל נתון אחר, כפי שימצא לנכון.

6.3.13. ועדת ההיגוי תיזום ביצוען של בדיקות התאמה אשר נועדו לוודא כי תשתית אבטחת המידע תואמת לסיכונים שאופיינו והוגדרו בארגון. ראה "נוהל סקר הנהלה".

6.4. חישוב דרגת החומרה

6.4.1. ממצאי סקרי הסיכונים יצביעו על דרגת החומרה של כל סיכון, ממנו ייגזרו דרכי הטיפול בממצאים, החלופות, דחיפות יישום ההמלצות והקצאת המשאבים.

6.4.2. דרגת החומרה תהיה מבוססת על מידת פוטנציאל התרחשות הסיכון ועל מידת הנזק הפוטנציאלי העלול להתרחש, באם הסיכון ימומש.

6.4.3. חישוב דרגת החומרה יבוצע על בסיס הנוסחה:

דרגת חומרה = (מידת פוטנציאל התרחשות הסיכון) x (מידת הנזק).

6.4.4. דרגת החומרה יכולה לנוע בטווח הערכים שבין 1 ל-25. ככל שה"ציון" גבוה יותר, כך גבוהה יותר דרגת החומרה.

6.4.5. מידת פוטנציאל התרחשות הסיכון תוערך בטווחים שבין 1 ל-5, לפי הפירוט הבא:

1: פוטנציאל נמוך.

- פנימי-

2 : פוטנציאל נמוך-בינוני.

3 : פוטנציאל בינוני-גבוה.

4 : פוטנציאל גבוה.

5 : פוטנציאל גבוה מאוד.

6.4.6. מידת הנזק תוערך בטווחים שבין 1 ל-5, לפי הפירוט הבא :

1 : **נזק קל מאוד:**

<u>תיאור הפגיעה :</u>

- פגיעה קלה מאוד בתהליכים ארגוניים.
- האטת פעילות / שיבוש ברמה קלה מאוד של הפעילות (עד שעה).
- נזק קל מאוד לנתונים / מאגרי המידע / מערכות המידע / ציוד.
- ללא שיבוש נתונים או חשיפת מידע רגיש.
- ללא פגיעה בתדמית המשרד.

<u>עלות תיקון הנזקים : חצי מיליון שקל</u>

2 : **נזק קל:**

<u>תיאור הפגיעה :</u>

- פגיעה קלה בתהליכים ארגוניים.
- האטת פעילות / שיבוש ברמה קלה של הפעילות (עד 3 שעות).
- נזק קל לנתונים / מאגרי המידע / מערכות המידע / ציוד.
- חשיפה בכמות מועטה של מידע בסיווג "חסוי", אך ללא חשיפת מידע בסיווג "מידע חסוי ביתר".
- ללא פגיעה בתדמית המשרד.

<u>עלות תיקון הנזקים :</u> מחצי מיליון שקל עד מיליון שקל

- פנימי-

3 : **נזק בינוני:**

<u>תיאור הפגיעה :</u>

- פגיעה בינונית בתהליכים ארגוניים.
- האטת פעילות / שיבוש ברמה בינונית של הפעילות (עד 12 שעות).
- נזק בינוני לנתונים / מאגרי המידע / מערכות המידע / ציוד.
- חשיפה בכמות בינונית של מידע בסיווג "חסוי", אך ללא חשיפת מידע בסיווג "מידע חסוי ביתר".
- פגיעה קלה בתדמית המשרד.

<u>עלות תיקון הנזקים :</u> ממיליון שקל עד חמישה מיליון

4 : **נזק כבד:**

<u>תיאור הפגיעה :</u>

- פגיעה קשה בתהליכים ארגוניים.
- האטת פעילות / שיבוש ברמה קשה של הפעילות (עד 24 שעות).
- נזק קשה לנתונים / מאגרי המידע / מערכות המידע / ציוד.
- חשיפה בכמות גדולה של מידע בסיווג "חסוי" / חשיפה בכמות מועטה של מידע בסיווג "מידע חסוי ביתר".
- פגיעה בינונית בתדמית המשרד.

<u>עלות תיקון הנזקים :</u> מחמישה מיליון שקל עד עשרה מיליון שקל

5 : **נזק כבד מאוד:**

<u>תיאור הפגיעה :</u>

- פנימי-

- פגיעה קשה מאוד בתהליכים ארגוניים.
- האטת פעילות / שיבוש ברמה קשה של הפעילות (מעל 24 שעות).
- נזק קשה מאוד לנתונים / מאגרי המידע / מערכות המידע / ציוד.
- חשיפה בכמות גדולה מאוד של מידע בסיווג "חסוי" / חשיפה בכמות בינונית ומעלה של מידע בסיווג "מידע חסוי ביתר".
- פגיעה קשה בתדמית המשרד.

<u>עלות תיקון הנזקים</u>: מעל עשרה מיליון שקל

6.5. חישוב דרגת החומרה

6.5.1. ממצאי סקרי הסיכונים יצביעו על דרגת החומרה של כל סיכון, ממנו ייגזרו דרכי הטיפול בממצאים, החלופות, דחיפות יישום ההמלצות והקצאת המשאבים.

6.5.2. דרגת החומרה תהיה מבוססת על מידת פוטנציאל התרחשות הסיכון ועל מידת הנזק הפוטנציאלי העלול להתרחש, באם הסיכון ימומש.

6.5.3. חישוב דרגת החומרה יבוצע על בסיס הנוסחה: דרגת חומרה = (מידת פוטנציאל התרחשות הסיכון) x (מידת הנזק).

דרגת החומרה יכולה לנוע בטווח הערכים שבין 1 ל-25. ככל שהציון גבוה יותר, כך גבוהה יותר דרגת החומרה.

1.1.1. סבירות והשפעת סיכון יוגדרו על פי הטבלה הבאה:

מידת הנזק	פגיעה קריטית	**נזק כבד מאוד**	**5**	5	10	15	20	25
	פגיעה משמעותית	**נזק כבד**	**4**	4	8	12	16	20
	פגיעה בינונית	**נזק בינוני**	**3**	3	6	9	12	15
	פגיעה מינורית	**נזק קל**	**2**	2	4	6	8	10

- פנימי -

	פגיעה שולית	**נזק קל מאוד**	**1**	1	2	3	4	5
				1	**2**	**3**	**4**	**5**
				נמוך	**נמוך - בינוני**	**בינוני**	**בינוני - גבוה**	**גבוה מאוד**
				סביר שלא יתרחש בקרוב	עלול להתרחש לעיתים רחוקות	עלול להתרחש בקרוב	עלול להתרחש לעיתים קרובות	עלול לקרות כל יום
				%				
פוטנציאל התרחשות הסיכון								

1.2. קבלה וטיפול בסיכונים

1.2.1. המשרד יקבל ויטפל בסיכונים בהתאם לרמת הסיכון:

1.2.1.1. עדיפות ראשונה – סיכונים בעלי ערך 15-25 (הקצאה מיידית של כל המשאבים הנדרשים להקטנת הסיכון או ביטולו).

1.2.1.2. עדיפות שניה – סיכונים בעלי ערך 10-12 (הקצאת משאבים על פי החלטת הנהלה להקטנת הסיכון או ביטולו).

1.2.1.3. עדיפות שלישית – סיכונים בעלי ערך 5-9 (יש להמשיך לעקוב תקופתית אחר סיכונים אלו, לא נדרשת כל פעולה).

1.2.1.4. עדיפות רביעית – סיכונים בעלי ערך 1-4 (לא נדרשת כל פעולה, ההנהלה מקבלת את הסיכון).

1.2.2. ועדת ההיגוי לנושא אבטחת מידע וסייבר תאשר את סדרי העדיפויות לטיפול בממצאים.

6.6. יישום המלצות סקרי הסיכונים

6.6.1. ועדת ההיגוי לנושא אבטחת מידע תאשר את סדרי העדיפויות לטיפול בממצאים, כפי שהומלצו על-ידי מנהל תחום אבטחת מידע ו/או מנהל מערך סייבר חרום וביטחון.

6.6.2. ממצאי סקרי הסיכונים יטופלו בהתאם לסדרי עדיפויות הנובעים מהפרמטרים הבאים:

- דרגת חומרת הסיכון (ככל שדרגת החומרה גבוהה יותר, כן יהיה דחוף יותר ליישם את אמצעי הטיפול בסיכון).

- פנימי -

- קלות יישום אמצעֵי הטיפול בסיכון (סיכונים שניתן "לפתור" במהירות, בקלות וללא דרישה למשאבים, יטופלו בדחיפות רבה יותר, אך מבלי לפגוע ביישום אמצעי הטיפול הכרוכים בסיכונים בעלי דרגת חומרה קשה).

6.6.3. מנהל תחום אבטחת מידע ו/או מנהל מערך סייבר חרום וביטחון ישאפו לכך כי יישום אמצעֵי הטיפול בסיכון, הנגזרים מדרגת חומרת הסיכון, יהיו בהתאם לטווחי הזמן הבאים:

- דרגת חומרה 21-25: עד שבוע.
- דרגת חומרה 16-20: עד חודש.
- דרגת חומרה 11-15: עד חודשיים.
- דרגת חומרה 6-10: עד 3 חודשים.
- דרגת חומרה 1-5: עד 4 חודשים.

6.7. עדכון שינויים משמעותיים

6.7.1. מנהל תחום אבטחת מידע וסייבר ומנהל מערך סייבר חרום וביטחון, כל אחד בתחומו, יהיו מעורבים בקיומם של פרויקטים / חידושים טכנולוגיים (לרבות מעבר לסביבה פיזית אחרת, הכנסת תוכנות או חומרות חדשות, החלפת תוכנות ומערכות מידע ומחשב, עדכון מהדורות והעלאת גרסאות של המערכות והתוכנות, שדרוגים, שינויי תשתית וכדומה) על-מנת להתאים את השינויים לסיכונים הדינמיים וכן על-מנת להתאים פתרונות אבטחתיים. במידת הצורך, יעדכן מנהל תחום אבטחת מידע וסייבר את השינויים ב"טבלה לניהול סיכונים" (לרבות בתחום האבטחה הפיזית).

6.7.2. מנהל תחום אבטחת מידע וסייבר ומנהל מערך סייבר חרום וביטחון, כל אחד בתחומו, יעדכנו את ה"טבלה לניהול סיכונים" בעקבות יישום המלצות הבדיקות, הסקרים ומבדקי החדירה. השינויים יובאו לאישורה של ועדת ההיגוי.

6.8. ניהול משאבים

6.8.1. מנהל מערך סייבר חרום וביטחון יקצה למשאבים הנדרשים לקיומה של תשתית אבטחת המידע, מנהל תחום אבטחת מידע וסייבר ירכז וינהל את משאבים אלו כנגזר ממדיניות הארגון ולפי הצורך המשתנה, הנובע מניהול סיכונים, ממצאי מבדקים פנימיים, אירועים חריגים, דרישות חוזיות מול ספקים או מול ממשקים עסקיים

- פנימי-

רלוונטיים אחרים, דרישות תחיקתיות (חוק המחשבים וחוק הגנת הפרטיות) או נסיבות אחרות.

6.8.2. ועדת ההיגוי לנושאי אבטחת מידע אחראית על הקצאת משאבים (כסף, כ"א וזמן) ליישום דרישות תשתית אבטחת המידע (ראה "נוהל סקר הנהלה")

6.8.3. מנהל מערך סייבר חירום וביטחון ומנהל תחום אבטחת מידע וסייבר ישקלו יחד את רמת הדחיפות ואת סדרי העדיפויות ביישומן של פעילויות אבטחה המחייבות הקצאתם של משאבים נוספים העולים במהלך שנת הפעילות ואשר לא תוכננו ממנהל.

- פנימי-

7. בקרה ועדכון

7.1. כללי

7.1.1. פעם בשנה, לכל הפחות, תבקר ותאכוף ועדת ההיגוי לנושאי אבטחת מידע את יישום הנחיות נוהל זה, בתחומי האבטחה הלוגית (המחשוב והתקשורת), האבטחה הפיזית, אבטחת הרשומות (מצעים פיזיים נושאי מידע) ומהימנות עובדים.

7.2. בדיקות בקרה

7.2.1. בדיקה של התאמת תכולת ה"טבלה לניהול סיכונים" לסיכונים הדינאמיים בשוק (במקרים בהם יצוצו סיכונים חדשים עליהם ידע שלא במסגרת המבדקים הפנימיים הסדירים, בכלל התחומים כמפורט בנוהל זה). ראה "נוהל מבדקים פנימיים".

7.2.2. בדיקה של תוכנית יישום המלצות הבדיקות, הסקרים ומבדקי החדירה.

7.2.3. בדיקה מדגמית של פרויקטים, במגמה לוודא את התאמת הפעילות לתכולת ה"טבלה לניהול סיכונים", כפי שקיימת בארגון בעת הבדיקה.

7.2.4. ממצאים חריגים אשר יעלו בבדיקות אלו ידווחו ויטופלו (בהתאם לשיקול דעתו של מנהל תחום אבטחת מידע וסייבר, בשיתוף מנהל מערך סייבר חרום וביטחון במידת הצורך) בכפוף להנחיות "נוהל דרישה לפעולה מתקנת והזדמנויות לשיפור".

8. נספחים

נספח א': פורמט טבלה לניהול סיכונים.

נספח ב': תוכנית לביצוע סקרי סיכונים.

- פנימי-

נספח א':

פורמט טבלה לניהול סיכונים

	פירוט הסיכונים					ממצאים והטמעה				סיכונים שיוריים			אישור הטיפול בסיכונים		
מס"ד	תיאור הסיכון	מערכת / מיקום	מידת הנזק *	פוטנציאל התרחשות *	דרגת החומרה *	המלצות / פתרונות	משאבים נדרשים	אחריות טיפול	לו"ז לטיפול	תיאור סיכונים שיוריים	דרגת חומרת כל סיכון שיורי	שם הגורם המאשר קיומו של הסיכון השיורי	אופן בדיקת אפקטיביות הטיפול בסיכון	שם הגורם הבודק/המ אשר את סיום הטיפול בסיכון	תאריך סיום הטיפול בסיכון

* ראה הרחבות בנוהל ניהול סיכונים

נספח ב':

תוכנית לביצוע סקרי סיכונים

סוג הבדיקה	תקציב / משאבים נדרשים	2015												2016											
		1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12

- פנימי-