תוכן עניינים

אישורים

מהדורה	שם	תפקיד	סימוכין	תאריך
1.1				

שינויים בנוהל

מהדורה	תאריך	מאשר	מהות השינוי
1.1	27/10/14		התאמות ועדכון הנוהל

1. רקע

1.1. יעד מרכזי ביישום והטמעת התקן הישראלי (ת"י) 27001:2013 על ידי משרד האוצר הנו שמירת עדכניות ויעילות של קובץ נהלי הגנת המידע והסייבר, וזאת לשם קיום אבטחה נאותה של המידע ונכסי המידע של משרד האוצר.

1.2. ועדת ההיגוי לנושא הגנת המידע והסייבר (להלן: "ועדת ההיגוי") התחייבה, במסמך המדיניות ובקובץ הנהלים, לבצע הליך מתמיד של שיפור וייעול מערך ניהול הגנת המידע והסייבר לשם העלאת רמת הגנת המידע והסייבר ומודעות העובדים בנושא.

1.3. משרד האוצר פועל כמיטב יכולתו לסילוק הסיבות לאי התאמות לנהלים ולחוקים בהיבטי הגנת המידע והסייבר וכן למנוע את הישנותם של אירועים חריגים.

1.4. מעקב אחר חריגות, אי התאמות וטעויות תוך טיפול יעיל ולימוד מהן, יימנעו הישנותן ויבטיחו עמידה ביעדי הגנת המידע והסייבר שהציבה לעצמה הנהלת משרד האוצר.

2. מטרה

2.1. מטרת הנוהל

2.1.1. צמצום סיכוני אבטחה העלולים לנבוע מהישנותם של אירועים, מתוך יישום פעולות מתקנות ומונעות.

2.1.2. קביעת שיטת טיפול אחידה בתהליכים הכרוכים בפעולות מתקנות ובהזדמנויות לשיפור.

3. הגדרות

3.1. **פעולה מתקנת:** פעולה הנובעת מאירוע חריג, חשד או כשל פוטנציאלי, אשר נועדה להביא את סטטוס הגנת המידע והסייבר למצב האופטימלי על-מנת למזער את סיכויי הישנותו של המקרה.

3.2. **הזדמנויות לשיפור:** פעולה שנועדה למזער את הסיכויים להתרחשותו של אירוע הגנת המידע והסייבר חריג, ופעולות לזיהוי הזדמנויות לשיפור.

- פנימי-

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

3.4. **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.

3.5. **הגנת המידע והסייבר -** מכלול הפעילויות והאמצעים הננקטים במטרה להבטיח את שלמות, סודיות, אמינות, זמינות ושרידות המידע.

4. אחריות

4.1. באחריות ועדת ההיגוי לנושא הגנת המידע והסייבר לגבש ולהתוות את מדיניות ועקרונות הטיפול בנושא פעולות מתקנות והזדמנויות לשיפור.

4.2. באחריות מנהל תחום הגנת המידע והסייבר לטפל בפעולות מתקנות ולזהות הזדמנויות לשיפור, כמוגדר בנוהל זה.

4.3. באחריות ועדת ההיגוי לבקר ולאכוף יישום הנחיות נוהל זה.

4.4. באחריות מנהל תחום הגנת המידע והסייבר 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 10.

5.2.2. טופס "דרישה לפעולה מתקנת (דפ"מ) – נספח א'.

5.2.3. טבלת מעקב פעולה מתקנת (דפ"מ) – נספח ב'.

- פנימי-

6. שיטה

6.1. גוף הנוהל

6.1.1. באחריות מנהל תחום הגנת המידע והסייבר ליזום הפקת "דרישה לפעולה מתקנת" (להלן: "דפ"מ"), בעקבות האירועים, הנהלים והיוזמים הבאים:

- מבדקי התאמה - עבור כל חריגה ו/או אי התאמה לנהלים, התקנים והחוקים יש לפעול לפי "נוהל מבדקים פנימיים".
- ניהול סיכונים - תשתית האבטחה של משרד האוצר מבוססת על הערכת סיכונים. במסגרת ניהול הסיכונים עשוי לעלות הצורך בפעולה מתקנת . יש לפעול בכפוף ל"נוהל ניהול סיכונים".
- אירועים חריגים - בעקבות אירועים חריגים בהיבט הגנת המידע והסייבר, כחלק מהשאיפה למנוע הישנות אירוע חוזר, יש לפעול לפי "נוהל טיפול באירוע אבטחתי חריג".
- סקר הנהלה - ועדת ההיגוי, תיזום פעולות למניעה ו/או תיקון בהיבטי הגנת המידע והסייבר. לשם כך יש לפעול לפי "נוהל סקר הנהלה".
- ועדת ההיגוי לנושא הגנת המידע והסייבר – הועדה תיזום פעולות להעלאת רמת האבטחה או לשינוי עקרונות האבטחה.
- עובד משרד האוצר (לרבות עובד ממשק עסקי) - כל עובד רשאי לפנות למנהל תחום הגנת המידע והסייבר או מי מטעמו להציג בעיה בתחום הגנת המידע והסייבר. מנהל תחום הגנת המידע והסייבר או מי מטעמו על פי שיקול דעתו יחליט האם ליזום לפעולה מתקנת בהיבטי הגנת המידע והסייבר.

6.1.2. מנהל תחום הגנת המידע והסייבר ינהל את הטיפול בדפ"מ אשר נוגע לתחומי פעילותו (לוגי ופיזי). כל זאת, לרבות הטיפול בשלבי התיעוד, הבקרה והמעקבים השוטפים. כמו כן, ינוהלו טבלאות למעקב אחר הטיפול בדפ"מ.

6.1.3. גורמי המקצוע המטפלים מטעם מנהל תחום הגנת המידע והסייבר וסייבר (להלן: "גורמי המקצוע המטפלים") ישקלו את עדכונם המידי של מנהל תחום הגנת המידע והסייבר (לפי הצורך) באשר לתחילת הטיפול בדפ"מ. בכל מקרה, יהיה עליהם לעדכן במקרים בהם הדפ"מ משקף פעילויות / אירועים אשר עלולים להשפיע על רמת הגנת המידע והסייבר של הארגון, המערכות הקריטיות או המידע.

- פנימי-

6.1.4. יוזם הדפ"מ וכן גורמי המקצוע המטפלים ימלאו את מקור הדפ"מ ואת הסיבת השורש שהביאה לטיפול בדפ"מ בטופס "דרישה לפעולה מתקנת" (ראה נספח א').

6.1.5. גורמי המקצוע המטפלים יתעדו את מהלך הבדיקות בטופס הדפ"מ.

6.1.6. גורמי המקצוע המטפלים יציינו את פרטי הדפ"מ ב"טבלת מעקב דפ"מ" (ראה נספח ב'), שם ינוהל מעקב מרוכז אחר כלל טיפולי הדפ"מ, ברמת פתיחת וסגירת הטיפול (תוכן הטיפול יתועד בנספח א').

6.1.7. גורמי המקצוע המטפלים יערבו גורמים מקצועיים מקרב עובדי משרד האוצר ו/או הממשקים העסקיים, לפי הצורך, על-מנת לקבל מידע נוסף.

6.1.8. לפי שיקול דעתם של מנהל תחום הגנת המידע והסייבר יעורבו גורמי הנהלה אשר אליהם רלוונטי הדפ"מ. זאת למען קבלת מידע חיוני, סיוע בקבלת החלטות בעניין המשך הטיפול ועדכון באשר לשינויים מתוכננים בעקבות הטיפול המיועד.

6.2. פעולות מתקנות והזדמנויות לשיפור

6.2.1. מנהל תחום הגנת המידע והסייבר בשיתוף עם מנהל חטיבת טכנולוגיות, יוזם הדפ"מ, מנהלים או גורמי מקצוע רלוונטיים (כל אלו בהתאם לשיקול דעתם), ייזמו פעילות מתקנת במטרה למזער את הסיכוי אשר בהישנות מקרים דומים. זאת, כגון הפעולות הבאות:

- גיבוש שיטות לאיתור מקרים דומים.
- הגדרת תהליכים באירוע.
- ביצוע פעולות מתקנות והמלצות לשיפור, לרבות שינוי ושיפור תהליכים, שינוי ועדכון נהלים ומדיניות משרד האוצר בנושאי הגנת המידע והסייבר והדרכת עובדים בהיבט הגנת המידע והסייבר.
- זיהוי גורם השורש
- יישום פעולות מניעה להישנות אירועים ותקלות בעתיד.
- קביעת אחראים לביצוע הפעולות הנ"ל.
- הגדרת לוח זמנים ומועדי סיום לביצוע הפעולות הנ"ל.

6.2.2. באחריות גורמי המקצוע המטפלים לתעד בטופס הדפ"מ את ההמלצות לטיפול, תוך פירוט הפעילויות המתבקשות, הגורמים האחרים לביצוע ולוחות הזמנים הנדרשים

- פנימי-

לסיום הטיפול.

6.2.3. באחריות מנהל תחום הגנת המידע והסייבר לעקוב אחר יישום ההמלצות לתיקון ולמניעה לפי המצוין בטופס הדפ"מ ולוודא סיום כל המטלות וההמלצות. עליהם לאשר את סיום הטיפול בחתימתם בטופס הדפ"מ ובטבלת המעקב (נספחים א' ו-ב').

6.2.4. גורמי המקצוע המטפלים ישלחו לכל הנוגעים בדבר את העתק טופס הדפ"מ ו/או הודעה בדבר סגירת הדפ"מ וביצוע כל ההמלצות והמטלות.

6.2.5. מנהל תחום הגנת המידע והסייברJ יתייק את טפסי הדפ"מ בתיק ייעודי אשר יהיה בחזקתם. טבלת המעקב תתויק בתחילת התיק.

6.3. בדיקת יעילות ושיפור

6.3.1. מנהל תחום הגנת המידע והסייבר יקבע שיטה ו/או מדדים לקביעת היעילות והשיפור שנבעו מפעילויות הדפ"מ. השיטה ו/או המדדים יתועדו בטופס הדפ"מ.

6.3.2. מדי חצי שנה, לכל הפחות, יבחן מנהל תחום הגנת המידע והסייבר את היעילות והשיפור באמצעות השיטה ו/או המדדים שנקבעו. מסקנות הבדיקה יתועדו אף הם בטופס הדפ"מ (עם סיום הטמעת השיפורים הנדרשים ניתן לחדול מקיומה של הבדיקה החוזרת ולבצע בדיקות שוטפות באמצעים הקיימים, כגון סקר הנהלה או מבדקים פנימיים).

6.3.3. במידה ורמת היעילות או השיפור אינה משביעת רצון, יש לשנות את השיטה, לעדכן את המדדים ולהמשיך בתהליך הבדיקה.

6.3.4. במידת הצורך, יש למלא טופס דפ"מ המשקף את הצורך בשינוי שיטת בדיקות היעילות והשיפור.

6.4. מעקב והמשך טיפול

6.4.1. במסגרת ישיבות סקר הנהלה ו/או ישיבות ועדת ההיגוי, יסקרו מנהל תחום הגנת המידע והסייבר ו/או מנהל מערך סייבר חרום וביטחון את מצב הפעולות המתקנות ואת ההזדמנויות לשיפור.

6.4.2. מנהל תחום הגנת המידע והסייבר ו/או מנהל מערך סייבר חרום וביטחון יפרטו את מידת היעילות והשיפור אשר נבעו מפעילות זו.

- פנימי-

6.4.3. חברי ועדת ההיגוי יתנו את הדעת באשר לצורך בשינוי מדיניות הגנת המידע והסייבר בהתבסס על ממצאי הטיפול בדפ"מ. החלטות אלו יתועדו בסיכום הישיבה וכן בטופס הדפ"מ.

6.5. בקרה

6.5.1. מדי חצי שנה, לכל הפחות, יבחן מנהל תחום הגנת המידע והסייבר את היעילות והשיפור באמצעות השיטה ו/או המדדים שנקבעו (עם סיום הטמעת השיפורים הנדרשים ניתן לחדול מקיומה של הבדיקה החוזרת ולבצע בדיקות שוטפות באמצעים הקיימים, כגון סקר הנהלה או מבדקים פנימיים).

6.5.2. הטיפול בדפ"מ ייבדק במסגרת מבדקים פנימיים, ישיבות ועדת ההיגוי וסקרי הנהלה, כמפורט בנהלים המתייחסים לתחומים אלו.

נספח א'
טופס דרישה לפעולה מתקנת (דפ"מ)

מספר דפ"מ : _____ **תאריך:** _____

פרטי יוזם הדפ"מ						
	שם	מספר עובד	תפקיד	חטיבה	טלפון פנימי	טלפון נייד
מקור הדפ"מ (סמן את הרלוונטי)						
	מבדק התאמה	ניהול סיכונים	אירוע חריג	קר הנהלה	ועדת ההיגוי	יוזמת עובד

תיאור הסיבה ליוזמת הדרישה ל"פעולה מתקנת " (צרף מסמכים תואמים, במידת הרלוונטיות)

_____

_____

תיאור הבדיקות

_____

_____

שם ממלא הפרטים: _____ **תפקיד:** _____ **חתימה:** _____ **תאריך:** _____

פעילויות שיפור / פעולות מתקנות

פעילות	אחריות	לו"ז לסיום	שם מאשר סיום הטיפול	חתימה	תאריך

בדיקת יעילות ושיפור (פירוט שיטה / מדדים לבדיקה ותוצאות הבדיקה)

_____

_____

_____

שם ממלא הפרטים: _____ **תפקיד:** _____ **חתימה:** _____ **תאריך:** _____

נספח ב'

טבלת מעקב – פעילות מתקנת (דפ"מ)

מספר דפ"מ	תאריך פתיחה	מקור הדפ"מ	שם "פותח" הדפ"מ	תיאור הסיבה ליוזמת הדפ"מ	תאריך סיום הטיפול בכלל הפעולות הנדרשות	שם מאשר סיום הטיפול	תפקיד	חתימה