מדינת ישראל
משרד האוצר

נהלי סייבר חירום וביטחון

נוהל סיווג מידע

משרד האוצר
מערך סייבר חירום וביטחון
סביבת הביטחון שלך

תוכן עניינים

אישורים

מהדורה	שם	תפקיד	סימוכין	תאריך
1.1				

שינויים בנוהל

מהדורה	תאריך	מאשר	מהות השינוי
1.1	21/07/14		התאמות ועדכון הנוהל

1. רקע

1.1. במסגרת עבודתם השוטפת עובדי משרד האוצר באים במגע עם מידע רב ומגוון. יש צורך להגדיר רגישות לסוגי המידע השונים, על מנת להתאים את ההתייחסות למידע מבחינת אבטחתו ושמירתו.

1.2. סיווג ורגישות מידע קשור למספר פרמטרים במשולב ונקבעים על בסיס רמת רגישות תפעולית (קריטיות המידע וצורך בו "בזמן אמת"), קיום מידע ממשלתי-רגיש, תחיקה, רצון ויכולת גורמים שונים לפגוע או לנצל לרעה את המערכת ועוד.

1.3. מבין הגורמים שפורטו לעיל, מידת הקריטיות התפעולית ומידת רגישות המידע, מהווים גורמים בסיסיים בשיקול הדעת הקובע את האמצעים אשר ינקטו לאבטחת המידע.

1.4. מידת הטיפול האבטחתי במידע נגזרת מרמת רגישותו, אשר אינה זהה בכל סוגי המידע ובכל סוגי המערכות.

2. מטרה

2.1. הגדרת רמות סיווג ורגישות מערכות המידע השונות במשרד, אשר ישמשו ככלי לקביעת רמת האבטחה הנדרשת במערכות אלו.

3. הגדרות

3.1. **מידע:** כל הנתונים הקשורים לפעילותו של המשרד, הקיימים על-גבי אמצעי אחסון ממוחשבים, מגנטיים או אלקטרוניים, ועל-גבי מצעים פיזיים.

3.2. **מערכת מידע:** שילוב אמצעי חומרה, תוכנה ומאגרי מידע באמצעותם ניתן לבצע פעולות על גבי מידע (כגון עריכה, אגירה, העברה, הדפסה, תכנון פעילות, הפצת מידע וכן הלאה). הגדרה זו תקפה גם כאשר מדובר במחשב בודד או במספר מחשבים המחוברים באמצעות רשת תקשורת נתונים, וכן בהתייחס למצעים פיזיים (רשומות, דיסקים, דיסקטים וכדומה).

3.3. **סיווג מידע:** הקניית הגדרת יחוס רגישות למידע ו/או למערכת ברמת המשרד וכן מתוקפם של חוקים ותקנות, כבסיס לטיפול אבטחתי.

3.4. **נזק** – פגיעה במשרד האוצר מבחינה כספית ו/או תפעולית ו/או תדמיתית למשרד, לעובדיו, לציבור ולמדינת ישראל בין שניתן לכמת את הנזק ובין שלא.

3.5. **איום הייחוס**: גרימת נזק (שיבוש, שינוי, מחיקה, העתקה או חשיפה של כל מידע בפני

גורמים בלתי מורשים) הגורם פגיעה במידע יכולה להתרחש בשוגג, במתכוון או ע"י אסונות טבע (שריפה, הצפה, רעידת אדמה וכיוצא בזה).

3.6. **מידע רגיש ממשלתי:** מידע השייך למשרד ומטופל במסגרת עבודתו השוטפת ואשר חשיפתו או הפגיעה בו עלולות לגרום לנזק (על פי "נוהל טיפול באירועי אבטחת מידע") לעבודת המשרד ו/או למדינה, או שחלה עליו הגדרת "מידע רגיש" מתוקף הוראת חוק הגנת הפרטיות 1981, התשמ"א.

3.6.1. **ללא סיווג**: מידע הפתוח לעיון הציבור, מידע שחשיפתו באופן בלתי מורשה או שיבוש בו לא יגרמו נזק, או מידע אשר יש לפרסמו על-פי דין, למעט "מידע" ו"ידיעה" על ענייניו הפרטיים של אדם כמשמעותם בחוק הגנת הפרטיות.

3.6.2. **פנימי**: מידע שחשיפתו באופן בלתי מורשה או שיבוש בו עשוי לגרום נזק לאינטרס ציבורי, או מידע שלא הותר לפרסום בהתאם להליך המקובל.

3.6.3. **חסוי** "ובכלל זה" **חסוי אישי**: מידע אשר פגיעה בחסיונו, שלמותו, מהימנותו, זמינותו ושרידותו עלולה לגרום לפגיעה בניהולו התקין של המשרד ו/או משרדי ממשלה אחרים ו/או במדינה או גופים ציבוריים אחרים ו/או לפגוע בפרטיות על פי הגדרת החוק.

3.6.4. **חסוי ביותר**: מידע אשר פגיעה בחסיונו , שלמותו, מהימנותו, זמינותו ושרידותו עלולה לגרום לפגיעה קשה ומתמשכת בניהולו התקין של המשרד ו/או משרדי ממשלה אחרים ו/או במדינה או גופים ציבוריים אחרים.

4. אחריות

4.1. באחריות ועדת ההיגוי לנושא הגנת המידע והסייבר לגבש ולהתוות את מדיניות ועקרונות סיווג המידע. באחריות ראש תחום מערך סייבר חירום וביטחון לאכוף את מימוש אבטחת המידע בהתאם לסיווג המידע.

4.2. אחריות יישום ותפעול הנוהל חלה על הגורמים הבאים כל אחד בתחומו כמפורט בנוהל:

4.2.1. משתמשים.

4.2.2. צוות תמיכה.

4.2.3. צוות System.

4.3. ראש תחום הגנת המידע והסייבר יבקר יישום הנחיות נוהל זה.

- פנימי-

4.4. אחריות עדכון נוהל זה, בהתאם לצורך, חלה על ראש תחום הגנת המידע והסייבר.

4.5. אחריות פיקוח: מבקר המשרד וגוף שיקבע לנושא בהחלטות הממשלה.

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 A 8.2.

6. שיטה

6.1. תהליך סיווג המידע

6.1.1. ראש תחום הגנת המידע והסייבר יגבש, בתיאום עם מנהל אגף חירום וביטחון, קריטריונים להגדרת סיווג רגישות המידע וחיוניותו, לפי מידת הנזק שייגרם למשרד, למדינת ישראל ו/או לגורמים אחרים, כתוצאה מחשיפה, חבלה, מחיקה או שיבוש של המידע, מאגריו או מערכותיו, בין אם במזיד ובין אם בשוגג.

6.1.2. סיווג המידע יתייחס לכל מצע או מאגר בהם קיים המידע (קבצים, בסיסי נתונים, מצעי מדיה מגנטיים או אופטית, עותקים קשיחים (נייר) וכדומה).

6.1.3. הסיווג יתבסס על הנזק הפוטנציאלי שעשוי להיגרם באם תיפגע רמת הסודיות, השלמות, הזמינות, הכלילות (Integrity) או השרידות של המידע או הנכס.

6.1.4. סיווגו של המידע יקבע בהתאם לרמת הרגישות הגבוהה ביותר הקיימת בקובץ, במאגר או במצע הפיזי בהם אגור המידע (על-פי עקרון "המחמיר קובע").

6.1.5. סיווג של מערכות או אפליקציות יוביל להגדרת רמת האבטחה הנדרשת, תוך התייחסות לרמת ההזדהות, רמת המידור, רמת הבקרה, צורך בהצפנה וכיו"ב. רמת האבטחה הנדרשת עבור כל מערכת תאושר על-ידי מנהל תחום הגנת המידע והסייבר באגף חירום וביטחון.

6.1.6. סיווג המידע ייקבע על-ידי מפיק המסמך או הקובץ או על-ידי בעל המידע, במקרה של סיווג מאגרי מידע, מערכות, אפליקציות (סיווג נכסים), על פי הנחיות ראש תחום

הגנת המידע והסייבר.

6.1.7. הסיווג של מערכת חדשה יתבצע כבר בשלב האפיון של המערכת, על מנת לאפשר את שילובם של אמצעי האבטחה הנדרשים בשלב הפיתוח.

6.2. סימון ושמירת מידע מסווג

6.2.1. רמות הסיווג יתוו את דרכי הטיפול במידע ויתבססו על הסיכונים הפוטנציאליים הרלוונטיים למשרד והמוגדרים באופן דינאמי במסגרת ביצוע סקרי הסיכונים המתקיימים במשרד האוצר מעת לעת.

6.2.2. יחד עם זאת, רמות סיווג המידע מבוססות על רמת רגישותו, ומתייחסות לכל תצורה שבה נשמר המידע (אם במערכות המחשוב, אם במסמכים ואם במדיה מגנטית/אופטית).

6.2.3. עובדי המשרד יסווגו באופן עצמאי מסמכים אשר נוצרים על-ידם (כגון מסמכי Office), בהתאם להנחיות הסיווג, אשר יופצו על-ידי ראש תחום הגנת המידע והסייבר.

6.2.4. לגבי כל רמת סיווג יסווגו משאבי המידע וייקבעו בהתאם לחוק ומדיניות הממשלה, דרישות אבטחת מידע, הנוגעות לרמת מידורו, ולאופן שמירתו, תיוגו, העתקתו, שליחתו ומחיקתו של המידע. דרישות אבטחת המידע יוגדרו על-ידי ראש תחום הגנת המידע והסייבר .

6.2.5. במערכות מידע יקבע סיווג המידע ע"י בעל המידע או מנהל המערכת בתאום ואישור ראש תחום הגנת המידע והסייבר במשרד.

6.2.6. הסמכות הבלעדית לשינוי סיווג המידע, לאחר קביעתו, ניתנת לגורם אשר סיווג את המידע במקור, לרבות מידע בקבצים, מאגרי או מערכות מידע.

6.2.7. בהתאם לסיווג המידע תקבע רמת האבטחה ואופן הטיפול במידע ע"י מפיק וע"י כל עובד במשרד המחזיק במידע.

6.2.8. סיווג המידע יסומן ("תויג") בראש כל עמוד במסמך / בקובץ באמצעות הקלדה ישירה של הסיווג או באמצעות מדבקה הנושאת את רמתו של הסיווג, על-גבי דיסקים, קלטות, ומצעים פיזיים אחרים. כמו כן, יש לרשום את הסיווג על-גבי מעטפות המשונעות בתוך המשרד. זאת, על-מנת לציין בפני מקבלי המעטפה את רמת רגישות החומר הנמצא במעטפה, בכדי שניתן יהיה לספק רמת אבטחה נאותה עד לפתיחתה או עד לפיזור החומר שבתוכה (משם, יבוצע טיפול אבטחתי פרטני, לכל

- פנימי-

מסמך בנפרד, בהתאם לסיווגו).

6.3. הטמעה

6.3.1. הגברת מודעותם של עובדי המשרד בנושא סיווג המידע תבוצע באמצעות מידע מודפס ולומדות הדרכה אשר יכילו את פירוט רמות הסיווג, דוגמאות ודרכי הטיפול במידע בהתאם לרמות הסיווג.

6.4. אכיפה

6.4.1. המנהלים במשרד אחראים לסייע בידי עובדיהם בסיווג המידע המופץ על ידם.

6.4.2. ראש תחום הגנת המידע והסייבר ישקול וינחיל פעולות מתקנות לפי הצורך (ריענון הנחיות בקרב עובדים ו/או יחידות ארגוניות רלוונטיות, טיפול משמעתי וכיוצא באלו).

6.5. טיפול בחריגים

6.5.1. כל בעיה או ספק הקשורים בסיווג מידע או העלולים להשליך על אבטחת המידע במשרד, ידווחו מידית למנהלים הרלוונטיים, אשר יספקו מענה מקצועי מידי וישקלו המשך דיווח לראש תחום הגנת המידע והסייבר ולגורמים אחרים, לפי הצורך.

6.5.2. ראש הגנת המידע והסייבר יטפל בבעיות חריגות ברמה ארגונית, בהיבטי עקרונות הסיווג או הטיפול במסגרת יחידות ארגוניות ספציפיות, וישקול שינויים במדיניות הסיווג ו/או בהנחיות, לפי הצורך ובאישור ועדת ההיגוי לנושאי אבטחת מידע.

תבנית לרישום מערכות המידע במשרד וסיווגן

שם המערכת	מקום	מע' הפעלה	יישום עיקרי	ממשק חיצוני	מנהל מערכת	סיווג	רגישות	קריטיות