



מדינת ישראל
משרד המשפטים

מדיניות ביטחון מידע

והגנה בסייבר

משרד המשפטים

מהדורה	שם	תפקיד	תאריך
1	אמי פלמור	מנכ"לית משרד המשפטים	27.3.2016

משרד המשפטים - מדיניות אבטחת מידע

עמוד 2 מתוך 15

נוהל זה הינו רכוש הבלעדי של משרד המשפטים
נוהל זה מצריך בדיקת עדכניות תקופתית כל 12 חודשים מיום : 2/9/2018
לתשומת לבך - עם הדפסת הנוהל, המסמך יהפוך להיות בלתי מבוקר ותוקפו יפוג שבוע מתאריך 13/02/2020

משרד המשפטים - מדיניות אבטחת מידע

1. רקע:

מסמך מדיניות זה נכתב לאור ההוראה לפעול ליישום תקן ISO27001 אשר נקבעה בהחלטת ממשלה מס' 2443.

תכלית המסמך:

הרשות מחזיקה במידע כנאמן הציבור וכי על פי חוק חופש המידע, תשנ"ח-1998 קיימת זכות לכל אדם לעיין במידע, עיון במידע ברשות ציבורית מוגבל למקרים בהם יש אינטרס ציבורי בחיסיון המידע, מכאן שמדיניות ביטחון מידע והגנה בסייבר במשרד, תכליתה לספק את ההגנה הראויה למידע המוגדר כמסווג או חסוי.

מדיניות ביטחון מידע והגנה בסייבר במשרד המשפטים (להלן "המשרד"), מהווה את התשתית להחלטות ההנהלה הקשורות לניהול מידע במשרד, ולפיה יש לתת מענה ארגוני כולל, לרבות אמצעים ומשאבים כלכליים, תוך הטמעה של תהליכי קבלת החלטות בנושאי מידע, ניהולן ובקרה על יישומן וזאת במסגרת אחריות מוגדרת של בעלי תפקידים במשרד המשפטים.

פעילותו התקינה של המשרד מושפעת ותלויה ברמת שלמות המידע המנוהל על ידי המשרד, סודיותו, אמינותו, עדכניותו, זמינותו ושרידותו.

2. מטרה:

התוויית מדיניות ביטחון מידע והגנה בסייבר במשרד, באופן שימזער פגיעה אפשרית במידע ובמערכות אגירתו ובכך תצמצם את החשיפה לסיכוני הפגיעה בתפקודו הסדיר של המשרד ואת סיכוני הפגיעה בפרטיות עובדי המשרד ואזרחים.

3. יישום המדיניות

3.1. משרד המשפטים מחויב כלפי מטרות ועקרונות ביטחון מידע והגנה בסייבר המפורטים במסמך זה. משרד המשפטים מכיר בחשיבות ביטחון מידע והגנה בסייבר ובחשיבות הטמעת עקרונות ביטחון מידע והגנה בסייבר בקרב עובדי המשרד.

3.2. משרד המשפטים מחויב לעקרונות מדיניות ביטחון מידע והגנה בסייבר, תוך ניהול והקצאת המשאבים ההולמים לקיום תקין של אכיפת ההליכים, והטמעת השיטות והכלים אשר יוגדרו מכוח מסמך זה.

3.3. ועדת ההיגוי בנושא תקשוב והגנת המידע אחראית על גיבוש ועדכון מסמך מדיניות זה ועל בסיסו להתוות נהלים ליישומן, לפקח על תכניות העבודה השנתיות, לקיים הערכת נזקים בעקבות תקלות ולגבש המלצות לטיפול והקצאת משאבים לניהול ואכיפת הנושא.

3.4. ממונה ביטחון מידע והגנה בסייבר אחראי להנחיה שוטפת בתחום ביטחון מידע והגנה בסייבר ובקרה על ביצוע החלטות וסיכומי ועדת ההיגוי בנושא תקשוב והגנת המידע.

3.5. האחריות לסיווג המידע ואבטחתו חלה על בעל המידע או מנהלו, בהתאם להנחיית ממונה ביטחון מידע והגנה בסייבר.

3.6. האחריות על ביטחון מידע והגנה בסייבר הינה על בעל המידע.

עמוד 3 מתוך 15

משרד המשפטים - מדיניות אבטחת מידע

4. שיטה:

4.1. ביטחון מידע והגנה בסייבר במשרד המשפטים תתבצע באמצעות מערך ביטחון מידע והגנה בסייבר המורכב מגופים אלה: ועדת ההיגוי, ממונה ביטחון מידע והגנה בסייבר, מנהל ביטחון מידע והגנה בסייבר באגף מערכות מידע ונאמן ביטחון מידע והגנה בסייבר יחידתי.

4.2. ביטחון מידע והגנה בסייבר כוללת את התחומים הבאים, המהווים את "חמשת מעגלי האבטחה":

4.2.1. אבטחה פיזית.

4.2.2. אבטחת רשומות.

4.2.3. אבטחה לוגית.

4.2.4. מהימנות עובדים.

4.2.5. אבטחת ממשקים עסקיים.

4.3. ביטחון מידע והגנה בסייבר במשרד תיושם בכפוף ובצמידות לחוקים, לתקנות והנחיות הנוגעים לתחום ביטחון מידע והגנה בסייבר, לרבות הנחיית הרשות הממלכתית לביטחון מידע והגנה בסייבר מכוח החוק להסדרת הביטחון בגופים ציבוריים התשנ"ח-1998, הנחיות הרשות להגנת הפרטיות (לשעבר רמ"ט) מכוח **חוק הגנת הפרטיות, התשמ"א-1981** (להלן: "**חוק הגנת הפרטיות**"), נציבות שרות המדינה מכוח התקש"יר ובהתייחס להחלטות ועדת ההיגוי בנושא תקשוב והגנת המידע.

4.4. מערך ביטחון מידע והגנה בסייבר יישאף להתאים לדרישות התקן ת"י ISO 27001, בהתאם להתוויה שהוגדרה בהחלטת הממשלה מס' 2443.

5. הגדרות:

5.1. **ביטחון מידע והגנה בסייבר**: מכלול הפעולות והאמצעים הננקטים והמיושמים במשרד, שמטרתם להביא לכך שהמידע ורכיבי החומרה היוצרים אותו, מאחסנים אותו ומטפלים בו, יוגנו מפני פגיעה, חשיפה או שינוי, במזיד או בשוגג, הן מתוך המשרד והן מחוצה לו על מנת שהמידע יהיה אמין, וזמין בכל עת לעובדי המשרד המורשים לו מתוקף תפקידם.

5.2. **אבטחה פיזית**: הינה הפעולה למתן הגנת פיזית למידע, תהליכים, אנשים וכלים – באמצעות יישום בקורות (מנעולים, מצלמות, כספות, דלתות, מאבטחים וכו').

5.3. **מידע**: כל נתון הנוגע או הקשור לפעילותו, תפעולו או תפקודו של המשרד, וכן כל נתון אודות אדם מזוהה או ניתן לזיהוי ומידע ממשלתי רגיש, הקיים על-גבי אמצעי אחסון ממוחשבים, מגנטיים, אופטיים או אלקטרוניים, על-גבי מצעים פיזיים וכן המועבר בעל-פה.

5.4. **מידע רגיש**: כל מידע אשר סווג ברמת פנימי ועד רמת חסוי ביותר.

5.5. **ביטחון מידע והגנה בסייבר**: מכלול הפעולות והאמצעים הננקטים והמיושמים במשרד, שמטרתם להביא לכך שהמידע ופריטי הציווד היוצרים אותו, מאחסנים אותו ומטפלים בו, יוגנו מפני פגיעה, חשיפה או שינוי, במזיד או בשוגג, הן מן המשרד והן מחוצה לו.

עמוד 4 מתוך 15

משרד המשפטים - מדיניות אבטחת מידע

5.6. ועדת ההיגוי בנושא תקשוב והגנת המידע (להלן "ועדת ההיגוי"): ועדה ניהולית בראשות המנכ"ל ובהשתתפות הנציגים הבאים:

- המנהל הכללי – יו"ר.
- סמנכ"ל בכיר (תפעול ולוגיסטיקה) – חבר
- סמנכ"ל בכיר (תכנון מדיניות ואסטרטגיה) – מ"מ יו"ר
- היועצת המשפטית – חברה
- מנהל אגף בכיר (מערכות מידע) – חבר
- מנהל אגף בכיר (ביטחון, חירום, מידע וסייבר) – חבר
- חשב בכיר משרד המשפטים – חבר
- מנהל אגף א (תקציבים) – חבר
- מנהל אגף א (ערוצי השירות והמידע) – חבר
- ראש רשות התאגידיים – חבר
- סגן האפוטרופוס הכללי והכונס הרשמי – חבר
- מנהל המרכז לשירותי ניהול, פרקליטות המדינה – חבר
- מרכזת הועדה – מוזמנת קבועה
- ממונה ביטחון מידע והגנה בסייבר – מוזמן קבוע
- מנהל ה-PMO באגף מערכות מידע – מוזמן קבוע
- מנהל ביטחון מידע והגנה בסייבר באגף מערכות מידע – יוזמן על פי צורך על ידי מנהל אגף בכיר (מערכות מידע)

ועדת ההיגוי נועדה לגבש ולעדכן את מדיניות המשרד בתחום ביטחון מידע והגנה בסייבר, להתוות אסטרטגיות פעילות, לפקח אחר תכניות העבודה השנתיות, לקיים הערכת נזקים בעקבות תקלות ולגבש המלצות לטיפול.

5.7. **ממונה הגנת סייבר** – גורם ניהולי בכיר, הממונה על ידי המנכ"ל בנוסף על תפקידו העיקרי, אשר משימתו ואחריותו הינן להוביל את ההיערכות הארגונית ולבקר את מימוש המדיניות בתחום הגנת הסייבר ובכלל זה: ניהול אסטרטגיה, תשתיות, כוח אדם, מדיניות, אכיפה, מודעות ארגונית לנושאי אבטחה ונושאים נוספים.

5.8. **ממונה ביטחון מידע והגנה בסייבר**: (להלן "הממונה") בעל תפקיד, כפוף לממונה הגנת סייבר, המהווה מנחה מקצועי בתחום ביטחון מידע והגנה בסייבר, גורם זה הינו מוסמך/מומחה במתודולוגיות הגנת סייבר אשר השלים את הידע הנדרש בטכנולוגיות הגנה או, לחילופין, מוסמך/מומחה בטכנולוגיות הגנת סייבר אשר השלים את הידע הנדרש

עמוד 5 מתוך 15

משרד המשפטים - מדיניות אבטחת מידע

במתודולוגיות הגנת סייבר, הגורם המוביל, המדריך והמבקר את התהליכים בתחום ביטחון מידע והגנה בסייבר והגנת סייבר כלפי יחידות המשרד.

5.9. **מנהל ביטחון מידע והגנה בסייבר באגף מערכות מידע**: מנהל מקצועי בתחום טכנולוגיות ביטחון מידע והגנה בסייבר וסייבר, הכפוף להנחיות הממונה, שותף לתהליכי עיצוב ופיתוח מערכות מידע. מוביל בחירה יישום והטמעה של טכנולוגיות לביטחון מידע והגנה בסייבר והסייבר. מבקר את תהליכי העבודה באגף מערכות מידע ואחראי על יישום מדיניות ביטחון מידע והגנה בסייבר באגף מערכות מידע. מדווח לממונה ביטחון מידע והגנה בסייבר על שינויים מהותיים, חריגות, תקלות ואירועי ביטחון מידע והגנה בסייבר הדורשים התייחסות של הממונה.

5.10. **נאמן ביטחון מידע והגנה בסייבר**: בכל יחידה ייקבע ע"י מנהל היחידה עובד אשר ישמש כנאמן ביטחון מידע והגנה בסייבר, נאמן ביטחון מידע והגנה בסייבר יונחה מקצועית על-ידי ממונה ביטחון מידע והגנה בסייבר והמסייעים בידו לקיים וליישם את פעילות ביטחון מידע והגנה בסייבר השוטפת ביחידה בשטח, ו/או ביחידות המרוחקות, כמוגדר על-ידי ממונה ביטחון מידע והגנה בסייבר וכנגזר משיטות, תהליכי וכלי העבודה המיושמים.

5.11. **בעל המידע**: מנהל (עובד המשרד) אשר הוגדר שכזה על-ידי המשרד, המשתמש העיקרי במידע בתחום מסוים או שהמידע נוצר בתחום אחריותו. בעל המידע יסייע בהגדרת סודיות, רגישות וחיוניות המידע וימליץ בפני ממונה ביטחון מידע והגנה בסייבר על סיווג של המידע ועל הטיפול הנגזר מכך.

5.12. **עובד המשרד**: עובד עבר וסיים את שלבי הקליטה הניהוליים אשר הופכים אותו לעובד מן המניין במשרד ו/או בגינו משלם המשרד שכר לחברה מטעמה מועסק העובד במשרד (OUTSOURCING) ו/או בעל חוזה העסקה, ישיר או עקיף עם המשרד, המבצע את תפקידו או מקיים את החוזה בתחומי או חצרי המשרד.

5.13. **אורח**: גורם שאינו נמנה על עובדי המשרד, אשר קיבל היתר מוגבל בזמנים לשהות במתחם העבודה או במערכות המחשב של המשרד ולהיחשף או לעשות שימוש במידע, בכפוף לנוהלי המשרד.

5.14. **שימוש אסור**: פעולה הכרוכה בשימוש כלשהו במידע, המבוצעת מבלי לקבל היתר לביצועה על-פי נהלי המשרד וכן פעולה שהותרה לביצוע, אך אינה תקינה בנסיבות ביצועה.

5.15. **עקרון "הצורך לדעת" (Need to Know)**: הגבלת הגישה למידע לבעלי התפקידים הזקוקים לו בלבד ועמידה בעיקרון הפרדת תפקידים. עקרון זה קובע הפרדה בין הגורמים השונים האחראים לביצוען של פעולות בארגון, כגון הפרדה בין גורם מבצע, מאשר ומבקר. המטרות העיקריות ביישום של מערך הרשאות נאות ועיקרון הפרדת התפקידים בארגון הינה מניעת טעויות ומעשי מרמה וכן הימנעות מיצירת תלות בפונקציה עיקרית אחת ושליטת גורם יחיד על תהליך שלם.

5.16. **פרופיל משתמש (User profile)**: אוסף הנתונים האישיים הנשמרים עבור משתמש קצה מסוים. פרופיל המשתמש נשמר על ידי כל מערכת המעוניינת בכך, אתה המשתמש בא במגע, החל מיישומים המעוניינים לשמור את הגדרות ממשק המשתמש, דרך מערכת הפעלה המעוניינת לשמור את פעולותיו האחרונות של המשתמש לצורך נוחות בהפעלה נוספת, וכלה באתר אינטרנט המכיל מידע אישי אותו הוא מציג

משרד המשפטים - מדיניות אבטחת מידע

למשתמש בכל פעם שזה גולש אליו. פרופיל משתמש אם כן הוא הייצוג הדיגיטלי של זהותו של אדם מסוים בעיני תוכנה מסוימת

6. מיפוי מידע:

6.1. המידע ימופה לפי סוגי המידע הקיימים במשרד (אחד או יותר):

6.1.1. מידע בטחוני.

6.1.2. מידע אישי, המוגן על פי חוק הגנת הפרטיות, או לפי התקנות שהותקנו בהתאם לחוק הגנת הפרטיות, או בהתאם להנחיות הרשם.

6.1.3. מידע כלכלי או מסחרי.

6.1.4. מידע על אודות מדיניות ציבורית בהתהוות.

6.1.5. מידע שקיים לגביו חיסיון לפי דין.

6.1.6. מידע הנוגע לשלום הציבור ו/או לשלום היחיד.

7. עקרונות ביטחון מידע והגנה בסייבר:

7.1. סיווג המידע

7.1.1. בנהלי המשרד יקבעו סיווגי רגישות לעניין מידע שאינו בטחוני, בהתאם ל- 4 הרמות הבאות:

7.1.1.1. **מידע ללא סיווג:** מידע הפתוח לעיון הציבור, מידע שחשיפתו או שיבוש בו לא יגרמו כל נזק, או שייגרם בשל כך נזק שאינו חמור, או מידע שיש לפרסמו בהתאם לדין. למעט "מידע" וידיעה על ענייני הפרטיות של אדם כמשמעותם בחוק הגנת הפרטיות.

7.1.1.2. **מידע פנימי:** מידע שחשיפתו באופן בלתי מורשה או שיבוש בו עשויים לגרום נזק לאינטרס ציבורי, או מידע שלא הותר לפרסום בהתאם להליך המקובל. ככלל כל מידע שנוצר במשרד המשפטים מהווה מידע פנימי.

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

7.1.1.4. **מידע חסוי ביותר:** מידע אשר פגיעה בחסיונו, שלמותו/מהימנותו, זמינותו ושרידותו עלולה לגרום לפגיעה מתמשכת בניהולו התקין של המשרד או משרדי ממשלה או במדינה או בגופים ציבוריים.

7.1.2. מנהל היחידה יגבש בתאום עם ממונה ביטחון מידע והגנה בסייבר קריטריונים להגדרת סיווג רגישות המידע וחיוניותו, לפי מידת הנזק שעשוי להיגרם לאזרח, למשרד המשפטים ולמדינת ישראל או לצד שלישי, כתוצאה מחשיפה, חבלה או שיבוש של המידע, מאגריו או מערכותיו, בין אם במזיד ובין אם בשוגג.

עמוד 7 מתוך 15

משרד המשפטים - מדיניות אבטחת מידע

7.1.3. סיווג המידע יתייחס לכל מצע או מאגר בהם קיים המידע (קבצים, בסיסי נתונים, מצעי מדיה אלקטרונית או אופטית, מסמכים, דו"חות, מידע בע"פ וכד').

7.1.4. סיווגו של המידע יקבע בהתאם לרמת הרגישות הגבוהה ביותר הקיימת בקובץ, במאגר או במאגר הפיזי בהם אגור המידע

7.1.5. ממונה ביטחון מידע והגנה בסייבר יקבע את רמת האבטחה הנדרשת לכל סיווג ויגדיר את משאבי הגנת המידע בהתאם בתיאום עם מנהל אגף התקציבים של המשרד.

7.2. מידור

7.2.1. יבוצע מידור של המידע ושל המשתמשים בו בהתאם לעקרון "הצורך לדעת" או הצורך להגן על המידע בהתאם לרמת רגישותו.

7.2.2. מידור המידע יעשה על ידי חלוקת המידע והמשתמשים לקבוצות שייכות או עניין ובהתאם לסביבות העבודה (פרופיל משתמשים).

7.2.3. עקרונות המידור יוגדרו בנוהל מפורט אשר יופץ בכל יחידות המשרד.

7.3. רמת ביטחון מידע והגנה בסייבר מחייבת

7.3.1. רמת ביטחון מידע והגנה בסייבר מחייבת תקבע בנוהל המחייב את בעל המידע, מאגריו ומערכותיו בהתאם לרמת רגישות החומר.

7.3.2. רמת האבטחה תקיף ותכסה את המידע על כל התחומים הנגזרים ממנו (אבטחה פיזית, אבטחת רשומות, אבטחה לוגית, אבטחת מהימנות עובדים ואבטחת ממשקים עסקיים).

7.3.3. רמת האבטחה בכל מערכת מידע לא תהיה פחותה מרמת האבטחה של המידע ברמת הסיווג הרגילה ביותר שמנוהל על ידי מערכת המידע.

7.3.4. רמת ביטחון מידע והגנה בסייבר בכל המערכות ומתקני המשרד לא תהיה פחותה מרמת האבטחה המחייבת הנמוכה ביותר שתקבע.

7.3.5. כל דרישה לחריגה מרמה זו תובא, מנומקת, לאישור ממונה ביטחון מידע והגנה בסייבר אשר יינתן מראש ובהתאם להוראות הדין ולתכנית ניהול הסיכונים.

7.4. ניהול סיכונים

7.4.1. עקרונות ביטחון מידע והגנה בסייבר יתבססו על נוהל ניהול סיכונים, אשר נועד לזהות, לבקר, למזער, או מונע את סיכוני האבטחה העלולים להשפיע על המידע, מאגריו או מערכותיו.

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

7.4.3. השיטות והכלים הנדרשים לביטחון מידע והגנה בסייבר יוגדרו בהתאם להערכת הסיכונים.

עמוד 8 מתוך 15

משרד המשפטים - מדיניות אבטחת מידע

7.5. בקרה ושיפור מתמיד:

- 7.5.1. ממונה ביטחון מידע והגנה בסייבר יפעיל שיטת מדידה, אשר תאפשר למדוד את רמת אפקטיביות ניהול ביטחון מידע והגנה בסייבר והקטנת הסיכונים.
- 7.5.2. בכל יחידה בה מעובד מידע בסיווג חסוי וחסוי ביותר, יערך אחת לשנתיים סקר פנימי לבחינת תהליכי ביטחון מידע והגנה בסייבר, על מנת להעריך את מידת עמידת היחידה בנהלי ביטחון מידע והגנה בסייבר שנקבעו.
- 7.5.3. תשומה של כל סקר פנימי תועבר לתוכנית שיפור אשר תוודא שיפור מתמיד של מערכת ביטחון מידע והגנה בסייבר. כל בעלי העניין יעודכנו אודות כל השיפורים שנעשו.

7.6. מעגלי האבטחה

7.6.1. אבטחה פיזית

- 7.6.1.1. מדיניות האבטחה הפיזית במשרד, מורכבת ממספר "מעגלי אבטחה", אשר במרכזם ניצבים נכסיו אשר הוגדרו ברי אבטחה, לרבות מידע, האמור להיתפס כאחד מן הנכסים העיקריים והמהותיים ביותר במשרד.
- 7.6.1.2. מעגל האבטחה הפיזי החיצוני כולל את היבטי האבטחה הפיזיים אשר נותנים מענה ראשון למתקפות כנגד המשרד (במכוון או בשוגג), באשר הן. מעגל זה כולל בעיקרו אבטחה היקפית למתקני המשרד ובקרת כניסה.
- 7.6.1.3. מעבר להגדרת האבטחה הפיזית החיצונית יוגדרו מעגלי אבטחה פיזית פנימיים בתוך המתקנים. יוגדרו הרשאות גישה למקומות שונים בהתאם לרגישותם, רגישותן הגבוהה של המערכות הממוחשבות וחיבתותן של המידע האגור בהן, מחייבים מידור פיזי של מורשי הגישה למערכות אלו. אמנם קיימים מעגלי אבטחה נוספים (לוגיים, בין היתר) אשר נועדו למנוע נגישות בלתי מורשית למידע, אך אין להתבסס עליהם בלבד ויש למנוע נזקים פוטנציאליים עוד באיבם, תוך איתורם באפיקים הפיזיים, כבר בכניסות לבניין, ב"אזורים הסטריליים" וכדומה (בטרם יגיעו כלל למערכות הממוחשבות עצמן).
- 7.6.1.4. מנהל אגף בכיר חירום, ביטחון מידע וסייבר יקבע לכל מתקן את רמת אבטחה פיזית המחייבת בהתאם לרמת סיווג הרגישות. ובכלל זה יקבע:
- 7.6.1.4.1. דרישות אבטחה למבנה ותנאים סביבתיים.
 - 7.6.1.4.2. שיטות וכלים למידור כניסה לאזורים מאובטחים.
 - 7.6.1.4.3. תהליכים ואמצעי בקרה (לדוגמא: טלוויזיה במעגל סגור ומצלמות אבטחה, מאבטחים, תגי כניסה).
 - 7.6.1.4.4. טיפול באירועים חריגים.
 - 7.6.1.4.5. אופן ביצוע פיקוח ובקרה.

7.6.2. אבטחת רשומות

עמוד 9 מתוך 15

משרד המשפטים - מדיניות אבטחת מידע

7.6.2.1. רשומות מידע הוא מונח המתאר אמצעי מידע פיזיים כגון מסמכים, תדפיסים, דיסקים, קלטות וסרטים.

7.6.2.2. אבטחת רשומות חיונית משום קיומו של מידע רגיש רב על-גבי מצעים פיזיים אשר הגעתם לידיים עוינות עלולה להוביל לנזקים. בנוסף לסיכוני ביטחון מידע והגנה בסייבר הקיימים לרשומות הנמצאות בשטח העבודה במשרד, מידע ברשומות עשוי לעתים להימצא מחוץ לשטח המשרד (לצרכי ישיבות או עבודה מרחוק וכן משום השלכת מסמכים לפחי אשפה הנלקחים מחוץ לבניין), שם הינו חשוף לסיכונים נוספים.

7.6.2.3. ממונה ביטחון מידע והגנה בסייבר יגדיר בנהלים את אמצעי ותהליכי הטיפול באבטחת רשומות, בהתאם לרגישות המידע. תחומי ההתייחסות יכללו:

7.6.2.3.1. שיטות וכלים לביטחון מידע והגנה בסייבר והשמדתו, בהתאם לסיווג המידע.

7.6.2.3.2. תהליכי ואמצעי שינוע מידע (פנים וחץ ארגוני).

7.6.2.3.3. טיפול באירועים חריגים.

7.6.2.3.4. אופן ביצוע פיקוח ובקרה.

7.6.3. אבטחה לוגית

7.6.3.1. האבטחה הלוגית מהווה את ה"שכבה" העיקרית והקרובה ביותר בהגנה על המידע המצוי במערכות המחשב והתקשורת.

7.6.3.2. יישום שגוי או אי יישום של "שכבה" זו, עשוי להביא לחשיפת המידע לגורמים שאינם מורשים, ולהסב נזק רב למשרד, לעובדיו או לפרטיות נושאי המידע.

7.6.3.3. תקבע רמת האבטחה הלוגית המחייבת עבור רכיביהן השונים של מערכות המחשב והתקשורת.

7.6.3.4. תיושם הגנה לוגית במערכות ההפעלה, בתוכנות ובאפליקציות, בקבצי ובבסיסי נתונים, בפעולות שינוי של הנתונים (ברמת הרשומה, השדות וסוג הפעולה) ובתקשורת.

7.6.3.5. תחומי התייחסות בהיבטים הלוגיים יכללו התוויה, הגדרה ובקרת יישום של:

7.6.3.5.1. שיטות וכלים לביטחון מידע והגנה בסייבר במערכות המחשב והתקשורת, בהתאם לסביבות העבודה ולהגדרות הפרופילים שיקבעו.

7.6.3.5.2. טיפול באירועים חריגים.

7.6.3.5.3. אופן ביצוע פיקוח ובקרה.

7.6.4. מהימנות עובדים

עמוד 10 מתוך 15

משרד המשפטים - מדיניות אבטחת מידע

7.6.4.1. יושרם ומהימנות העובדים מהווים הבסיס לביטחון מידע והגנה בסייבר, מעצם חשיפת העובדים למידע ומתוקף היותם המפעילים, המאפיינים, המתחזקים והמשתמשים במערכות המידע, מאגריו ומצעיו.

7.6.4.2. על האחראים במשרד הקולטים עובדים חדשים או משנים הרשאות גישה לעובדים קיימים, לוודא יישום הליכי בקרה הנוגעים ליושרם ולאמינותם של העובדים.

7.6.4.3. ממונה ביטחון מידע והגנה בסייבר ימליץ למנהל אגף הביטחון על הסיווגים הביטחוניים הנדרשים מעובדי המשרד, תוך התייחסות לקריטריונים ספציפיים הנוגעים לרגישות המידע אליו יחשפו.

7.6.4.4. מנהל אגף הביטחון יאשר את סיווגי משרות במשרד, תוך התייחסות לקריטריונים ספציפיים הנוגעים לרגישות המידע אליו יחשפו בעלי התפקידים.

7.7. איסור שינוי לא מבוקר

7.7.1. יוגדרו נהלים המתווים את אופן ביצוע השינויים בנתונים, בתוכנות יישומיות, בתוכנות תשתית ובחומרה, של מערכות המשרד.

7.7.2. חל איסור על ביצוע שינוי במידע שלא במהלך הפעילות הרגילה, בתוכנה יישומית, ובהתאם להנחיות, תוך התייעצות עם גורמי ההנהלה הרלוונטיים.

7.7.3. תבוצע הפרדה בין סביבות פיתוח, בדיקות יישומים ומערכות לבין סביבת הייצור במערכות.

7.7.4. מנהל אגף מערכות מידע יגדיר את העקרונות, האמצעים והתהליכים ליישום שינויים מבוקרים.

7.7.5. ממונה ביטחון מידע והגנה בסייבר יבקר את הנהלים והתהליכים הנדרשים לקיומה של בקרת השינויים כמוגדר.

7.8. שינויים טכנולוגיים

7.8.1. שינוי מהותי במפרטים הטכניים של מערכות המידע במשרד, העשוי לשנות את מצב ביטחון מידע והגנה בסייבר, מחייב מעורבות מראש של מנהל ביטחון מידע והגנה בסייבר באגף מערכות מידע, ידוע מראש של ממונה ביטחון מידע והגנה בסייבר וביצוע ניהול הסיכונים.

7.9. ביטחון מידע והגנה בסייבר בתהליך הפיתוח והתחזוקה

7.9.1. מנהל ביטחון מידע והגנה בסייבר באגף מערכות מידע, אחראי להגדרת דרישות ביטחון מידע והגנה בסייבר, בנושאים שבפיתוח ובתחזוקה.

7.9.2. ממונה ביטחון מידע והגנה בסייבר יבקר את עמידת תהליכי הפיתוח והתחזוקה במדיניות שנקבעה.

7.10. גיבויים

עמוד 11 מתוך 15

משרד המשפטים - מדיניות אבטחת מידע

7.10.1. כלל המידע במערכות המשרד יגובה, יאובטח ויבדק באופן שוטף בהתאם לנהלים שייקבעו לעניין זה.

7.11. טיפול בתוכנות זדוניות (וירוסים, ונדלים)

7.11.1. מנהל ביטחון מידע והגנה בסייבר באגף מערכות מידע יגדיר את ההליכים והכלים הנדרשים לעדכון הטכנולוגי הנדרש לצורך מניעת סיכונים תוכנות זדוניות, רוגלות ונדלים, בהתאם לסיכונים הדינמיים החלים בתחום ביטחון מידע והגנה בסייבר, ובכפוף לטכנולוגיות הקיימות והעדכניות.

7.12. הצפנה

7.12.1. אגף מערכות מידע יערוך סקר סיכונים מידע, אשר על פיו יחליט ממונה ביטחון מידע והגנה בסייבר על הצורך בהצפנת מידע רגיש.

7.12.2. ממונה ביטחון מידע והגנה בסייבר יבקר את תהליכי ההצפנה.

7.13. בקרה וכלי בקרה

7.13.1. נהלי המשרד יגדירו ויתוו את אמצעי ותהליכי הבקרה בתחומי ביטחון מידע והגנה בסייבר של המשרד. במסגרת זו, יוגדרו תחומי והיקפי האחריות של בעלי התפקידים.

7.13.2. באחריות ממונה ביטחון מידע והגנה בסייבר לבקר, בצורה אקראית, את הפעילויות המתבצעות על ועם המידע, בכדי לוודא כי המשרד עומד בדרישות החוקים, התקנות, התקנים והנהלים ובהתאם לכללי המינהל התקין.

7.13.3. ממונה ביטחון מידע והגנה בסייבר בשיתוף עם אגף מערכות מידע יאפינו ויבחרו כלים ייעודיים והולמים לשליטה ובקרה בתחום ביטחון מידע והגנה בסייבר, לצורך בקרה על יישום מדיניות ונוהל ביטחון מידע והגנה בסייבר. מנהל אגף מערכות המידע יהא אחראי על יישום כלים אלו, על בקרתם ועל דיווח לגבי האמור ל ממונה ביטחון מידע והגנה בסייבר.

7.14. רישום בקרות

7.14.1. אגף מערכות מידע יישם בקרות המאפשרות זיהוי חד-ערכי של משתמשים אשר ביצעו שינויים במידע או בתוכנה או אשר ניגשו למידע רגיש, תוך פירוט הפעילות שבוצעה וזמן הביצוע, לפי הגדרות ממונה ביטחון מידע והגנה בסייבר.

7.14.2. אגף מערכות מידע יוודא אשר מתבצעת בקרה ורישום הפעילות בשתי רמות :

7.14.2.1. זיהוי ורישום גישה לרשת ע"י גורמים מרוחקים, ניסיונות חדירה וגישה לקבצים רגישים.

7.14.2.2. תיעוד ברמת האפליקציה של גישה למידע רגיש על-ידי משתמש. התיעוד יבדיל בין שינוי נתונים לקריאתם.

7.15. אבטחת נותני שירותים

7.15.1. במשרד משולבים ממשקים עסקיים רבים, המסופקים ע"י נותני שירותים בתחומי פעילות שונים.

עמוד 12 מתוך 15

משרד המשפטים - מדיניות אבטחת מידע

7.15.2. נותני השירות נבדלים זה מזה בהיקף ואופן חשיפתם למידע המצוי במשרד. חלקם רשאים להיכנס לאזורי עבודה מסוימים אך אמורים להיות מנועים מחשיפה למידע רגיש. בעוד לאחרים עשויות להינתן הרשאות גישה מקיפות יותר.

7.15.3. נסיבות עבודה אלו, מהוות סיכון אבטחתי משמעותי ביותר, העלול להוביל לתרחישי דלף מידע קשים.

7.15.4. כל מכרז או חוזה התקשרות עם נותן שירותים אשר יש בהם היבטים של ביטחון מידע והגנה בסייבר, יעבור את אישורו של ממונה ביטחון מידע והגנה בסייבר לבדיקת היבטי ביטחון מידע והגנה בסייבר בכל הנוגע להתקשרויות עם נותני שירותים.

7.15.5. ממונה ביטחון מידע והגנה בסייבר יתווה את תהליכים ואופן ביטחון מידע והגנה בסייבר בכל שקשור לנותני שירותים חיצוניים למשרד לרבות:

7.15.5.1. קריטריונים להגדרת רגישות / סיווג הממשק העסקי.

7.15.5.2. דרישות האבטחה בכפוף לסיווג הממשק העסקי.

7.15.5.3. שיטות וכלים לאכיפת הדרישות.

7.15.5.4. תהליכים ואמצעים לפיקוח ובקרה ולטיפול בחריגים.

8. אחריות אישית לביטחון מידע והגנה בסייבר

8.1.1. לעובד תהא אחריות אישית לכלל המידע עליו הוא מופקד וכן על המידע שבחזקתו, לרבות מידע שנשלח או שהועבר אליו על-ידי גורם אחר.

8.1.2. העובד יהא אחראי באופן אישי לביטחון מידע והגנה בסייבר בנושאים עליהם הוא מופקד.

8.1.3. מנהלים יישאו באחריות כוללת ליישום מדיניות ונהלי ביטחון מידע והגנה בסייבר בתחומי סמכותם, לפעילות הולמת של עובדיהם מהיבטי האבטחה וכן לטיפול בנושאי ביטחון מידע והגנה בסייבר חריגים בשיתוף עם ממונה ביטחון מידע והגנה בסייבר.

8.1.4. האחריות לביטחון מידע והגנה בסייבר, בין אם הנה מוטלת על עובדי המשרד ובין אם על מנהליו, מתייחסת לאבטחה הפיזית, אבטחת הרשומות והאבטחה הלוגית.

8.1.5. עובד המשרד אחראי ולפעול לדיווח ישירות ובאופן מידי לממונה ביטחון מידע והגנה בסייבר, על כל פעילות העלולה להשפיע על ביטחון מידע והגנה בסייבר.

9. טיפול באירועי ביטחון מידע והגנה בסייבר חריגים

9.1.1. ממונה ביטחון מידע והגנה בסייבר יגדיר מהו אירוע אבטחה חריג המחייב דיווח להנהלת המשרד. דיווח הממונה לרשויות כדן, על אירוע כאמור, יעשה בכפוף להוראת החוק.

9.1.2. יוגדר נוהל דיווח, תיעוד ורישום לפעילויות חריגות ברות השלכה על ביטחון מידע והגנה בסייבר.

עמוד 13 מתוך 15

משרד המשפטים - מדיניות אבטחת מידע

9.1.3. חריגות בתחום ביטחון מידע והגנה בסייבר המאותרות על-ידי גורמי המשרד או אחרים, ידווחו לממונה ביטחון מידע והגנה בסייבר ויועברו לפי הצורך להמשך טיפול וחקירה של ממונה ביטחון מידע והגנה בסייבר, מנהל אגף הביטחון, המבקר הפנימי או המנהל הרלוונטי.

9.1.4. הנהלת המשרד תדון ותחליט על דרך התמודדות טיפול עם על אירועי ביטחון מידע והגנה בסייבר חריגים, בכפוף לנהלי המשרד ולכל דין.

9.1.5. במקרים של אירועי ביטחון מידע והגנה בסייבר חריגים, יועבר דיווח לוועדת ההיגוי.

10. היערכות להמשכיות עסקית

10.1.1. היערכות להמשכיות עסקית נועדה לסכל סיכונים להפרעות בפעילות השוטפת של המשרד. במסגרת הערכות זו, יפעל המשרד להגן על נתונים מפני הרס, שיבוש, מחיקה וכדומה, הנגרמים בהשפעת מקרי כשל רציניים או מקרי אסון (שריפה, הצפה, אסונות טבע וכדומה), במערכות המידע הפיזיות והלוגיות של המשרד.

10.1.2. המשרד ימנה אחראי על נושא ההיערכות להמשכיות עסקית.

10.1.3. ממונה ההיערכות להמשכיות עסקית, יקבע את תכנית אסטרטגית המבוססת על הערכת סיכונים נאותה, וכן את עקרונות ההיערכות להמשכיות עסקית של מערכות המידע במשרד, בכפוף לאישור המשרד. עקרונות אלו יהוו תכנית אסטרטגית, מבוססת על הערכת סיכונים נאותה, לטיפול כולל בהמשכיות תפעולית.

10.1.4. עקרונות ההיערכות יובאו לאישור הנהלת המשרד בטרם עיגונם בנהלים ממונה ההיערכות להמשכיות עסקית יפעל ליישום עקרונות ההיערכות להמשכיות עסקית שנקבעו ויהיה אחראי על תחזוקתה ועדכנותה של התכנית ההיערכות להמשכיות עסקית.

11. נהלים

11.1.1. ממונה ביטחון מידע והגנה בסייבר אחראי לפיתוח, אישור ופרסום נהלים לשם הסדרת פעילויות ביטחון מידע והגנה בסייבר במשרד.

11.1.2. ממונה ביטחון מידע והגנה בסייבר יהיה מעורב בפיתוח כלל הנהלים שיש להם השלכה על ביטחון מידע והגנה בסייבר במשרד.

11.1.3. נהלי ביטחון מידע והגנה בסייבר חלים על כל עובדי המשרד ועל ממשקיו באשר הם, אשר להם מעורבות בפיתוח, בתפעול, בתחזוקה, ביישום ובשימוש במידע.

12. הדרכה והטמעה של ביטחון מידע והגנה בסייבר

12.1.1. ממונה ביטחון מידע והגנה בסייבר יפעל להטמעת ביטחון מידע והגנה בסייבר במשרד ובכלל זה את מדיניות ביטחון מידע והגנה בסייבר ונהלים בנושא, ביחידות המשרד ובכל מערך המחשוב המשרדי.

12.1.2. ממונה ביטחון מידע והגנה בסייבר יפעל להטמעת מדיניות ונהלי ביטחון מידע והגנה בסייבר בתהליכי העבודה של המשרד.

עמוד 14 מתוך 15

משרד המשפטים - מדיניות אבטחת מידע

12.1.3. ממונה ביטחון מידע והגנה בסייבר יפעל להעלאת המודעות לביטחון מידע והגנה בסייבר ובכלל זה מדיניות ונוהל ביטחון מידע והגנה בסייבר בקרב עובדי המשרד, ממשקיו והגורמים האחרים להם נגישות למידע בהתאם למשאבים ותקציבים שיוקצו לכך.

13. תוכנית עבודה ותקציב

13.1.1. ממונה ביטחון מידע והגנה בסייבר יקיים דיוני עבודה ומעקב אחר ביצוע מדיניות ונוהלי ביטחון מידע והגנה בסייבר.

13.1.2. ממונה ביטחון מידע והגנה בסייבר ידווח תקופתית לוועדת ההיגוי על פעילויות ביטחון מידע והגנה בסייבר, על פעולות הבקרה והפיקוח ועל אירועי ביטחון מידע והגנה בסייבר.

13.1.3. ועדת ההיגוי תמליץ על היקף תקציב הנדרש לפעילות ביטחון מידע והגנה בסייבר במשרד וסדרי העדיפות בו לגורמי ההחלטה התקציביים.

13.1.4. ועדת ההיגוי תמליץ למשרד על הקצאת משאבים לממונה ביטחון מידע והגנה בסייבר ליישום, אכיפה, הדרכה וביצוע ביקורות בכלל היחידות ליישום המדיניות ונהלי ביטחון מידע והגנה בסייבר.

14. שיתוף פעולה פנים / חוץ ארגוני

14.1.1. המשרד יפעל לקיומם של ערוצי תקשורת והתקשרות עם גורמי פנים / חוץ משרדיים עמם יתקיים שיתוף פעולה מקצועי, לצורך עדכון וקידום הדדי ולצורך קבלת שירותים חיוניים.

15. שיפור מתמיד

15.1.1. דרישות לביטחון מידע והגנה בסייבר ייקבעו בהתאם לתהליך ניהול סיכונים ביטחון מידע והגנה בסייבר ודרישות החוקים, התקנות, ההנחיות הרגולטוריות והתקנים. ממונה ביטחון מידע והגנה בסייבר יורה על ביצוע סקר סיכונים מתודולוגי אחת ל-18 חודשים לפחות לפיו ייקבעו תהליכי הקטנת סיכונים ביטחון מידע והגנה בסייבר ובקרתם.

15.1.2. ממונה ביטחון מידע והגנה בסייבר יקבע ויחיל את שיטת מדידת ביצועי מערכת ביטחון מידע והגנה בסייבר. שיטת המדידה תאפשר להעריך את רמת אפקטיביות ניהול ביטחון מידע והגנה בסייבר והקטנת סיכונים הגנה על מידע.

15.1.3. ממונה ביטחון מידע והגנה בסייבר ידאג לכך שאחת לשנה יבוצע סקר פנימי של תהליכי ביטחון מידע והגנה בסייבר על מנת להעריך את מידת ההתאמה של הנהלים להשגת המטרות.

15.1.4. תשומה של כל סקר פנימי תעובד לתוכנית שיפור אשר תוודא שיפור מתמיד של מערכת ביטחון מידע והגנה בסייבר. כל בעלי העניין יעודכנו אודות כל השיפורים שנעשו.

עמוד 15 מתוך 15