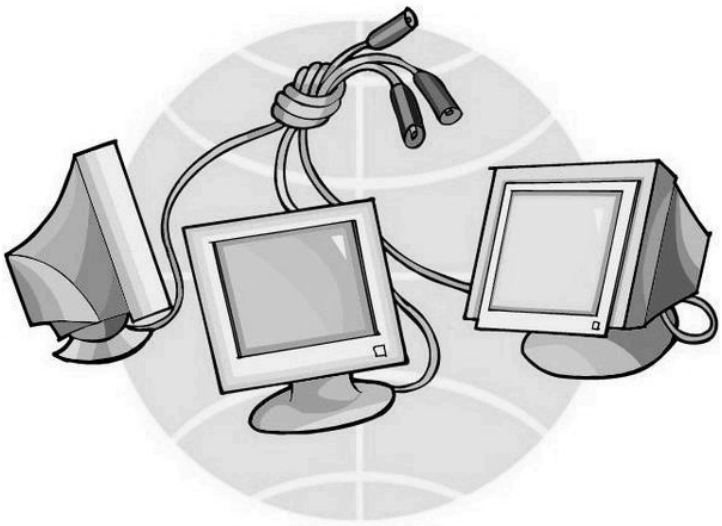
משרד ראש הממשלה
אגף בכיר לביקורת המדינה והביקורת הפנימית
המועצה המייעצת לביקורת ואבטחת מידע

נהלי מסגרת לאבטחת מידע



מהדורה שלישית

ירושלים אלול תשס״ה ספטמבר 2005

משרד ראש הממשלה
אגף בכיר לביקורת המדינה והביקורת הפנימית
המועצה המייעצת לביקורת ואבטחת מידע

מהדורה חדשה זו כוללת 38 נהלי מסגרת, מתוכם 4 נהלי מסגרת חדשים ונוהל מסגרת אחד מעודכן. כמו כן, נמצאים בהכנה נהלים נוספים: "זיהוי משתמשים חזק", "עבודה מרחוק", "אבטחת תשתיות הרשת", "טכנולוגיות אבטחת מידע", "מרכז בקרת אבטחה – Security SOC –Operation Center".

נהלי מסגרת מעצם הגדרתם אינם תחליף לנוהלי המשרדים.

על כל משרד לגבש את נהליו בהתאם למשימות המוטלות עליו. נוהלי המסגרת יהיו לנגד עיני המשרדים במהלך קביעת הכללים המחייבים.

תקוותנו כי תרמנו במשהו בנהלים אלה לאבטחת המידע והמערכות הממוחשבות, לשיפור ניהול המידע, וסביבת המידע.

תודה לגב' ויקטוריה טננבאום, אשר ריכזה וערכה את הנהלים, ולחברי "המועצה" מר אהוד אבנר ומר יאיר רודיאקוב על הסיוע והייעוץ.

בברכה

עוזי ברלינסקי
המפקח הכללי

תוכן עניינים

קביעת מדיניות אבטחת "מידע רגיש" ומערכי מידע בממשלה ומוסדותיה

נוהל מס' 1

מבוא

משרדי הממשלה, מוסדותיה ורשויות על פי חוק משתמשים במערכי מידע טכנולוגיים לניתוח וקבלת החלטות, למעקב, לבקרה, לפיתוח ולפיקוח על אופן יישום המדיניות הממשלתית, לאכיפת החוק ולניהול משק המדינה.

הצורך בהגנה על "מידע רגיש" ומערכי מידע, שליטה ובקרה הקיימים במשרד, נובע מאחד או כמה, מהטעמים האלה:

א. ניהולו התקין של המשרד וביצוע תפקידיו.
ב. ניהולו התקין של משק המדינה.
ג. הגנה על צנעת הפרט, על פי החוק להגנת הפרטיות, התשמ"א-1981 ותקנותיו.

ד. שמירה על "מידע רגיש", אשר גילויו היה תנאי למסירתו, או שגילויו עלול לפגוע בהמשך קבלת המידע.

ה. מניעת פגיעה בהליכי חקירה או משפט או בזכותו של אדם למשפט הוגן.

ו. שמירת המידע ומערכי המידע, על פי הוראת כל דין.

השימוש במערכי המידע החיוניים לפעילותם התקינה של המשרדים, מותנה בשמירה איכותית על - הזמינות, השלמות, האמינות, הסודיות והשרידות של כל אלה: המידע, התוכנות, הנתונים האמצעים והתהליכים, בהם המידע נאסף, נשמר, מעובד ומועבר.

מטרות הנוהל

א. להנחות את המנהל הכללי וגורמי המטה במשרד, להכנת מסמך "מדיניות אבטחת "המידע הרגיש" ומערכי המידע", אשר באחריות המשרד (להלן - "**מסמך מדיניות אבטחת המידע**"), ולהטמיעו בקרב כל עובדי המשרד.

ב. לתאר בפני כל עובדי המשרד המטפלים, עוסקים, או נעזרים ב"מידע רגיש", ובמערכי המידע, השליטה והבקרה, את העקרונות לאבטחת "מידע רגיש" ומערכי מידע, שליטה ובקרה, שנקבעו על ידי "המועצה", אשר מהם נגזר נוהל מסגרת ממשלתי זה.

הגדרות

"**מידע**" - ידיעות, נתונים, סימנים, מושגים או הוראות המובעים בשפת אנוש או מחשב, במסמך או בטיוטה, המטופלים או נשמרים בכל מקום אחסון אפשרי, והמועברים בכל תווך אפשרי.

"**מידע רגיש**" - כל מידע הנמצא בידי משרדי הממשלה, מוסדותיה, או, ברשויות ציבוריות אחרות, על גבי כל סוג של מצע מידע, בשלבי טיפול, בהעברה, באחסון או בגניזה ושמירתו נדרשת בשל היותו אחד מאלה:

א. מידע אשר פגיעה בסודיותו, שלמותו/מהימנותו, זמינותו ושרידותו עלולה לגרום לאחת (לפחות) מהפגיעות האלה:

1. פגיעה בניהולה התקין של המדינה.
2. פגיעה בפעילותם התקינה של משרדי הממשלה, או, רשויות ציבוריות אחרות.

ב. מידע המכיל פרטים אישיים, המוגנים על ידי החוק להגנת -הפרטיות, התשנ"א 1981- ותקנותיו.

ג. מידע המכיל סודות כלכליים, מסחריים, משפטיים, ארגוניים או אחרים, אשר נמסרו, על - פי רצון חופשי או כחובה, מאנשים או תאגידים והמצויים בידי משרדי הממשלה ומוסדותיה, אשר נדרשים לשמור על הסודות הנ"ל, על פי כל דין, או, על פי בקשת בעלי, או מוסרי המידע.

ד. מידע החייב בשמירה על פי כל דין.

"**אבטחת מידע**" - כלל הפעולות והאמצעים הננקטים והמיושמים במשרד, שמטרתם להבטיח כי המידע ומערכי המידע היוצרים אותו והמטפלים בו, יוגנו מפני: פגיעה, חשיפה ושינוי במזיד או בשוגג, באופן שייִשָמרו - **הזמינות, השלמות, המהימנות הסודיות, והשרידות** של המידע ומערכי המידע.

אחראי לביצוע הנוהל

על **המנהל הכללי** במשרד חלה אחריות מינהלית כוללת להכנת "מסמך מדיניות לאבטחת מידע רגיש, מערכי מידע, שליטה ובקרה", ולפקח על אופן יישום המדיניות שנקבעה.

על הממונה על אבטחת המידע (להלן - "**הממונה**") חלה אחריות להכנת מסמך המדיניות של המשרד (בהיוועצות עם מנהל מערכות המידע), במסמך אשר לא יגרע מהאמור בנוהל זה, והבאתו לאישור וחתימה של המנהל הכללי.

על כל אחד מעובדי המשרד, ללא יוצא מהכלל, חלה אחריות-אישית לפעול על פי ההנחיות המפורטות במסמך המדיניות של המשרד, ונהלי האבטחה המשרדיים הנגזרים ממנו.

גוף הנוהל

תחומי האבטחה - אבטחת המידע ומערכי המידע, השליטה והבקרה תיושם במשרדי הממשלה, במוסדותיה ורשויות על פי חוק, בתחומים הבאים :

א. אבטחה פיזית של מחשבים וסביבתם ושל "**רשומות** (ניירת) **רגישות**".

ב. אבטחה לוגית של הגישה למידע והשימוש המותר במידע ובמערכי המידע.
ג. אבטחת תקשורת המידע והנתונים (של מערכי המידע, השליטה והבקרה) במבנים ובחצרות של המשרד, וגם זו המועברת בתוואים שהם נטולי פיקוח או שליטה ע"י המשרד.

ד. אבטחת פלטי מחשב ומצעי מידע לסוגיהם .

ה. אבטחה של מחשבים אישיים ובכלל זה נישאים.

ו. היערכות לשעת אסון (הכנת חלופות תפעול למצב של השבתת מערכי מידע, מערכי תקשורת, שליטה ובקרה) ובחינה חד - שנתית של יישומה.

ז. אבטחת **רשומות רגישות** שאינן מגנטיות או אופטיות (ניירת, תעודות רשמיות, חותמות וכד'**).**

ח. עריכת בדיקות מהימנות לעובדים עם מידע רגיש או בתפקידים רגישים עם מערכי מידע, שליטה ובקרה טכנולוגיים במשרד (כל העובדים, כולל קבלנים ועובדיהם).

ט. קיום פעילויות בקרה וביקורת על אבטחת "**המידע הרגיש**" ומערכי המידע, השליטה והבקרה, כחלק מובנה מתפקיד "**הממונה**".

מבנה ארגוני של ניהול ויישום אבטחת המידע

המבנה הארגוני הנוגע לניהול, ליישום ולביקורת על אבטחת המידע ומערכי המידע יושתת על עיקרון "**הפרדת הסמכויות**", על פיו תמנה הנהלת המשרד בעלי-תפקיד שונים לתפקידים המתוארים להלן:

א. גורם ניהולי בכיר- המנהל הכללי (או המשנה למנכ"ל, או הסמנכ"ל למינהל) - בעל אחריות מינהלית כוללת ליישום נהלי המסגרת הממשלתיים שאישרה "**המועצה**".

ב. גורם ניהולי אבטחתי - "ממונה על אבטחת מידע רגיש" (להלן- "**ממונה**") המכוון את בעלי התפקיד ואת כלל "**משתמשי-הקצה**" ליישום נהלי אבטחת "**מידע-רגיש**" ומערכי המידע. בין כלל תפקידיו - יישום המדיניות לאבטחת "מידע-רגיש". אינו כפוף מינהלית (או באופן אחר) למנהל מערכות המידע, **בשל ניגוד עניינים בין שני התפקידים ! "הממונה"** מהווה במשרדו גורם מנחה מקצועי-אבטחתי, הפועל על פי המדיניות של משרדו, ונוהלי המסגרת של "**המועצה**". בין יתר תפקידיו, מוסמך לערוך ביקורות לבחינת אופן יישום הנהלים האבטחתיים המחייבים, ולקבוע אירועים פעילויות מסוימים כ"חריגים", בשל היותם מסכנים, בפועל או בכוח, את יכולת הניהול התקין של המשרד, או למשק המדינה.

ג. גורמי ביצוע - מנהל מערכות המידע ומנהל התקשורת - האחראים בין היתר על יישום הכלים והשיטות לאבטחת מידע, על פי נהלים פנימיים שקבעה הנהלת המשרד, לנוהל מסגרת זה ועל פי הנחייה ישירה של "הממונה".

ד. גורם סיוע אבטחתי [**נאמני אבטחת מידע**] - בעלי תפקיד טכניים בתחום הטיפול והתחזוקה של מערכי המידע - שבנוסף לתפקידם הם גם מסייעים ל"**ממונה**" ביישום הנהלים ומונחים על ידו מקצועית בנושאי האבטחה.

ה. קצין ביטחון (קב"ט) – האחראי על האבטחה הפיזית של מתקנים ובדיקת מהימנות העובדים..

ו. אחראי על מסירת מידע לציבור - מי שהתמנה ע"י הנהלת המשרד כממונה על מסירת מידע לציבור, על פי הוראות החוק לחופש המידע, התשנ"ח - 1998.

ז. אחראי לביקורת - מבקר הפנים של המשרד אחראי על קיום ביקורת של אופן היישום בפועל של המדיניות, ושל הנהלים הפנימיים לאבטחת מידע.

מיפוי וסיווג המידע, הנתונים ומערכי המידע, השליטה והבקרה.

א. "**הממונה**", בשיתוף עם מנהלי מאגרי מידע (כל סוג של מאגר מידע, ובכלל זה מאגר מידע המכיל מידע אישי-רגיש, המוגן עפ"י החוק להגנת הפרטיות, התשמ"א - 1981), **יאתרו וימפו את** כל מערכי מידע והיישומים, ויקבעו את רמת הסיווג שלהם, על פי שני התבחינים הבאים:

1. חיסיון המידע - על פי שלוש רמות של חיסיון/סודיות: "**בלתי-מסווג**" "**חסוי**" ו- "**חסוי-ביותר**".

2. חיוניות המידע, הנתונים, מערכי המידע ומערכי שליטה ובקרה - על פי שלוש רמות חיוניות, כדלהלן: "**חיוניות בסיסית**" "**חיוניות בינונית**" ו-"**חיוניות גבוהה**" (לפי מידת הנזק שייגרם לארגון, למשק המדינה, לפרט, או לגורמים אחרים), כתוצאה מפגיעה בזמינות המידע, בשלמותו, באמינותו, ובהתאם למדיניות "המועצה לאבטחת המידע הרגיש",ועל פי כל דין.

רמה מחייבת של אבטחת מידע

רמת האבטחה של "**מידע-רגיש**" או של מערכי מידע, שליטה ובקרה, נובעת מהגבוהה מבין שתי הרגישויות [חיסיון/סודיות, או חיוניות] - ראה לעיל.

התבחינים הנ"ל, יאובחנו **קודם לכן**, בתהליך הסיווג של המידע ומערכי המידע.

מידור והרשאות גישה ל"מידע רגיש" ומערכי מידע, שליטה ובקרה:

א. על פי עקרון "**הצורך לדעת ולעשות**" (במידע, ובמערכי המידע, השליטה והבקרה) ימדר המשרד את המידע ומערכות המידע, השליטה והבקרה ואת המורשים להשתמש או לטפל בהם, ויעניק הרשאות גישה **רק לפרטי מידע ומערכות מידע, שליטה ובקרה, הנדרשים [על פי קביעת גורם מינהלי בכיר במשרד], לצורך ביצוע תפקידים במשרד.**

ב. המידור ייעשה על ידי חלוקת המשתמשים לקבוצות שייכות או נושא) כשבכל הרשאה יוגדר גם מה מותר לעובד לעשות (מידע/נתונים - קריאה, כתיבה, מחיקה, העברה וכיוצא בכך. מערכי מידע, תקשורת, שליטה ובקרה - הפעלה, כיבוי, תחזוקה, הוספת חומרה וכו').

ג. עקרונות המידור יוגדרו על ידי "הממונה", תוך היוועצות מוקדמת עם גורמי המטה המקצועיים לכל תחום פעילות במשרד ולכל מאגר מידע, ויובאו לאישור ועדת המשנה לאבטחת מידע, שתמונה על ידי ועדת ההיגוי למחשוב.

אחריותם האישית של העובדים לאבטח את המידע

א. הסמנכ"ל הבכיר למינהל יעגן בנהלי המשרד את האחריות האישית של כל עובד לפעול לאבטחת המידע ומערכי המידע הנמצאים ברשותו, או באחריותו.

ב. מנהלים יישאו באחריות כוללת ליישום נהלי אבטחת המידע בתחומי סמכותם לפעילות עובדיהם מהיבטי האבטחה .

הכנת נהלי אבטחה

א. "**הממונה**" ייזום פיתוח נהלי אבטחה פנימיים, לשם הסדרת פעילויות אבטחת המידע במשרד. נהלים אלה ייגזרו מנהלי המסגרת של "**המועצה**", לא יצמצמו את דרישותיהם האבטחתיות ולא יעמדו בסתירה להן.

ב. "**הממונה**" יהיה מעורב בפיתוח כל נהלי המשרד שיש להם השלכה על אבטחת המידע ומערכי המידע, השליטה והבקרה שבאחריות המשרד.

ג. נהלי אבטחת המידע של המשרד חלים על **כל** עובדי המשרד וכל אדם אחר, הפועל עבור המשרד.

ד. המשרד יעגן בחוזה, החלת נהלי אבטחת מידע, על כלל המשתמשים החיצוניים, ועל כל יתר הגורמים אשר יש להם מעורבות בפיתוח, בתפעול ובתחזוקה של מערכי המידע, השליטה והבקרה שבמשרד, **כולל יועצים וספקי "מיקור-החוץ"** ("OUTSOURCING").

הדרכה והטמעת הנהלים

א. "**הממונה**" יפעל להטמעת כללי אבטחת המידע ונורמות של שימוש אתי במידע, בכל יחידות המשרד. דגש יושם על יחידת מערכות המידע.

ב. "**הממונה**" יטמיע במשרדו את הנהלים לאבטחת "**מידע-רגיש**" שאישרה "המועצה" וכן את הנהלים הפנימיים של המשרד (על פי הצורך יסתייע במסגרת ההדרכה שבמשרדו).

ביקורת פנימית

בפעילות השנתית של יחידת הביקורת הפנימית יש לכלול גם עריכת ביקורת על נושאים בתחום הפיתוח, הניהול, התפעול, התחזוקה והאבטחה של מערכי המידע, השליטה והבקרה הטכנולוגיות, בהיקף שיהיה תואם את ה**רגישות המרבית** של המידע המעובד במערכות, את פרישת מערכי המידע, ואת מורכבותם. פעילות הביקורת תקבל תקציב ראוי.

קדימות רבה תינתן לבחינת מערכי המידע והפעילויות הממוחשבות שנמסרו לביצוע על ידי ספק "**מיקור-חוץ**" (OUTSOURCING).

בקרה, וכלי בקרה

א. באחריות "**הממונה**" לבקר את הפעילויות הממוחשבות המתבצעות במשרד, כדי לוודא כי המשרד עומד בדרישות האבטחתיות של החוקים, התקנות והנהלים.

ב. ברשות "**הממונה**" יהיו כלים טכנולוגיים שיאפשרו לו לבחון את דרך יישומה בפועל של מדיניות אבטחת המידע (בדיקות אלה תעשנה באופן שוטף בכל יחידות המשרד, תוך שימת דגש על בחינת פעילויות הנעשות ע"י ספק "מיקור-חוץ").

ג. כלים טכנולוגיים אלה יועמדו גם לרשות "**מבקר מערכות המידע**".

יישום נתיב בקורת (AUDIT TRAIL).

במערכי המידע של המשרד ייושמו כלים המאפשרים זיהוי חד-ערכי של משתמשים אשר ביצעו שינויים במידע, בנתונים, בתוכנה, בטבלת ניהול הרשאות למיניהן, או שניגשו **למידע "חסוי"** או "חסוי-ביותר", תוך פירוט ורישום סוגי הפעולות שבוצעה, מועד בצועה, מאיזו עמדה בוצעה, מי ביצע וכיוצא בכך. בנהלי המשרד ייקבע היקף הנתונים ומשך שמירתם.

הטיפול באירועים "חריגים"

א. לכל פעילות "**חריגה**" בעלת השלכות על אבטחת המידע, יוגדרו דרכי:
1. רישומה, **2.** הדיווח עליה, **3.** התגובה הנדרשת.

ב. "**אירועים חריגים**" בתחום אבטחת המידע יטופלו באחריות "הממונה". על פי קביעתו יוכל להעביר את הטיפול לידי גורם מקצועי הבקיא בחקירת עבירות מחשב.

ג. רשלנות ביישום של הנחיות לאבטחת מידע, שנמסרו כדין, יטופלו בהליך משמעתי.

ד. פגיעה בזדון במידע, או במערכי מידע שבאחריות המשרד, או ניסיון לכך, מהווה עבירה פלילית, על **חוק המחשבים** התשנ"ו - 1996, ומחייבת מעורבות פעילה של הממונה על המשמעת במשרד וכן בנציבות שירות המדינה.

ה. במקרים של "**אירוע חריג**" שארע במזיד, תינקטנה פעולות מידיות לביטול כל הרשאות הגישה ל"**מידע הרגיש**" ומערכי המידע, שניתנו לעובד.

היבטים אבטחתיים טכניים-טכנולוגיים

א. **איסור שינוי לא מבוקר -** חל איסור על ביצוע שינוי בנתונים, בתוכנה יישומית, בתוכנת תשתית, ובחומרה, אלא אם הדבר נעשה באופן מאובטח, מבוקר ומתועד ובהתאם להנחיה מפורשת של **מנהל מערכות המידע**.

ב. **ביצוע שינויים טכנולוגיים -** כל כוונה לעריכת שינוי במפרטים הטכניים או הטכנולוגיים של מערכי המידע, השליטה והבקרה, אשר עשוי לשנות את מצב אבטחת המידע של המערכת, מחייב את מעורבותו של **הממונה על אבטחת המידע טרם ביצוע השינוי.**

ג. **כלים טכנולוגיים מתקדמים לאבטחת המידע**

1. המשרד יישם כלים טכנולוגיים ושיטות טכנולוגיות מתקדמים למימוש מדיניות והנהלים לאבטחת "**המידע הרגיש**".

2. "**הממונה**" ינחה (בעצמו או ע"י יועצים) את "**נאמני אבטחת המידע**" והגורמים המקצועיים, אודות השימוש בכלים טכנולוגיים (חומרה ותוכנה) ואת אופן העברת המידע והנתונים, הנוגעים לאבטחת מידע ומערכי המידע - לידיעתו.

ד. אבטחת המידע בתהליך הפיתוח

1. מנהל מערכות המידע יוודא ביצוע **הפרדה מוחלטת** בין מערכות ייצור לבין מערכות בשלבי פיתוח.

2. הדרישות לאבטחת מידע בתהליכי הפיתוח, ייקבעו על ידי "**הממונה**".

היערכות לשעת אסון

א. מנכ"ל המשרד אחראי אחריות מינהלית כוללת על יישום הפעילויות שייעודן היערכות המשרד למצבי חירום ובכלל זה קביעת צוותי עבודה אשר יכווינו את הפעילות הנדרשת בשלבי - התגובה, ההתאוששות והשיקום.

ב. היערכות המשרד למצבי חירום תיעשה על פי נוהל מס' 10 הוראת שעה (נסמך על התקן הישראלי 1495 חלק 5') .

ג. "**הממונה**", בשיתוף עם **מנהל מערכות המידע, הממונה על הביטחון (קב"ט)** יקבעו יחדיו, את עקרונות ההיערכות לשעת אסון של יחידת מערכי המידע.

ד. עקרונות ההיערכות לשעת אסון יובאו לאישור ועדת-ההיגוי למחשוב.

ה. **מנהל מערכות המידע** אחראי ליישום עקרונות ההיערכות לשעת אסון וכן על תחזוקתה ועדכניותה של התכנית.

ו. "**הממונה**" אחראי על יישום נהלי אבטחת המידע בכל שלבי ההיערכות הנ"ל.

תוכנית עבודה ותקצוב

א. בתחילת כל שנת תקציב, יכין "הממונה" תכנית עבודה שנתית לאבטחת מידע ומערכי מידע ויעבירה לאישור הממונה הישיר עליו ולידיעת מנהל "היחידה". תכנית העבודה השנתית תשקף את כל הנושאים והמקורות הבאים:

1) תכנית העבודה של יחידת המחשוב, **2)** מסמך המדיניות לאבטחת מידע של המשרד **3)** ליקויים שחשפו מבקר המדינה, "היחידה" או הביקורת הפנימית, **4)** הוראות כל דין, **5)** נהלי "המועצה", **6)** רגישות המידע ומערכי המידע [היבטי חיסיון וחיוניות], **7)** פרישה ארצית של מערכי המידע, השליטה והבקרה וכן **8)** ממצאי סקר להערכת -סיכונים.

ב. פעילות אבטחת "המידע הרגיש" במשרד, תתוקצב בסעיף תקציבי ייחודי שיהיה באחריות "הממונה" ותהווה חלק אורגני מתוכנית העבודה השנתית, והרב-שנתית של המשרד.

ג. פעילות אבטחת המידע במשרד תתוקצב בהתאם לתבחינים הבאים:

1. רגישויות (חיסיון וחיוניות) המידע הנמצא ברשות ובאחריות המשרד.
2. היקף מערכות המידע.
3. מורכבות מערכות המידע (כולל זה המטופל ב- "מיקור-חוץ" (OUTSOURCING),
4. פרישת המערכות.

ד. **תיקצוב פעילות האבטחה של מערכי מידע קיימים** (רכישה, התקנה, תחזוקה,

יועצים, סקרים ואח'): תתוקצב בסכום המהווה, לפחות, **5%** מהתקציב השנתי לרכישת חומרה, תוכנה ותשתיות של היחידה למערכות מידע במשרד.

ה. תיקצוב אבטחתם של מערכי מידע חדשים: רכישת מערכי מידע חדשים, כולל פיתוח עצמי או חיצוני תהיה מותנית בשילוב כלי אבטחה הולמים בתוך המערכות או לצדן, על פי העניין (תוכנה ו/או, חומרה) לאבטחת המידע, וקבלת אישור בכתב ומראש, מ"הממונה על אבטחת המידע" כי מבחינתו נתמלאו התנאים המקדימים לרכישה.

שילוב שיקולי אבטחת המידע בתהליכי תכנון ותקצוב מערכות מידע

א. בכל הקשור עם תהליכים לרכישה, פיתוח, או תחזוקה של מערכות מידע, יקבלו שיקולי אבטחת המידע, משקל שאינו נמוך ממשקל התמורה הכספית ומהיבטים משקיים אחרים.

ב. במקרים הבאים, יקבלו שיקולי אבטחת המידע **משקל מכריע** על פני שיקולים אחרים:

1. בעת רכישה, פיתוח או תחזוקה של מערכות מידע שהן בעלות חיוניות רבה לניהול משק המדינה והביטחון הלאומי שלה.
2. בעת רכישה, פיתוח או תחזוקה של כלים ייעודיים לאבטחת מידע.

היערכות ל"מיקור-חוץ" (OUTSOURCING) במערכות המידע, השליטה והבקרה

א. ועדת ההיגוי למחשוב מוסמכת לקבוע, אילו משאבי מידע, **לא יימסרו לטיפול בידי גורמי-חוץ** מסחריים, על פי תבחינים אלה:

1. "**מידע רגיש**" אשר "**הממונה**" הגדיר כי הוא בעל חסיון רב או חיוניות קריטית לניהול פעילויות ממשל, או לניהול משק המדינה והביטחון הלאומי.

2. חשש סביר כי הקבלן עלול להימצא במצב של ניגוד עניינים, בשל טיפולו במערכות נוספות.

3. שיקולים אחרים שהציגה הנהלת המשרד.

ב. חל איסור מוחלט על מסירת האחריות לניהול אבטחת המידע, קרי - קביעת מדיניות, וכן האחריות לקיומם של - מעקב, בקרה, וביקורת שוטפים [על דרך יישומה], לידי גורמים שאינם עובדים מן המניין במשרד (כגון: עובדי קבלן, "מיקור חוץ" ואחרים).

ג. ניהול הרשאות הגישה וניהול תחום ההצפנה **ייעשו רק** על ידי עובדי המשרד.

מסירת "מידע-רגיש"

א. הנהלים, השיטות והכלים לאבטחת "**מידע-רגיש**" ומערכי המידע בממשלה במוסדותיה וברשויות על פי חוק, מסווגים בסיווג "**חסוי**", או "**חסוי-ביותר**" (על פי העניין). חל איסור על העברתם, בכל דרך שהיא, לידי גורמים שלא הותרו לכך מראש ובכתב על ידי "**הממונה**".

ב. בכל הקשור עם מסירת "**מידע רגיש**" לידי גורמים שמחוץ למשרד, על כל עובד לנהוג על פי כל דין ועל פי הנהלים לאבטחת "**מידע-רגיש**".

גורמי הצלחה קריטיים

הניסיון מלמד שהגורמים שלהלן הם לפעמים קריטיים להצלחת המימוש של אבטחת מידע במשרד:

א. מדיניות אבטחה, מטרות ופעילויות המשקפות את מטרת העסק,
ב. גישה למימוש האבטחה, המתאימה לתרבות הארגונית,
ג. תמיכה ומחויבות גלויות של ההנהלה,

ד. הבנה טובה של דרישות האבטחה, הערכת סיכונים וניהול הסיכונים,
ה. שיווק אפקטיבי של האבטחה לכל המנהלים והעובדים,
ו. הפצת הנחיות באשר למדיניות אבטחת המידע ולתקני אבטחת מידע, לכל העובדים והקבלנים,
ז. הדרכה ותרגול נאותים,
ח. שיטה מקיפה ומאוזנת של מדידה המשמשת להערכת ביצועים בניהול אבטחת מידע, והצעת משוב לשיפורים

ההנהלה תקבע מדיניות ברורה לגבי אבטחת מידע, ותציג מחויבות לנושא ותמיכה בו, באמצעות פרסום המדיניות וקידומה, בכל המשרד.
ההנהלה תאשר מסמך מדיניות, תפרסם ותפיץ אותו באופן ראוי בין כל העובדים. המסמך יכיל הצהרה בדבר מחויבות ההנהלה ויקבע את גישת המשרד לניהול אבטחת מידע. המסמך יכלול לפחות פרטים אלה:

א. הגדרה של אבטחת מידע, מטרותיה הכלליות ותחום יישומה וחשיבות האבטחה כמנגנון המאפשר שיתוף מידע.
ב. הצהרת כוונות של ההנהלה, התומכת במטרות ובעקרונות של אבטחת המידע.
ג. הסבר קצר על השיטות, העקרונות, התקנים ודרישות ההתאמה שהן חשובות במיוחד למשרד כגון:
1. התאמה לדרישות על פי דין ולדרישות חוזיות
2. דרישות הדרכה בנושא אבטחה
3. מניעה וגילוי של וירוסים ותוכנות זדוניות אחרות
4. ניהול המשכיות עסקית (היערכות למצב חירום ותכנית התאוששות)
5. תוצאות הפרה של מדיניות האבטחה

ד. הגדרת אחריות כללית וספציפית לנושאי ניהול אבטחת מידע, לרבות דיווח על אירועי אבטחה.
ה. התייחסות לתיעוד העשוי לתמוך במדיניות, כגון פירוט נוסף של שיטות האבטחה ונוהלי האבטחה המתייחסים למערכות מידע מסוימות או כללי אבטחה שהמשתמשים מחויבים לעמוד בהם.

המדיניות תופץ למשתמשים ברחבי המשרד, בצורה שתהיה רלבנטית, נגישה וברורה לקוראים המיועדים.

למדיניות יהיה בעלים שיהיה אחראי לתחזק ולסקור את המדיניות בתהליך סקירה מוגדר. התהליך יבטיח שייעשה סקר בתגובה לכל שינוי המשפיע על הבסיס להערכת סיכונים המקורית, כגון אירועי אבטחה משמעותיים, פגיעויות חדשות או שינויים בתשתית הארגונית או הטכנית. ייערכו גם סקרים תקופתיים בנושאים אלה:

א. היעילות של המדיניות כפי שהיא מתבטאת באמצעות טיבם, מספרם והשפעתם של אירועי אבטחה.
ב. העלות וההשפעה של הבקרות על היעילות העסקית.
ג. השפעת שינויים בטכנולוגיה.

מקורות

נהלי מסגרת – אבטחת מידע רגיש ומערכות מידע. משרד ראש הממשלה, אגף בכיר לביקורת המדינה וביקורת פנימית, מאי 2000.

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

נוהלי אבטחת המידע בעיריית ירושלים, פברואר 2001.

מכון התקנים הישראלי, תקן 7799: ניהול אבטחת מידע.

מיפוי וסיווג "מידע-רגיש" ומערכי מידע

נוהל מס' 2

מבוא

תהליך המיפוי והסיווג של "**מידע רגיש**", הקיים בארגונים (הכוונה למאגרי-מידע מכל סוג של מידע), ליישומים, לפרוייקטים ואח', אשר יתואר להלן, הנו צעד ראשון וראשי בחשיבותו, מבין כלל הפעילויות לאבטחת "**מידע רגיש**" במשרדי הממשלה ומוסדותיה.

מטרות הנוהל

הנוהל יתאר את דרך ביצוע המיפוי והסיווג של "**מידע-רגיש**" (לא בטחוני), משאבים ומערכי המידע שבאחריות המשרד.

יישום הנוהל יצור מצב אשר בו כל מערכי המידע ומשאבי המידע הקיימים במשרד, יהיו רשומים בצורה מסודרת וניתנים לעיון של בעלי תפקיד שונים לצורך קבלת החלטות בתחומים: ניהול מערכות המידע, פיתוח, רכש, תחזוקה, אבטחה, בטיחות והתקשרות עם ספקי חוץ.

מיפוי מדוקדק של כל סוגי המידע ומערכי המידע, השליטה והבקרה יאפשר בהמשך לקבוע לכל משאב מידע את הרגישויות הייחודיות שלו, אשר מהן ייגזרו השיטות והכלים המיועדים לשמור ולשמר אותם.

כל זאת על פי שני סוגים עיקריים של רגישויות:

א. סודיות / חיסיון
ב. חיוניות (שמירת הזמינות, השלמות, האמינות והשרידות של המידע).
פעילות זו, של מיפוי וסיווג, הנה אבן- דרך ותנאי סף להמשך כל עשייה, בתחום מערכי המידע בארגון.

בצוע תהליך המיפוי והסיווג הכרחי לביצוע היעדים האלה:

א. אפיון מערכי המידע הטכנולוגיים (כנדרש על פי נוהל מפת"ח), טרם פיתוח, רכישה וכיוצא בכך. כאחד הנתונים המערכתיים הנלקחים בחשבון בעת תהליך האפיון, וזאת על פי הרגישויות והסיכונים הנשקפים למידע או למערכי המידע - **כתנאי לאישור התיקצוב**.

ב. הכנת תוכנית עבודה שנתית להגנה על המידע ומערכי המידע, תוך התבססות, בין היתר, על סדר עדיפויות, הנובע משלוש רמות שנתקבלו בתהליך סיווג המידע ומערכות המידע, וכן מהסיכונים הנשקפים להם (עפ"י ממצאי תהליך "**הערכת סיכונים**").

ג. התקנת כלים טכנולוגיים ומינהליים הנגזרים מסיווג המידע .

ד. קיום בקרות וביקורות על הפעילות לאבטחת המידע, על פי סדר העדיפויות שנגזר מהסיווג.

ה. הכנת מסמך בסיסי לקראת עריכת סקר "**הערכת סיכונים**" למידע ומאגרי המידע שבארגון, המתבסס על מדיניות אבטחת המידע של הארגון ועל סיווג המידע.

<u>הערה</u>: סקר "**הערכת-סיכונים**" מהווה שיטה דינמית הנדרשת במקום השיטה היקרה והאיטית שכונתה "**ניתוח סיכונים**". **"המועצה" לא ממליצה על ביצוע ניתוח-סיכונים !**

ו. לשמור על **תקן ממשלתי וציבורי אחיד** לשמירת "המידע הרגיש" בכל מחזור חייו של המידע, ובהדגשה על העברתו בין הגופים הציבוריים.

אחראי לביצוע הנוהל

הממונה על אבטחת המידע הרגיש, אחראי על יישום נוהל זה, בטרם תבוצע בארגון כל פעילות אחרת לאבטחת מידע. למען הסר ספק - ביצוע סקר "הערכת סיכונים, יבוצע, במידת הצורך, **רק** לאחר ביצוע מיפוי וסיווג המידע, ומערכות המידע !!.
המנהל הכללי אחראי אחריות מינהלית כוללת, על יישום נוהל זה.

גוף הנוהל

הפעילות תתבצע בשני שלבים עוקבים:

שלב א' - עריכת מיפוי כללי בארגון
בתהליך זה על מנהל מערכות המידע, בסיוע מנהל התקשורת, לסקור ולמפות את כל מאגרי המידע למיניהם (**"מאגר מידע" - כל סוג של מידע ולא רק מאגר הנוגע לצנעת הפרט).** כאמור לעיל, יש למפות את כל היישומים והפרוייקטים הקיימים בארגון, על פי הפרמטרים המתוארים **בנספח** למסמך זה.
לנוחות ביצוע המיפוי - ניתן להיעזר בדוגמאות אשר בנספח.

שלב ב' - סיווג המאגרים, היישומים והפרוייקטים:
א. שלב זה ייעשה על ידי **"ועדה לסיווג מידע"** בראשות **"הממונה"**, אשר תקבל ממנהל מערכות המידע, עותק מלא של תהליך המיפוי (שנעשה בשלב א').

ב. **ועדת-הסיווג** תפעל כדלהלן:
1. ייקבע סיווג הולם לכל אחד מהיישומים, הפרוייקטים, מאגרי - המידע ומערכות המידע אשר קיימים בארגון ו/או באחריותו (כולל תהליכי "מיקור-חוץ" (**OUTSOURCING**).

2. פרמטר **הסודיות/החיסיון**, יסווג על פי הנזק המירבי שיתרחש בשל חשיפת המידע לגורמים לא מורשים.

3. **יסווג גם** פרמטר **החיוניות** של המידע ומערכי טכנולוגיית המידע המשמשים לצורך הטיפול בו.
הערה: גם אם למידע אין רגישות של חיסיון (מידע בלמ"סי) יתכן מאד כי תידרש שמירה בשל - חיוניותו (שמירת האמינות, השלמות הזמינות וכיוצא בכך).

חשיבות הדיוק וקביעת "סיווג-אמת" למידע.

הגזמה, או, המעטה בחשיבותו של פרט מידע או מערכי מידע אלו ואחרים (הנדרשים לניהולם התקין של המדינה והמשרדים, או להגנה על צנעת-הפרט, או בשל צורך חוקי או אחר בשמירת המידע), כאמור, עלולה לגרום לסיכול יכולת הטמעת נושא אבטחת המידע בארגון במשאבים שבהם הוא באמת קריטי ליישום, להוצאות כספיות כבדות ומיותרות, וכן להקשות ולעכב את השגת יעדי הארגון.

וועדת סיווג מידע: המורכבת מה"ה: הממונה על אבטחת המידע, מנהל מערכות המידע, ומנהל היחידה לארגון ושיטות, יבחנו את המידע שנאסף בשלב א' ויקבעו לכל יישום, מערכת מידע ומאגר מידע את **מידת הסודיות/החיסיון,** וכן את **מידת החיוניות** ההולמות אותו.

לצורך קביעת רמת הסיווג, יש להיעזר בנוהל **"תבחינים לסיווג מידע רגיש ומערכות מידע"**.

עותק של מסמך **"סיווג המידע, המשאבים ומערכי המידע"** , חתום בידי חברי הוועדה, יועבר גם לידי הגורמים האלה:

א) הממונה הישיר על **"ממונה אבטחת המידע"** (מנכ"ל המשרד, המשנה למנכ"ל, או הסמנכ"ל הבכיר למינהל).
ב) מבקר מערכות המידע ביחידת הביקורת הפנימית.

"הממונה על אבטחת המידע", יעביר אחת לשנה, אל מנהל **"היחידה הממשלתית לביקורת ואבטחת מידע רגיש"**, עותק עדכני של מסמך המיפוי, יחד עם טיוטת תכנית העבודה השנתית.
לכל "מאגר מידע" יקבע סיווג ע"י מנהל המאגר במשרד. מנהל המאגר יודיע לממונה אבטחת מידע על כל מאגר מידע חדש.

כל אמצעי קלט/פלט של "מאגר מידע" יקבלו רמת סיווג זהה לסיווג של "מאגר מידע". על פי אישור של ממונה אבטחת מידע, ניתן יהיה לסווג אמצעי מסוים בסיווג יותר נמוך, כגון: דו"ח הכולל נתונים סטטיסטיים בלבד, או נגזרת מצומצמת של המאגר. ממונה אבטחת מידע יחזיק רישום מעודכן של כל המאגרים וסיווגם. מסמך זה ישתייך לקטגורית הסיווג הגבוה.
בכל ישיבה של הוועדה העליונה לאבטחת מידע ייכלל בסדר היום מסמך שיציג את כל העדכונים בנושא סיווג המידע. הוועדה תהיה רשאית לשנות סיווגים שניתנו, אחרי בירור הולם עם הנוגעים בדבר.
אמצעי קלט/פלט המכיל נתונים ממאגרי מידע שונים, יסווג בהתאם למאגר בעל הסיווג הגבוה ביניהם.

הנושאים שלהלן, יסווגו תמיד בסיווג הגבוה ביותר:

א. אמצעי אחסון משולבים של כל המערכות. כגון: קלטות הגיבוי של מערכת מרכזית.
ב. מידע אודות אמצעי אבטחה בתוכנה. כגון: חבילת תוכנה לאבטחה, מנגנוני זיהוי והרשאה בתוכנה.
ג. מערך התקשורת של הארגון, מערך ההגנה עליו מפגיעות חוץ ופנים ארגוניות.

רמת סיווג חיסיון של "מידע רגיש" בממשלה ומוסדותיה

1. מידע "בלתי-מסווג" (בלמ"ס) - מידע אשר עונה על כל התבחינים האלה:
א. אינו רגיש מהיבטי סודיות/מידור וניתן לפרסמו בציבור.
ב. אינו עונה על התבחינים לסיווגי מידע "חסוי", או, "חסוי-ביותר" שלהלן.

2. מידע "חסוי"
מידע שפגיעה בזמינותו בשלמותו באמינותו, בסודיותו או בשרידותו עלולה לגרום לתקלות כגון אלה:
א. פגיעה או הכבדה על ביצוע תוכניות או פעולות כלכליות, מינהליות, חברתיות, משפטיות ואחרות, של המדינה.
ב. גרימת תקלה לעבודת הגופים הציבוריים שמשמעה עיכוב או ייקור תהליכי עבודה, או, הפרעה בביצוע אכיפת החוק.
ג. חשיפת מידע-אישי המוגן על ידי החוק להגנת הפרטיות, התשמ"א- 1981.
ד. הפרת כל דין המחייב שמירה על סודיות (או חיסיון) מידע.
ה. מידע פנים ארגוני שהנהלת הארגון רוצה לשמור על חשאיותה מול ארגון מתחרה.

3. מידע "חסוי ביותר"

מידע שפגיעה בזמינותו, בשלמותו, באמינותו, בסודיותו, או, בשרידותו עלולה לגרום לפגיעה, או לשיתוק (חלקי או מלא) ביכולת ניהול המדינה או הגופים הציבוריים, ע"י:

א. הקניית יתרון כלכלי מכריע למדינה זרה או לגורם זר.
ב. הכשלת תוכניות או פעולות כלכליות ומסחריות של מדינת ישראל.
ג. חשיפת מידע העלול לגרום לבהלה בציבור.
ד. חשיפת מידע אישי "רגיש", או, "מוגבל", כמשמעו בחוק הגנת הפרטיות, שהינו רגיש ייחודית.
ה. שיתוק מערכות המידע של הגופים הציבוריים.
ו. פגיעה בהיערכות, או החלשה, או קריסה של מערכות משק המדינה לשעת חירום.

לקט דוגמאות לסיווג מידע "רגיש"

א. להלן לקט של נושאים המוגדרים כמידע "רגיש", אשר בד"כ יסווגו כמידע

"בלתי- סווג"

1. מידע אודות פעילויות תרבות והשכלה במשרדים.

2. מידע אודות תוצאות מכרז, בשלב שנקבע כפומבי ובלבד שאינו מכיל פרטים חסויים.
3. נושאי מדיניות אשר הנהלת המשרד אישרה את פרסומם.

<u>לתשומת הלב</u>: לנושאים הנ"ל אין אמנם רגישות מהיבטי חיסיון, אך עשויה להיות להם בהחלט מידה של חיוניות (זמינות, שלמות, ואמינות) הדורשים אבטחה הולמת.

ב. להלן לקט נושאים המוגדרים כ- "מידע ציבורי-רגיש" והמצדיקים, בדרך כלל, את סיווגם בסיווג "חסוי" (רמת סיווג אמצעית):

1. שלבים לא פומביים במשא ומתן בין משרדי הממשלה או גופים ציבוריים אחרים ושלוחותיהם, לבין גורם אחר.
2. שלבים לא פומביים של וועדות משרדיות.
3. מידע על פעילות משרדי הממשלה וגופים ציבוריים שפרסומו עלול לעיכוב פעילותם לייקור העלויות של הגופים, או לפגיעה במחויבותיהם לתאגידים או לפרטים.
4. דו"חות של משרדי הממשלה ומוסדותיה, או, של וועדות ממשלתיות שהנהלות הגופים החליטו שאין לפרסמם.
5. מידע אודות מדיניות הנמצאת בשלבי עיצוב, דיונים פנימיים או ניהול פנימי של גופים-ציבוריים, לרבות חוות-דעת, תחקיר פנימי, טיוטה, עצה, המלצה, אשר ניתנו לצורך קבלת החלטה וכן תרשומות.
6. מידע המוגן על ידי החוק להגנת הפרטיות, התשמ"א- 1981 והמוגדר בחוק זה כ- "מידע-רגיש", או, "מידע מוגבל", כמשמעם בחוק הנ"ל, אך למעט הנושאים האלה: אימוצים, בריאות הנפש, מחלות מין ומחלת האיידס.
7. מידע החייב בשמירה על פי כל דין.
8. מידע אודות השיטות והכלים לאבטחת מידע "חסוי".

ג. להלן לקט נושאים המצדיקים, בדרך כלל, את סיווגם בסיווג "חסוי-ביותר":

1. תוכניות, פעולות ואמצעים כלכליים ומסחריים שיש להם ערך מכריע לניהול התקין של המדינה, ובכלל זה: מקורות המימון וקניות הגומלין של המדינה.

2. נושאי מחקר, פיתוח וייצור של התעשייה האזרחית בישראל אשר נמסרו לממשלה, מרצון, או כחובה, או שנמצאים בידי הגופים הציבוריים.

3. תוכניות פעולה ופרטים בנושא רכש לא בטחוני החיוניים למדינה.

4. תוכניות לשינויים מכריעים במדיניות הכלכלית של מדינת ישראל.

5. מידע אודות הכלים והשיטות לאבטחת מידע "חסוי-ביותר".

6. מידע אשר נמסר לממשלה על ידי מודיעים ואשר פרסומו או פרסום מקורות המידע עלול לפגוע בהמשך קבלת המידע.

7. מידע בנושאים: אימוצים, בריאות הנפש, מגפות, מחלות מין ומחלת האיידס, המוגנים על ידי החוק להגנת הפרטיות, התשמ"א- 1981.

8. מידע הנוגע למשק **החשמל, הדלק, הגז והמים**, אודות:
א. השיטות והכלים שייעודם -
1) אבטחת המידע ומערכות המידע (כולל מערכות השליטה והבקרה).
2) אבטחה פיזית של המאגרים, או תחנות הכוח.
ב. תהליכי הרכישה, ההובלה והטיפול במלאים **לשעת-חירום** של חומרי-גלם לייצור אנרגיה.

9. מידע אודות תהליכי הרכש, ההובלה והשימור, הנעשים על ידי הממשלה או גוף מטעמה,

של **מלאים קריטיים לשעת חירום**, כגון: תרופות, מזון, דגנים ואחרים.

מקורות

נהלי מסגרת – אבטחת מידע רגיש ומערכות מידע. משרד ראש הממשלה, אגף בכיר לביקורת המדינה וביקורת פנימית, מאי 2000.

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

סקרי סיכונים - ניהול והערכה

הנוהל מס׳ 3

מטרות הנוהל

להבטיח מודעות לסיכונים ואיומים אפשריים על מערכי המידע והמחשוב, להעריך אותם בצורה נאותה ולנהל אותם לאורך הזמן.

הגדרות

אבטחת מידע - שמירת חיסיון, כלילות (integrity) וזמינות של מידע.
חיסיון - הבטחת נגישותו של מידע רק לגורמים מורשים.
כלילות - שמירת הדיוק והשלמות של מידע ושל שיטות עיבוד.
זמינות - הבטחה שמשתמשים מורשים יוכלו לגשת למידע ולמשאבים מסומכים אליו, לפי הצורך.
עודף מידע – הבטחה שמשתמשים מורשים יוכלו לגשת רק למידע שאליו הם צריכים לגשת.

הערכת סיכונים
הערכת פגיעותם של מידע ושל אפשרויות לעיבוד מידע, הערכת איומים והשפעות עליהם והערכת הייתכנות התממשותם.

ניהול סיכונים
תהליך הזיהוי, הבקרה והמזעור או סילוק של סיכוני אבטחה העלולים להשפיע על מערכות מידע, הנעשה בעלות קבילה. במסגרת ניהול הסיכונים מתבצע סקר סיכונים, שמטרתו לאתר את הסיכונים לארגון ולעריך את חומרתם, זאת על מנת לאפשר קבלת החלטה מבוססת באיזה סיכונים לטפל, ובאיזה סדר עדיפות , עלות ולוח זמנים.
המתודולוגיה המקובלת לביצוע סקר סיכונים מדגירה מספר גורמים:

איום (Threat)
איום מזוהה עם יריב, שיש לו גם כוונות וגם יכולות לבצע פעולה שתפגע בארגון. מלבד הכוונות והיכולות, גם פעילות היריב בעבר נלקחת בחשבון בעת הערכת האיום. מקובל להניח שהאיום מוכתב ע״י היריב, למרות שמידת הנזק האפשרית, הפגיעויות בנכסים ואמצעי ההגנה שיינקטו, יכולים להשפיע על כוונת היריב לפעול.

פגיעות (Vulnerability)
פגיעות היא חולשה בנכסים או אמצעי ההגנה של הארגון, שהיריב יכול לנצלה על מנת לגרום נזק לארגון. אמצעי הגנה מתאימים מפחיתים את הפגיעות .

נכס (Asset)
כל דבר בעל ערך לארגון – כגון כוח אדם, מידע, ציוד, מתקנים, תוכנה, פעילות שוטפת, מוניטין. ככל שלנכס ערך רב יותר לארגון, כך הנזק יהיה גדול יותר בעת הפגיעה בנכס.

אמצעי הגנה (Countermeasures)
פעולות או אמצעים שמפחיתים את הסיכון על ידי השפעתם על הנכסים (ובכך על הנזק האפשרי), הפגיעויות והאיומים.

סיכון (Risk)
סיכון מאירוע כלשהו מורכב מגודל הנזק שייגרם לארגון בקורות האירוע, ומהסבירות שהאירוע יתרחש. הסבירות מושפעת על ידי רמת האיום ורמת הפגיעות. ישנם מודלים בהם נותנים ערכים מספריים לרמת הנזק, רמת האיום ואמת הפגיעות בכל אירוע אליו מתייחסים, ואז מחשבים:

$$\text{סיכון} = \text{רמת נזק} * \text{רמת איום} * \text{רמת פגיעות}$$

אחראי על ביצוע הנוהל
מנהל אגף מערכות מידע, ממונה על אבטחת מידע.

גוף הנוהל

הערכת הסיכונים במערכות מידע ומחשוב במשרד (תהליך הקרוי "סקר סיכונים") הנה שלב מקדים בתהליך עיצוב מדיניות אבטחת המידע.

דרישות האבטחה מזוהות באמצעות הערכה מתודולוגית של סיכוני אבטחה. ההוצאות הכספיות על אמצעי הבקרה צריכות להיקבע לפי הנזק העלול להיגרם לעסק ממקרי כשל אבטחה. אפשר ליישם טכניקות של הערכת סיכונים לכל משרד, או רק לחלקים ממנו, ואפילו למערכות מידע מסוימות בלבד, לרכיבים ספציפיים במערכת או לשירותים ספציפיים, לפי מידת התועלת ולפי העניין.

הערכת סיכונים היא שיקול שיטתי של:

א. הנזק העלול להיגרם לעסק כתוצאה מכשל אבטחה, בהתחשב בהוצאות אפשריות של אובדן חיסיון, כלילות או זמינות של מידע ושל נכסים אחרים,

ב. הייתכנות הממשית של התרחשות כשל כזה, לאור האיומים הקיימים והפגיעויות, ועל סמך אמצעי הבקרה המיושמים באופן שוטף

תוצאות ההערכה יסייעו לקבוע מהן פעולות הניהול שראוי לנקוט, איך לקבוע קדימויות לניהול סיכוני אבטחת מידע, ואיך ליישם את אמצעי הבקרה שנבחרו, כדי להתגונן מפני הסיכונים. ייתכן שאת תהליך ההערכה ובחירת אמצעי הבקרה צריך יהיה לבצע כמה פעמים, כדי לטפל בחלקים שונים של המשרד או במערכות מידע שונות.

חשוב לסקור את סיכוני האבטחה באופן סדיר וליישם אמצעי בקרה, כדי להבטיח:

א. שהובאו בחשבון שינויים בדרישות העסק ובקדימויות שלו,
ב. שהובאו בחשבון איומים חדשים ופגיעויות חדשות
ג. שהובטח שאמצעי הבקרה לא יאבדו את האפקטיביות ואת הנאותות שלהם.

ייערכו סקרים ברמות שונות של עומק, לפי תוצאות ההערכות הקודמות ולפי השינויים ברמות הסיכון שההנהלה מוכנה לקבל. הערכות סיכונים נעשות לעתים קרובות קודם כל ברמה גבוהה, כאמצעי לקביעת קדימויות להקצאת משאבים בתחומים שבסיכון גבוה, ואחר כך יורדים לרמות מפורטות יותר, כדי לטפל בסיכונים ספציפיים.

בהמשך לסקר הסיכונים, נדרשת המלצה באשר לאמצעי ההגנה שיפחיתו את הסיכון. בבחינת מידת היעילות של אמצעי הגנה שונים כגון פגיעויות שונות ויריבים שונים, ובחישוב הסיכון שנותר לאחר יישום אמצעי הגנה אלה, ניתן לבדוק מהי הדרך היעילה להפחתת הסיכון, והאם הסיכון השיורי הוא כזה שמוכנים/יכולים לחיות איתו.

רצוני להציג למקבלי ההחלות יותר מאפשרות (חבילת אמצעי הגנה) אחת, כאשר לכל אפשרות מוצגת עלותה (מחיר המשאבים הנחוצים ליישומה, ומידת פגיעתה בתפקוד הארגון) והסיכון השיורי הנובע מיישומה. בדרך זו מועבר המידע הנחוץ למקבלי ההחלטות.

<u>ניהול סיכונים כפעילות מתמדת</u>

מודל ניהול סיכונים הוא תהליך רציף, ואינו מיועד להציג את הסיכונים לארגון רק בנקודת זמן אחת. על הארגון לבחון כל העת שינויים בנכסים, באיומים ובפגיעויות, וכן בסיבה בה מתקיים הארגון. כשמזהים שינויים, יש להעריך מחדש את הסיכונים ולבחון את התאמת אמצעי ההגנה. במידת הצורך,יש להמליץ על יישום אמצעי הגנה חדשים ועל ביטול או שינוי אמצעי הגנה ישנים.

מקורות

מכון התקנים הישראלי, תקן 7799: ניהול אבטחת מידע, הוראות שב"כ.

גורמי אבטחת מידע – הגדרות ותפקידים

נוהל מס' 4

מבוא

חוק הגנת הפרטיות מחייב את כל הגופים הציבוריים במינוי ממונה על אבטחת מידע.

לצורך ניהול ויישום אבטחת המידע במשרדים, יושתת המבנה הארגוני על עקרון "הפרדת הסמכויות" אשר על פיו תמנה הנהלת המשרד בעלי תפקידים בתחום זה – ראה בהמשך.

מטרות הנוהל

מתן דגש למדיניות אבטחת מידע בהגדרת סמכויות אבטחת מידע במשרדי הממשלה ותפקידיהם. פירוט אחריות, כפיפות, תפקידים, סמכויות ופעילות לצורכי אבטחת מידע במשרד.

אחראי לביצוע הנוהל

להלן בעלי התפקידים המרכיבים את המבנה הארגוני ליישום אבטחת מידע במשרד:

גורם ניהולי בכיר – מנכ"ל או הסמנכ"ל למינהל ולמשאבי אנוש, בעלי האחריות ליישום נהלי אבטחת מידע של המשרד, על פי חוק הגנת הפרטיות, התשמ"א – 1981 ותיקוניו.

גורם מכוון – וועדת היגוי לאבטחת מידע, שתפקידה בין היתר, להמליץ בדבר קווים מנחים, אישור נהלים מוצעים, הכוונה בקביעת מדיניות בדבר הרשאות גישה למידע וקביעת האירועים והפעילויות החריגות, שמהווים סיכון בכוח או בפועל, לניהולו התקין של המשרד. **ראה נוהל "ועדות היגוי למחשוב".**

גורם ניהולי אבטחתי - הממונה על אבטחת מידע – מהווה גורם מקצועי – אבטחתי, הפועל על פי נהלי אבטחת המידע במשרד. תפקידו יהיה לכוון את בעלי התפקידים ואת כלל "משתמשי הקצה" לשמור נהלי אבטחת מידע. הממונה מוסמך לערוך ביקורת לבחינת אופן יישום נהלי אבטחת מידע. הממונה אחראי ליזום, לעדכן, להטמיע וליישם נהלי עבודה והנחיות, בתחום אבטחת מידע.

גורם סיוע אבטחתי – נאמני אבטחת מידע – בעלי תפקיד טכני בתחום הטיפול והתחזוקה של מערכות המידע ביחידותיהם – שבנוסף לתפקידם הם מסייעים לממונה אבטחת מידע ביישום הנהלים ומונחים על ידו (בנושאי האבטחה).

גורמי ביצוע – **מנהלי מערכות המידע, מנהלי מאגרי המידע ועובדי התשתיות – אחראים על יישום הכלים והשיטות לאבטחת מידע, על פי נהלים שקבעה הנהלת המשרד, ובהנחיה ישירה של ממונה אבטחת מידע.**

גורם אחראי על מסירת מידע לציבור – בעל סמכות לבחינת בקשות מגורמים חיצוניים לקבלת מידע המצוי במשרד ואישורן, או דחייתן, על פי הוראות חוק לחופש המידע, התשנ"ח – 1998.

גורם אחראי על מסירת מידע לגופים ציבוריים – כמתחייב מחוק הגנת הפרטיות התשמ"א- 1981, נושא זה יטופל ע"י הממונה על אבטחת מידע.

גוף הנוהל

תפקידיו העיקריים של ממונה אבטחת מידע:

1) פיתוח, עדכון, הדרכה, הטמעה, הפצה ובדיקת היישום של נהלי אבטחת מידע.

2) מתן ייעוץ בנושאי אבטחה ובקרה בעת פיתוח יישומים חדשים.
3) בדיקת יישומים קיימים ומתן ייעוץ לשיפור הבקרות בהם.
4) טיפול שוטף בהרחבת המודעות לסוגיות אבטחת מידע בדרגים השונים.
5) הכנת תוכנית פעילות שנתית בנושאי אבטחת מידע, במסגרת ועדת היגוי למחשוב ועמידה ביעדים שהוצבו.
6) דיווחים לוועדת היגוי למחשוב.
7) סיוע במיפוי וסיווג של מאגרי המידע השונים.
8) אחזקת הרישום המעודכן של כל היישומים וסיווגם.
9) חברות בוועדת ענ"א.
10) תיאום עם גורמי הביקורת וביטחון המשרד.
11) מיפוי ההרשאות, כולל עדכון שוטף.
12) הגדרת פעילויות חריגות.
13) מעורבות בהתקשרות עם גורמי חוץ רלוונטיים ומתן הנחיות אבטחת מידע על פי הצורך.
14) פיקוח על שירותי ספקים רלוונטיים.
15) יעוץ בעת חתימת חוזים רלוונטיים.
16) ריכוז כל סיכומי אירועי ה"וירוסים", תקלות וניסיונות פריצה במשרד.
17) השתתפות בהכנת תכנית התאוששות מאסון והמשכיות עסקית.
18) ייזום בדיקות תקופתיות במחשבים אישיים.
19) ייזום בדיקות תקופתיות של רשת החשמל וציוד מיגון למערכות מחשוב במשרד.
20) ייזום תקופתי של בדיקות סיכוני האש ומערכת המניעה, ע"י מומחים.
21) קשר עם רשם מאגרי המידע במשרד המשפטים, כולל טיפול בדרישות החוק.
22) אחזקת הרשימות המעודכנות של הגורמים המחזיקים בנהלי אבטחת מידע.
23) קיום מפגשים תקופתיים עם נאמני אבטחת מידע והנחייתם בהתאם לצורך.

הממונה יתאם את פעילותו בתחומים הרלוונטיים עם היחידה למערכות מידע של המשרד, היחידות השונות ועם גורמי המטה של המשרד כגון: יועץ משפטי, קב"ט ארצי, אחראי לניהול רשומות וכו'.

הממונה יכין לקראת כל ישיבה של ועדת היגוי למחשוב דו"ח מפורט, שיכלול את כל העשייה למן הישיבה הקודמת, ובין היתר את כל הליקויים שנחשפו. כן יכלול הדו"ח את תכנון הפעילות לתקופה הבאה.

מנהל אגף מערכות מידע (מנמ"ר).

קיימת חשיבות תפעולית ואבטחתית במינוי אחראי לכל מערכת מידע. מנהל האגף ינחה, יתאם וירכז פעילות האגף. כמו כן, המנהל או מי שהוסמך עלי ידו, ימנה אחראי לכל מערכת הקיימת במשרד (כגון מערכת כוח אדם, מערכת שכר, מערכת רכש וכד'). אחראי המערכת ירכז את כל המשתמשים ויהיה זה המוסיף או הגורע משתמשים מן המערכת. אחראי מערכת יתודרך תקופתית ע"י הממונה על אבטחת מידע במכלול נושאי האבטחה השוטפים והמתחדשים. ביעור חומר עודף או מיותר יתבצע ע"י אחראי המערכת.

נאמן אבטחת המידע יקבל תדרוך לתפקידו בכתב ובעל פה ע"י הממונה על אבטחת מידע.
כאשר יש כוונה למנות כנאמן אבטחת מידע את "נאמן הביטחון" שמונה ע"י הקב"ט, ייעשה המינוי בתאום עם הקב"ט הארצי.
בכל מקום בו יש רפרנט למחשוב, ישמש הוא כנאמן אבטחת מידע.
בכל מקום בו קיימת רשת מקומית, ישמש מנהל הרשת נאמן אבטחת הרשת.
ממונה אבטחת מידע ינהל רשימה מעודכנת של כל נאמני אבטחת מידע, לרבות לאריכי מינויים.
הממונה על אבטחת המידע יקיים מפגשים עם נאמני אבטחת מידע, באתרים השונים, בהתאם לצורך.
פעם בשנה, לכל הפחות, תיערך השתלמות לקבוצת נאמני אבטחת מידע.

מקורות

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

נוהלי אבטחת המידע בעיריית ירושלים ,פברואר 2001.

נוהלי אבטחת מידע של רשות הדואר, דצמבר 2002.

ועדות היגוי למחשוב ואבטחת מידע

נוהל מס׳ 5

מטרות הנוהל

להסדיר פעילותה של הסמכות העליונה בנושא אבטחת מידע. לנהל את אבטחת המידע בתוך המשרד.

גוף הנוהל

אבטחת מידע היא אחריות של המשרד, המתחלקת בין כל חברי צוות הניהול. לכן יש להקים ועדת מנהלים שתבטיח קיום הכוונה ברורה ליוזמות בנושאי אבטחה ושהתמיכה בהן נראית לעין. הוועדה תקדם נושאי אבטחה ברחבי המשרד, באמצעות מחויבות נאותה והקצאת משאבים נאותים. הוועדה יכולה להיות חלק מגוף ניהול קיים. ועדה כזו מקבלת על עצמו בדרך כלל את המחויבויות שלהלן:

א. סקירה ושיפור של מדיניות אבטחת מידע ואחריות כללית
ב. ניטור שינויים משמעותיים במידת החשיפה של נכסי מידע לאיומים גדולים
ג. סקירה וניטור של אירועי אבטחה
ד. שיפור יוזמות עיקריות לחיזוק אבטחת המידע

במשרד גדול, לצורך תיאום היישום של בקרות אבטחת מידע, ייתכן שיהיה צורך בהקמת ועדה בין תחומית של נציגי ההנהלה מתחומי המשרד הרלבנטיים. ועדה כזו מקבלת על עצמו בדרך כלל:

א. לקבוע תפקידים מוגדרים ואחריות מוגדרות בנושאי אבטחת מידע בכל המשרד,
ב. לקבוע מתודולוגיות ותהליכים לאבטחת מידע, כגון הערכת סיכונים ושיטת סיווג אבטחה,
ג. להסכים לגבי יוזמות כלל ארגוניות בנושא אבטחת מידע לתמוך בהן, כגון הפעלת תוכנית להגברת מודעות לאבטחה,
ד. לוודא שהאבטחה היא חלק מתהליך תכנון המידע עוד בתחילתו ולא רק הביקורת שבסוף התהליך,
ה. להעריך את הנאותות של בקרות מוגדרות של אבטחת מידע, המיועדות למערכות או לשירותים חדשים, ולתאם את יישומן,
ו. לסקור אירועי אבטחת מידע,
ז. לקדם את הפרסום של תמיכת המשרד באבטחת מידע, ברחבי המשרד.
ח. תקצוב פעולות אבטחת מידע.

הוועדה לנושא אבטחת מידע הנה הסמכות העליונה לנושא זה, ותתפקד לצורך זה באופן רציף.
הוועדה תורכב מנושאי המשרה הבאים:

א. סמנכ״ל בכיר למינהל, יו״ר.
ב. מנהל אגף בכיר למערכות מידע וענ״א.
ג. חשב המשרד.
ד. המבקר הפנימי.
ה. נציג היועץ המשפטי.
ו. קצין הביטחון.
ז. הממונה על אבטחת מידע – מרכז.

מוזמן קבוע: נציג האגף לביקורת המדינה והביקורת הפנימית במשרד ראש הממשלה.

הוועדה תעסוק בין היתר בנושאים הבאים:

א. קביעת מדיניות המחשוב ואבטחת מידע.

ב. אישור תוכניות עבודה שנתית בתחום אבטחת מידע, לרבות תקציבים, לוחות זמנים ותחומי אחריות.
ג. קבלת דיווחים ומעקב ביצוע.
ד. סיווג המידע

הוועדה תתכנס לפחות פעמיים בכל שנת כספים.

הוועדה תוכל להזמין לישיבותיה מומחים ונציגי משתמשים, בהתאם לצורך.

מקורות

החלטות הממשלה מספר **בק/9** מיום 20 למארס 1997, ו- **בק/179** מיום 23 למארס 1999.

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

נוהלי אבטחת המידע בעיריית ירושלים ,פברואר 2001.

נוהלי עבודה – אגף לשירותי מידע ומחשוב, משרד הבריאות, פברואר 2000.

נוהלי אבטחת מידע של רשות הדואר ,דצמבר 2002.

בדיקת מהימנות העובדים, התחייבות לשמירת הסודיות

נוהל מס' 6

מטרות הנוהל

להפחית סיכוני טעויות אנוש, גניבה, הונאה או שימוש לרעה במידע הנאגר במשרד. נושאי אבטחת המידע ושמירת הסודיות יטופלו בשלב גיוס העובדים, יכללו בחוזים, וינוטרו במשך זמן העסקתו של העובד. כל מועמד פוטנציאלי לעבודה יתוחקר כראוי, במיוחד עבור תפקידים רגישים. כל העובדים ומשתמשי צד שלישי, המשתמשים באפשרויות לעיבוד מידע, יחתמו על הסכם שמירת חיסיון.

אחראי לביצוע הנוהל

כל גורם המועסק במשרד, ישא באופן אישי באחריות לשמירה על המידע המצוי בשימושו ו/או אשר הגיע לידיו/ידיעתו. מנהל מחלקת כ"א ישא באחריות להחתמת עובדי המשרד. מנהלי היחידות בהן מועסקים עובדי קבלן/ספקי משנה, יישאו באחריות להחתימם על טופס זה.

גוף הנוהל

תנאי ההעסקה יציינו את אחריותו של העובד לאבטחת מידע. אם אפשר, האחריות תהיה תקפה למשך תקופה מוגדרת גם אחרי גמר העסקתו במשרד. יפורט גם איזו פעולה יש לנקוט במקרה שהעובד אינו מציית לדרישות האבטחה. הזכויות והחובות של העובד בנושא אבטחה, כגון על פי דיני שמירת זכויות יוצרים והחקיקה בנושא הגנת נתונים, יובהרו ויכללו בין תנאי העסקתו. גם האחריות לסיווג ולניהול של נתוני המעסיק תיכלל. אם אפשר, תנאי ההעסקה יכללו גם הצהרה שאחריות חלה על עובד גם מחוץ לכותלי המשרד וגם מעבר לשעות העבודה הרגילות, כגון במקרה של עבודה בבית.

הנוהל יחול גם על יועצים, עובדים בפרויקטים ועובדי חברות כוח אדם וגם על קבלני המשנה. כל עובדי המשרד יוחתמו על טפסי התחייבות לשמירת סודיות המידע המגיע לידיעתם, בתוקף תפקידם, עם קליטתם בעבודה. החתימה תתבצע באופן אישי, באמצעות יחידת משאבי אנוש. הטופס החתום יישאר ויתויק בתיק העובד. העתק יימסר לעובד. עובדים, המועסקים דרך קבלנים, יחתמו בנוסף לטופס "הצהרה וכתב התחייבות בדבר שמירה על הסודיות", גם על טופס "הצהרה ושמירת סודיות של גורם חוץ". החתימה תתבצע באופן אישי, בפני נאמן אבטחת מידע או גורם מוסמך אחר. החברה המעסיקה את העובדים תתחייב כלפי המשרד לשמירת המידע ואי שימוש בו לצרכים אחרים מאלו שלהם נוצרו קשרי העבודה הספציפיים.

מנהלי היחידות בהן מועסק עובד קבלן/ספק משנה, ידווחו לממונה אבטחת מידע טרם תחילת העסקתו של הגורם, ויקבלו ממנו הנחיות אבטחת מידע כתובות, בהתאם לצורך, כנספח לטופס ההתחייבות לשמירת סודיות. מנהלי היחידות יוודאו החתמתו של הגורם ויעבירו העתק מהנספח החתום לממונה אבטחת מידע. הטפסים ישמרו לתקופה מוגדרת מיום עזיבתו של העובד/גורם חוץ.

מקורות

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.
אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.
נוהלי אבטחת המידע בעיריית ירושלים ,פברואר 2001.
מכון התקנים הישראלי, תקן 7799: ניהול אבטחת מידע.

קשר עם גורמי חוץ ב-outsourcing (מיקור חוץ)

נוהל מס׳ 7

מטרת הנוהל

הגדרת אופן קיום הקשר העסקי עם גורמי חוץ, במגמה לצמצם את הסיכון למערכות הממוחשבות ולמאגרי מידע.

אחראי לביצוע הנוהל

מנהל היחידה המעסיקה את גורם החוץ יוודא החתמתו על נספח אבטחת מידע, תוך מעורבותו של מממונה אבטחת מידע, כמפורט בהמשך. באחריות מנהל היחידה לוודא כי גורם החוץ המועסק על ידו אושר מראש על ידי ממונה אבטחת המידע וכי הנחיות נוהל זה ייושמו לגביו.

ממונה אבטחת המידע יהיה אחראי לביצוע הנחיות נוהל זה, בכל הנוגע לאישורו של גורם החוץ, כמפורט בנוהל זה.

גוף הנוהל

ייחתם חוזה עם כל גורם חוץ או נציגיו הבאים במגע חיצוני עם עמדת עבודה או המחשב המרכזי (למשל קבלן ניקיון), בו תהיה התייחסות מיוחדת לנושא אבטחת המידע. ההתקשרות עם גורם החוץ מותנית באישור מוקדם של ממונה אבטחת המידע. החוזה יתייחס לטיפול נאות בציוד, לאי נגיעה בעמדות העבודה, לאי נגיעה בחומר הנמצא באמצעים מגנטיים/פלטים מודפסים/ מסמכי קלט, ובשמירה מוחלטת של סודיות לגבי כל שיתגלה בפניהם.

בחוזה עם כל גורם חוץ, כולל ספק ציוד או שרות לחומרה או תוכנה, ייקבע פרק בנושא אבטחה שיכלול את כל הנחיות אבטחת המידע המתייחסות לכלל דרכי הגישה של גורם החוץ למידע, באשר הוא, כאמור בסעיף הקודם. בנוסף לכך יכלול החוזה את הרשימה השמית המדויקת של נציגי גורם החוץ שיורשו לבצע את הפעילות עבור המשרד, וכן התחייבות שלא להוציא כל חומר ו/או ציוד מהמשרד, אלא בידיעת וברשות מפורשת של ממונה אבטחת המידע.

עניין השירות מתייחס גם למצעים מגנטיים, כולל כאלה שהוגדרו כבלתי שמישים.

שילוב תנאי האבטחה בחוזה יהיה באחריות הגורם המזמין (מנהל היחידה).

בנוסף להנחיות המפורטות לעיל, יחתמו גורם החוץ ועובדיו על התחייבות לשמירת סודיות.

מנהל היחידה המבקש ליצור קשרי עבודה עם גורם חוץ חדש, יוודא החתמתו הנאותה על החוזה הכולל את נספח אבטחת המידע. כל זאת, בטרם תחילת העסקתו ו/או נגישותו למידע, המוקדם מבין השניים, ותוך קבלת אישורו מראש של ממונה אבטחת המידע.

זיהוי סיכונים הנובעים מגישת צד שלישי

לסוג הגישה הניתן לצד שלישי חשיבות מיוחדת. למשל, הסיכונים בגישה דרך חיבור לרשת, שונים מהסיכונים הנובעים מגישה פיזית. סוגי הגישה שיש לשקול הם אלה:

א. גישה פיזית, כגון גישה למשרדים, לחדרי מחשבים, לארונות תיוק.
ב. גישה לוגית, כגון למסד נתונים של הארגון, למערכות המידע.

צד שלישי יכול לקבל הרשאת גישה מכמה סיבות. למשל, צד שלישי שהוא ספק שירותים לארגון והוא איננו ממוקם באתר, יכול לקבל אפשרות לגישה פיזית ולוגית, כגון:

א. צוות תמיכה בחומרה ובתוכנה, הזקוקים לגישה ליישומים ברמת המערכת או ברמה נמוכה יותר,

ב. שותפי סחר או שותפים עסקיים העשויים להחליף מידע ביניהם, לגשת למערכות המידע או לחלוק ביניהם מסדי נתונים משותפים.

המידע עלול להיחשף לסכנה אם הצד שלישי אינו מנהל כראוי את אבטחת המידע. אם יש צורך עסקי להתחבר לאתר שבו ממוקם הצד שלישי, תיעשה הערכת סיכונים כדי לזהות כל דרישה לאמצעי בקרה מיוחדים. ההערכה תביא בחשבון את סוג הגישה הנדרש, את ערכו של המידע, את אמצעי הבקרה שהצד שלישי משתמש בהם ואת השלכות מתן הגישה הזאת על אבטחת המידע של הארגון.

צד שלישי הממוקם בתוך הארגון לפרק זמן מוגדר בחוזה, עלול אף הוא לגרום היווצרות של נקודות תורפה באבטחה. דוגמות לצד שלישי הממוקם בתוך הארגון הן:

א. צוותי תמיכה ותחזוקה של חומרה ותוכנה,
ב. שירותי ניקיון, הסעדה, שמירה ואנשי שירותים אחרים חיצוניים,
ג. סטודנטים ועובדים מזדמנים אחרים המועסקים לפרקי זמן קצרים,
ד. יועצים.

חיוני להבין אילו אמצעי בקרה נחוצים כדי לנהל גישת צד שלישי למתקני עיבוד מידע. בדרך כלל, כל דרישות האבטחה הנובעות מגישת צד שלישי או אמצעי הבקרה הפנימיים, יובאו לידי ביטוי בחוזה שנערך עם הצד השלישי. למשל, אם יש צורך מיוחד בשמירת חיסיון המידע, אפשר להשתמש בהסכם אי-חשיפה.
גישת צד שלישי למידע ולמתקני עיבוד מידע, לא תינתן אלא לאחר שיושמו הבקרות הראויות ונחתם חוזה המגדיר את תנאי ההתחברות או הגישה.

סידורים הקשורים בגישת צד שלישי למתקני עיבוד מידע של הארגון, יתבססו על חוזה רשמי המכיל את כל דרישות האבטחה, או המתייחס אליהן, כדי להבטיח התאמה לשיטות האבטחה ולתקני האבטחה של הארגון. החוזה יבטיח שלא יהיו אי-הבנות בין הארגון לבין צד שלישי. ארגונים יבטיחו את עצמם באשר לשיפוי של הספק שלהם. להלן עניינים שיש לשקול הכללתם בחוזה:

א. המדיניות הכוללת לגבי אבטחת המידע,
ב. הגנת נכסים, לרבות:
   1. נהלים להגנת נכסים ארגוניים, לרבות מידע ותוכנה,
   2. נהלים לקביעה האם הייתה העמדה בסכנה של נכסים כלשהם, כגון, האם נתונים אבדו או שונו,
   3. אמצעי בקרה להבטיח החזרה או השמדה של מידע ונכסים בגמר תקופת ההתקשרות החוזית, או בכל נקודת זמן אחרת במהלך ההתקשרות,
   4. כלילות (integrity) וזמינות,
   5. הגבלות העתקה וחשיפה של מידע

ג. תיאור של כל שירות שייעשה זמין,
ד. רמת השירות המיועדת ורמות אי קבילות של שירות,
ה. אמצעים להעברת צוות העובדים, לפי העניין,
ו. ההתחייבויות (החבויות) המתאימות של הצדדים להסכם,
ז. האחריות לגבי עניינים הקשורים בחוק, כגון חקיקה בנושאי הגנת נתונים, תוך התחשבות מיוחדת במערכות חוקים שונות, במקרה שהחוזה כרוך בשיתוף פעולה עם ארגונים בארצות אחרות.
ח. זכויות קניין רוחני, זכויות יוצרים והגנה על כל עבודה משותפת,
ט. הסכמים לגבי בקרת גישה, הכוללים:
   1. שיטות גישה מורשות, בקרות מזהים ייחודיים (חד ערכיים) והשימוש בהם, כגון מספר זיהוי של משתמש וסיסמא,
   2. נוהל הרשאה למשתמש, לקבלת גישה וזכויות יתר,
   3. דרישה לתחזק רשימה של האנשים המורשים להשתמש בשירותים הזמינים, ופירוט זכויותיהם וזכויות היתר שלהם לגבי שימוש כזה,

י. הגדרת קריטריונים לביצועים הניתנים לאימות, ניטורם והדיווח לגביהם,

יא. הזכות לנטר את הפעילות המשתמש ולהפסיקה,
יב. הזכות לבדוק אחריות חוזיות או הזכות למסור את עריכת המבדקים לצד שלישי,
יג. קביעת תהליך מתפתח לפתרון בעיות, סידורים לשעת חירום יובאו אף הם בחשבון, לפי העניין
יד. האחריות לגבי התקינות ותחזוקה של חומרה ותוכנה,
טו. מבנה ברור של דיווח וטופסי דיווח מוסכמים,
טז. תהליך ברור ומוגדר של ניהול שינויים,
יז. כל בקרה הדרושה להגנה פיזית ומנגנונים שיבטיחו שהבקרה מתפקדת,
יח. הכשרת משתמשים ואנשי מנהלה בשיטות, נהלים ואבטחה,
יט. בקרות להבטחת הגנה מפני תוכנה זדונית,
כ. סידורי דיווח, יידוע וחקירה של אירועי אבטחה ופריצות אבטחה,
כא. מעורבות צד שלישי עם קבלני משנה.

הערה

בנוסף ראה נוהל "אבטחת מידע בפיתוח מערכות מידע חדשות".

מקורות

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

נוהלי אבטחת המידע בעיריית ירושלים ,פברואר 2001.

מכון התקנים הישראלי, תקן 7799 : ניהול אבטחת מידע.

מודעות, הדרכה, הטמעה והסברה

נוהל מס׳ 8

מטרות הנוהל

להבטיח שהמשתמשים, מנהלי המערכות ואנשי התמיכה מודעים לאיומי אבטחת המידע, ושהם מצוידים בכל הדרוש לתמיכה במדיניות האבטחה של המשרד בעבודתם הרגילה.

אחראי על ביצוע הנוהל

יישום הנחיות אבטחת המידע המוכתבות במשרד חלות על כל עובד באופן אישי, ברמת המידע בו הוא עוסק ו/או המגיע לידיו או לידיעתו.

ממונה אבטחת מידע ישא באחריות לביצוע הנחיות נוהל זה.

גוף הנוהל

המשתמשים יקבלו הדרכה בנושא נהלי אבטחה והשימוש הנכון באפשרות לעיבוד מידע, כדי למזער סיכוני אבטחה אפשריים. פעילות הדרכה תקבל תקציב הולם.
מנהלי המערכות השונות ואנשי התמיכה יקבלו הדרכה שהם אלה שאחראים ליישום אבטחת המידע בשטח – וממונה אבטחת המידע אחראי מינהלית.

כל עובדי המשרד, ואם רלוונטי – גם משתמשי צד שלישי, יקבלו הדרכה נאותה ויעודכנו דרך קבע באשר לשיטות הפעולה והנהלים של המשרד. ההדרכה תכלול דרישות אבטחה, מחויבויות על פי החוק ובקרות של המשרד, וכן הדרכה לשימוש נכון באפשרות לעיבוד מידע, כגון נהלי כניסה למערכת, שימוש בחבילות תוכנה, כל זאת, לפני מתן הרשאת גישה למידע או לשירותים.

פעם בשנה תתבצענה פעילויות הדרכה בנושא אבטחת מידע לקבוצות עובדים, משתמשי מחשב ו/או לקבוצות להן נגיעה למידע. הפעילות תתבצע באופן קבוצתי בחלוקה לבעלי תפקידים שונים: מנהלים בכירים, עובדי האגפים השונים, מתאמי מחשוב, מנהלי מאגרים וקבוצות עובדים אחרות.

ההדרכה תאורגן ע״י ממונה על אבטחת המידע, בתיאום עם הממונה על ההדרכה. ימי עיון ייעודיים לעובדים חדשים או שטרם הודרכו, יתואמו עם מחלקת הדרכה.

במהלך השנה תתבצע פעילות של רענון להגברת המודעות האבטחתית.

אודות כל יישום, תתבצע הדרכה להצגת הכלים האבטחתיים הנוגעים לאותו יישום. מדבקות ופלקטים שיעודדו מודעות לנושאי האבטחה, יפוזרו בקרבת מוקדים של מערכות ממוחשבות.

מנהלים ועובדים יתודרכו לדווח על כל חריגה או על כל תופעה לא סבירה או תמוהה בתחום המערכות הממוחשבות ובכל נושא העלול להשליך על נושאי אבטחת המידע. דיווח של עובד יימסר באמצעות הממונה עליו, אלא אם מעורב במקרה הממונה עצמו.

כל מקרה של אירוע אבטחתי חריג ייחקר. מטרת התחקיר – הסקת מסקנות כדי למנוע אירוע כזה בעתיד.

במקרה של חשד לעבירה משמעתית או פלילית בנוגע לגילוי סודות או למסירת מידע שלא כדין, יש לדווח מייד לסמנכ״ל בכיר למינהל.

מקורות

חוק הגנת הפרטיות, התשמ״א – 1981, ותקנותיו.

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

נוהלי אבטחת המידע בעיריית ירושלים ,פברואר 2001.

מכון התקנים הישראלי, תקן 7799 : ניהול אבטחת מידע.

Social Engineering – הנדסה חברתית

נוהל מס׳ 9 (בהכנה)

הגדרה:

Social Engineering (הנדסה חברתית) הינה ביצוע מניפולציות של גורם חיצוני (וגם פנימי) על עובדים בארגון, על מנת לזכות בזכויות גישה שלא כדין אשר יאפשרו לו גישה כמשתמש לגיטימי למידע בעל ערך או למערכת בה אגור מידע בעל ערך.

מתקפת Social Engineering מוצלחת איננה מעוררת חשד כי ברוב המקרים אין כלי תוכנה / חומרה אשר יכולים להתריע על התרחשותם.

אחראי על ביצוע הנוהל

על הממונה על אבטחת המידע בארגון לוודא כי לא ניתן יהיה להשיג מידע רגיש תוך שימוש ב-Social Engineering. נוהל מסגרת זה מצביע על כשלי אבטחה וסימנים המעידים על מתקפת, ומציע דרכי התגוננות.

גוף הנוהל

כשלי אבטחה המקלים על ניצול מתקפת Social Engineering

א. אי הקפדה על מדיניות סיסמאות
ב. חיבור מודמים ובעקבותיהם תוכנות כגון Anywhere–PC
ג. תהליכי תמיכה Help Desk – אשר אינם נותנים מענה לאיום.
ד. אתרי אינטרנט ארגוניים המספקים מידע עודף / מיותר על תהליכי העבודה והמבנה הארגוני.

איך מתגוננים:

1. אבטחה פיזית:
בודד את הזרים / אוחים בארגון.
השיטה: חובת ענידת תגים לכל. תג עובד שונה ויזואלית באופן בולט מתג אורח / מבקר. בנוסף, יש לוודא כי מידע מסווג איננו ניתן להשגה מקרית על ידי בלתי מורשה.

2. אין להשאיר מרווח לשיקול דעת במתן תמיכה בנושא סיסמאות / הזדהות כלפי הגורם נותן תמיכה.
אין להעביר סיסמא באופן שאיננו מבטיח כי היא מועברת רק למי שזכאי לקבלה כדין. לדוגמא: קבע מערכת הזדהות חליפית אקראית, חייב הזדהות פיזית במקרים מסוימים וכדו׳.

3. מול כל גורם נותן תמיכה (בנוסף ל – Help Desk), יש לבסס שיטות להזדהות, הן של המשתמש והן של גורם התמיכה.

4. הצב מגרסות במספר מספיק ובפריסה ארגונית מתאימה.

5. קבע מדיניות והנהג נהלים. על מנת שאילו יהיו אפקטיביים עליהם לכלול:
- נהלים הניתנים למימוש בלבד.
- לתמצת כללי התנהגות לעובדים: בעיקר ״עשה״ ואל תרבה ב״אל תעשה״.
- להתעדכן תקופתית.
- נגישות לכל העובדים דרך אינטרא-נט.

והעיקר: מודעות ועוד מודעות לעובדים ולמנהלים בכל עת: בעת קבלה לעבודה, בעת פגישות הנהלה, בעת פגישות מחלקתיות / צוות.

סימנים מעידים למתקפת Social Engineering:

א. סירוב לבקשת פעילות לפי הנהלים.
ב. דרישה מוגזמת לזירוז התהליך.
ג. הפעלת לחצים / איומים על מנת לקבל השרות.
ד. בקשה לקבלת מידע מסווג האסור למסירה או מתן הרשאה שאיננה מותרת.
ה. השמטת שם.

שיטה טובה ליצירת מודעות, הינה הוספת link באתר האינטרא – נט של הארגון לנושא אבטחת מידע. ב-link זה מומלץ להקדיש תחום לנושא Social Engineering.
כמו כן, תרגול מצבים של מתקפת Social Engineering בדיוק כפי שמבצעים תרגול לכל סוג אחר של מתקפה.

מקורות:

הנוהל הוכן עפ"י הרצאתו של מר **יאיר רודיאקוב** מחברת Avnet בישיבת המועצה לביקורת ואבטחת מידע שהתקיימה בתאריך 19.11.2003.

ביקורת של אבטחת מידע

נוהל מס׳ 10

מטרת הנוהל

בדיקת יישום נהלי אבטחת מידע, בדיקת הבקרות לאבטחת מידע וקבלת היזון חוזר מן השטח. להגדיר את התהליכים הנדרשים לביצוע של תוכנית ביקורות תקופתיות.

אחראי לביצוע הנוהל

ממונה על אבטחת המידע יבצע ביקורות בתחום אחריותו המקצועית בכל הגופים הממשלתיים שבתחום המשרד.

גוף הנוהל

כל משרד יקבע לעצמו לוח זמנים לביקורות שוטפות ביחידת המחשב המרכזית, ביחידות השונות של המשרד הראשי, ביחידות הנמצאות מחוץ למבני המשרד הראשי ו/או במחוזות ובמוסדות הממשלתיים.

יש להשתדל לבצע כמה שיותר סוגי ביקורות על מנת לתת מענה מקיף לכלל תחומי אבטחת המידע. כדאי להכין רשימת תיוג לבדיקה מהירה של הנושאים, על מנת להקל עם הבודקים ושלא יפסחו על בדיקה כלשהי מחמת השכחה. יש להתייעץ עם המחלקה המשפטית לפני ביצוע ביקורות אשר עלולות לפגוע בצנעת הפרט, או לעבור על התקנות של חוק הגנת הפרטיות.

מבקר הפנים של המשרד יעודכן בתכני תכנית הביקורת עם פרסומה. לגבי כל ביקורת ייכתב פורמט המפרט את סוג הבדיקות שייערכו. רשימת הפרמטרים תועבר לנבדקים טרם ביצוע הביקורת בליווי התכנון הרבעוני.

ממונה על אבטחת המידע יתאם כל ביקורת מראש עם מנהל היחידה המבוקרת. זאת כדי להבטיח הערכות הגוף המבוקר לסייע בתהליך הביקורת.

ביקורת אבטחת משרדים

ביקורת אבטחת משרדים תבוצע בסוף יום העבודה. מטרתה לבדוק את יישום ההנחיות לאבטחת מידע בסיום יום העבודה.
ביקורת זאת תהיה ביקורת פתע ולא ייקבע לה תאריך מיועד בתוכנית הביקורת התקופתית.
הביקורת תבוצע בשיתוף עם קב״ט המשרד ונאמן אבטחת מידע של המחלקה הנבדקת.
הביקורת תבדוק את קיום נוהלי אבטחת המידע בסוף יום עבודה כפי שמופיעים בנוהל, ובכלל זה:
שמירת מסמכים רגישים בארון או מגירה נעולים,
כיבוי המחשב בסוף יום העבודה,
נעילת משרדים שמירת מחשב נייד למניעת גישת בלתי מורשים.

ביקורת תחנות קצה

ביקורת תחנות קצה תכלול בדיקה מדגמית של תחנות קצה.
הפרמטרים לבדיקה יתבססו על נוהל ״אבטחת תוכנה וחומרה במחשבים האישיים״ ובין היתר יכללו את הנקודות הבאות:

- עדכניות תוכנת האנטי וירוס וקבצי חתימות הוירוסים, וביצוע סריקות בהתאם לנוהל
- שימוש בסיסמא בהתאם לנוהל
- קיום חומרה לא מאושרת – דוגמת מודם
- שמירת קבצים על הספריות המקומיות
- קישוריות לאינטרנט
- תוכנות לא מורשות

את הבדיקה יש לערוך בנוכחות הבעלים של התחנה אשר עושה בה שימוש.

ביקורת שרתים

יש לבצע בדיקה מדגמית של השרתים במשרד. הבדיקה תוודא כי נוהלי אבטחת המידע של המשרד מקוימים הלכה למעשה. יש לתת דגש לשרתים חדשים או שרתים ששודרגו. הביקורת תיעשה תוך יידוע מנהל מערכות מידע. יש להסתמך בביקורת על נהלי המשרד הרלוונטיים למערכת (נהלי עבודה, נהלי הקשחת מערכת וכו') וכן על הנקודות הבאות:

- קיום ניהול הרשאות תקני בהתאם לנהלים
- הפרדה בין סביבת ייצור לפיתוח
- הגנה על קוד מקור וספריות מערכת
- אבטחת מערכת ההפעלה בהתאם לנוהל הקשחת שרת
- קיום ושמירת אמצעי גיבוי רלוונטיים
- קיום בקרה על אמצעי אבטחה ושימוש בקבצי ה-LOG
- מעבר תקופתי על קבצי LOG של המערכת
- הטמעת אמצעים למניעה ואיתור אירועי אבטחה (לדוגמא תוכנות אנטי – וירוס, תוכנות לגילוי ניסיונות פריצה וכו')

ביקורת תקשורת

יש לבצע בדיקה על תשתיות התקשורת במשרד. הבדיקה תכלול הרצת תוכנות IDS וביצוע מבדקי חדירה תקופתיים. ניסיונות חדירה למערכת תקשורת על ידי כלים ממוכנים (כגון: ניסיון פריצה לנתבים על ידי שימוש בכלי – JOHN THE RIPPER). כמו כן יבוצעו ביקורות מדגמיות על אבטחת התשתיות בהיבט הפיזי.

ביקורת אפליקציות

אחת לתקופה תבוצע ביקורת מדגמית על יישום במשרד. הבדיקה תכלול בין היתר את הפרמטרים הבאים:

- מעבר על לוגים לגילוי תקלות ובעיות שנרשמו.
- בדיקה מדגמית של הרשאות משתמשים במערכת
- בדיקה מדגמית של הרשאות משתמשים בעלי זכויות יתר במערכת
- גישה לנתונים שלא דרך היישום
- ניסיון לבצע מניפולציות כמשתמש מורשה במערכת של בעל הרשאות מינימליות
- ניסיון לעקוף את מנגנוני ההגנה ולקבל שליטה על המערכת כמנהל המערכת
- ניסיון לבצע מניפולציות במידע הנשמר בבסיס הנתונים המקושר ליישום

ביקורת חוק הגנת הפרטיות

מומלץ כי בכל רבעון ייבחר לצורכי ביקורת מאגר מידע, אשר מוגן מתוקף חוק הגנת הפרטיות ורשום כחוק. הביקורת תבדוק את ביצוע החוק והתקנות שנושאן אבטחת מידע. הביקורת תסתמך על הכתוב בנוהל "קיום חוק הגנת הפרטיות", וכן על כל שינוי/תיקון שנעשה בחוק האמור טרם ביצוע הביקורת. הביקורת תתואם ותלווה על ידי המנהל הממונה של המאגר. הנושאים שיבדקו:

- ביצוע רישום מאגרי מידע חדשים,

- מידת עדכניות פרטי הגדרת המאגר (לרבות בקרה מול פנקס המאגרים),
- עדכניות מינוי מנהל המאגר,
- תיעוד ותיוק השינויים והאישורים לכל מאגר מידע,
- בקרת השינויים היישומיים ו/או הטכנולוגיים שנעשו בין ביקורות בהקשר של שינויים בסיווג המידע שבמאגר (בין היתר בשינויים הנובעים משינוי במבנה הנתונים של המאגר), שיניים שהתרחשו ברמת השימושיות של המערכות ומידת הזמינות והגישה אל המערכת.

ביקורת בקרת גישה

ביקורת זו תבחן את קיום נהלי בקרת הגישה במתחם המשרד. בביקורת זו יש להתבסס על שני שלבים עיקריים:

- בדיקה סמויה, על ידי בקר חיצוני אשר ינסה לקבל גישה למתחם.
- ביקורת גלויה אשר תבדוק את ביצוע בקרת הגישה ברמה הפיזית בפועל.

יש להסתמך בפרמטרים לביקורת זאת על נוהל "אבטחת משרדי החברה".

כל ביקורת תסוכם בדו"ח תמציתי. הדו"ח יכלול:

א. מבוא קצר על יחידה והקשר שלה לנושאי אבטחת מידע.
ב. פירוט הנושאים שבוקרו.
ג. התרשמות כללית
ד. ליקויים שיש לתקן, כולל לוח זמנים וגורמים אחראים לתיקונם.

ברשימת הליקויים שיש לתקנם, יושם דגש על ליקויים חוזרים. לא תיערך ביקורת שלישית ביחידה לפני שיובטח תיקון כל הליקויים החוזרים. המקרה כזה, על הגוף המבוקר להוציא מכתב בו הוא מפרט את כל שעשה לתיקון הליקויים החוזרים, ואשר מאפשר לדעתו לבצע אצלו ביקורת נוספת.
הדו"ח יוגש גם למנהל הכללי של המשרד.

טיפול בממצאים שהתגלו

ממצאים שליליים שעלו במהלך הביקורת ידורגו על ידי מנהל אבטחת מידע שידרג את הממצאים שיש לטפל בהם ודחיפות הטיפול. על פי חומרת הממצאים יחליט מנהל אבטחת מידע על זמן סביר שיינתן לטיפול בממצא. עיקרי הממצאים ירוכזו ויועברו על בסיס רבעוני לעיון וועדת ההיגוי לאבטחת מידע. ממצאים הנוגעים ישירות לפעילותם של העובדים יובאו לידיעת העובד, מנהל אבטחת מידע, מנהל כוח אדם ומנהל הישיר של העובד.

ממונה אבטחת מידע ישמור אצלו את העתקי כל דו"חות הביקורת ממוינים לפי יחידות/שירותים/ אגפים/מוסדות וכו'. המידע יישמר בצורה שתאפשר ריכוז בעיות וכן אחזור תוך חיתוך על פי הגדרה.

ביקורות פתע ייערכו רק אחרי קבלת אישור מן המשנה למנכ"ל.

תוכנית הביקורת תתואם באחריות ממונה אבטחת מידע עם מבקר הפנים של המשרד והקב"ט, על מנת למנוע כפילויות והתנגשויות בביקורות השונות.

בכל ביקורת יתבצעו ע"י המבקר הפעילויות המתבקשות ממנו ישירות בנהלים: "רשימות תפוצה", "מצבת חומרה תוכנה".

בחירת אמצעי בקרה

משהוגדרו דרישות האבטחה, יש לבחור אמצעי בקרה וליישם אותם, כדי להבטיח את הקטנת הסיכונים לרמה קבילה. את אמצעי הבקרה ניתן לבחור מתוך מסמך זה או מתוך מסמך סדרה אחרת של אמצעי בקרה, וניתן לתכנן אמצעי בקרה חדשים, לפי הצרכים הספציפיים ולפי העניין. ישנן דרכים רבות לניהול סיכונים ומסמך זה מביא דוגמות של גישות מקובלות. על כל פנים, יש להבין שלא כל אמצעי בקרה ישים לכל מערכת מידע או לכל סביבה, ולא תמיד הוא ישים לכל משרד. לדוגמא, יש תיאור של הפרדת תפקידים כדי למנוע מעשי הונאה או טעויות. במשרדים קטנים ייתכן שלא ניתן יהיה להפריד את כל התפקידים, וצריך יהיה לפעול בדרכים אחרות כדי להשיג את אותן מטרות בקרה.

את אמצעי הבקרה יש לבחור על פי עלות יישומם, שתישקל לעומת הקטנת הסיכונים ולעומת הנזקים העלולים להיגרם במקרה של פריצת אבטחה. יובאו בחשבון גם שיקולים לא כספיים, כגון פגיעה במוניטין. אל חלק מאמצעי הבקרה במסמך זה אפשר להתייחס כאל עקרונות מנחים לניהול אבטחת מידע, הישימים לרוב המשרדים.

אמצעי הבקרה הנחשבים חיוניים לארגונים מבחינת החוק, הם אמצעים כגון:

א. זכויות קניין אינטלקטואלי
ב. הגנת רשומות הארגון
ג. הגנת הנתונים ופרטיות של מידע אישי

אמצעי בקרה הנחשבים אמצעים מקובלים ונאותים לאבטחת מידע, הם אמצעים כגון:

א. מסמך מדיניות אבטחת מידע
ב. הטלת אחריות בנושא אבטחת מידע
ג. הדרכה ותרגול בנושאי אבטחת מידע
ד. דיווח על אירועי אבטחה
ה. ניהול המשכיות עסקית (תכנית התאוששות)

אמצעי בקרה אלה ישימים לרוב המשרדים ולכל הסביבות. יש לציין, שלמרות העובדה שכל אמצעי הבקרה במסמך זה הם חשובים, יש לקבוע את הרלוונטיות של כל אחד מהם, לפי הסיכונים מיוחדים לכל משרד.

להלן מוצע שאלון תיוג כבסיס לביקורות אבטחת המידע.

אבטחת מידע בממשלה - שאלון להערכה עצמית

אחריות הניהול	קיים	לא קיים
1. קיום מדיניות אבטחת מידע		
2. קיום תהליך לבחינת יישום המדיניות		
3. קיום נוהל לניתוח סיכונים		
4. המצאות תוכנית אבטחה		
5. קיום נהלים לאבטחת תווך חיצוני		
6. הכרת המדיניות על ידי העובדים		
7. קיום תוכנית הדרכה לאבטחת מידע		
8. ביצוע הדרכת עובדים חדשים באבטחת מידע		
9. המצאות ממונה על אבטחת מידע		
10. קיום נוהל אבטחה והאם אושר		
11. האם מתקיימת הדרכה שוטפת בנושאי האבטחה		
12. האם מופעלת שיטה לאימות וזיהוי		
13. האם קיימת תוכנית גיבוי והתאוששות		
14. קיום תוכנית לטיפול באירועים		

אחריות הניהול	קיים	לא קיים
15. נהלים כתובים המגדירים סמכות ואחריות		
16. קיום מסמך המפרט את המערך הטכנולוגי והאחראים לו		

עובדי הארגון	קיים	לא קיים
17. האם מתקיימת בדיקת ביטחונית לעובדים חדשים		
18. האם מוחתמים העובדים על התחייבויות לשמירה מידע		
19. האם אובחנו נושאי תפקידים חיוניים במערכות המידע, והאם יש להם מחליפים		
20. האם הוזהרו נושאי משרה, בגין הפרת סודיות		
21. האם קיים נוהל אבטחת מידע לגבי קבלנים ועובדי חוץ		
22. האם קיים נוהל שימושי מקוצר (עמוד אחד), בנושאי המערכות ואבטחתן		
קבלנים		
23. האם קיים חוזה אחיד עם קבלנים בנושא האבטחה ושמירת מידע		
24. האם מתבצעים סיווגים ביטחוניים לקבלנים		
25. האם מתקיימות בדיקת ביטחוניות של נותני שירותים חיצוניים		

תוכנה	קיים	לא קיים
26. האם קיימות הנחיות בעניין הבאת תוכנה מחוץ למשרד		
27. האם קיימת התייחסות מוגדרת בתהליך הפיתוח, למגבלות אבטחה וביטחון		
28. האם מתקיים תהליך בדיקה, לפני רכישת תוכנה		
29. האם קיים נוהל להתקנה של תוכנה חדשה		
30. האם מופעלות תוכנות אנטי - וירוס בכל המערכות		
31. האם המשתמשים יודעים לטפל בוירוסים		
32. האם ישנו פיקוח על הורדת תוכנות מהרשת		
33. האם קיימת מודעות להוראות חוק זכויות יוצרים		
34. האם מותר להוריד מהרשת תוכנות חדשות		
35. האם מידע חיוני מגובה במקום מרוחק		
36. האם קיימות הגנות לתוכנות קריטיות		

חומרה	קיים	לא קיים
37. האם קיימות הוראות בכתב לגבי הבאת תוכנות מחוץ לארגון		
38. האם קיים נוהל להשמדת חומרה		
39.האם קיימת הוראה המחייבת שימוש במחשב רק למטרות המשרד		
40. האם קיים נוהל להכנסת ציוד חדש		
41. האם מתקיימות בדיקות ביטחוניות טרם רכישה של חומרה		
42. האם מודעים העובדים לאחריותם לציוד שברשותם		

תיעוד	קיים	לא קיים
43. האם הופץ מסמך מדיניות האבטחה לכל עובדים		
44. האם קיים מדריך אבטחה אצל העובדים		
45. האם המסמכים הנ״ל מעודכנים באופן שוטף		
46. האם קיימים נהלים המגדירים סמכות ואחריות במערכות המידע		
47. האם נשמרים מסמכי המערכת במקום בטוח		
מדיות מגנטיות ואופטיות		
48. האם מדיות נרשמות, והאם מוטבע עליהן מספר זיהוי		
49. האם מתבצעת בדיקה מתוכננת של מצאי מדיות		
50. האם קיימים נהלים לטיפול בחסרים		

חומרה	קיים	לא קיים
51. האם קיימים נהלים לאחסון מדיות		
52. האם קיימים נהלים להעברת מדיות		
53. האם קיימים נהלים להשמדת מדיות		
54. האם קיימים נהלים לטיפול במדיות פעילות		
זיהוי ואימות	**קיים**	**לא קיים**
55. האם קיימים נהלי הרשאות והאם קיים ביצוע עליהם		
56. האם קיימים נהלים לגבי סיסמאות וכרטיסים מגנטיים, חכמים, ביומטריים, וכו'		
57. האם מותקנת במערכת "התראות" מפני ניסיונות חדירה		
58. האם מונה אחראי להרשאות כניסה		
59. האם קיימת החלפה של סיסמאות כניסה לתוכנה		
60. האם קיים נוהל לחסימת משתמש, לאחר מספר ניסיונות כושלים של כניסה למערכת		
61. האם מתקיימת הצפנה של סיסמאות		
62. האם קיימים אמצעי זיהוי "חזקים"		
63. האם קיימים סיסמאות ופינים אישיים		
תקשורת		
64. האם קיים נוהל ותיעוד שינויים להגנת פורטים (PORTS)		
65. האם קיים נוהל להגנת ציוד הרשת המשרדית		
66. האם קיים נוהל להגנת תוכנת הרשת		
67. האם מופעלות תוכנות IDS		
68. האם קיים (FIREWALL) והאם קיים נוהל הפעלה		
69. האם קיים נוהל להצפנה		
70. האם קיים נוהל לשימוש בדואר אלקטרוני		
71 האם קיים נוהל להפעלת טל-נט		
תיעוד תנועות מערכת	**קיים**	**לא קיים**
72. האם הגיבוי מתבצע על פי נוהל ועל בסיס קבוע		
טיפול באירועים		
73. האם קיים נוהל לטיפול באירועים		
תכנון שרידות המערכת		
74. האם קיימת תוכנית שרידות והתאוששות לאחר אירוע DRP		

מקורות

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

השאלון פותח באגף הבכיר לביקורת המדינה וביקורת פנימית במשרד ראש הממשלה.

תוכנית הכשרה של אחראים על אבטחה וביקורת של המידע

נוהל מס׳ 11

להלן תוכנית הכשרה כמתבקש מן ההחלטה דלקמן, ולאחר שעברה אישור המועצה המייעצת לביקורת מערכות ממוחשבות ואבטחת מידע, המפקח הכללי במשרד ראש הממשלה, והממונה על ההדרכה בנציבות שירות המדינה.

החלטה 3582 (בק/77) מיום 02.04.1998 של הממשלה

א. המנהלים הכלליים של משרדי הממשלה יוודאו קיום תוכנית עבודה שנתית ואמצעים לאבטחה ולביקורת על המידע במשרדיהם, ובהתאם להוראות פרק 66 בתקשי״ר.

ב. במשרדים ימונה עובד לתפקיד ״אחראי על אבטחה וביקורת של המידע״. היקף המשרה ייקבע על-ידי נציבות שירות המדינה.

ג. האחראי על אבטחה וביקורת של המידע, יטמיע במשרדו שיטות, כלים ונהלים לשמירת הזמינות, השלמות, המהימנות, השרידות והסודיות של המידע.

ד. האחראים על אבטחה וביקורת של המידע יוכשרו ויופעלו על-פי תוכנית שתגובש בין נציבות שירות המדינה והאגף לביקורת המדינה במשרד ראש הממשלה.

ה. דו״ח על הביצוע יועבר לאגף לביקורת המדינה בתוך שלושה חודשים.

מטרות התוכנית

הכשרה מקיפה ויסודית בתחומי אבטחה וביקורת המידע בארגון, שתאפשר לבוגרים לתכנן את אסטרטגית הביקורת ואבטחת המידע; הקניית ידע בתחומים הדרושים לאבטחה וביקורת המידע, כגון: אבטחת מחשוב ומערכות הפעלה, חומרה, תקשורת, בסיסי נתונים, ניתוח מערכות, כלי אבטחה הקיימים בשוק וכד׳; לימוד אבטחה וביקורת המידע ברשתות הנפוצות תוך שילוב תרגול מעשי של הנושאים הנלמדים.

קהל היעד

מנהלי מערכות מידע ורשתות, מנהלי יחידות הביטחון, ממונים על אבטחת מידע, מבקרים, ובעלי תפקידים בתחום התקשוב בארגון.

היקף

התוכנית הינה בהיקף של **300** שעות לימוד, וכוללת **60** שעות פרוייקט מונחה.

תכנית הקורס

1. הקדמה ומבוא לאבטחת מערכות מידע בארגון – **15** ש׳
2. ניהול סיכונים – **20** ש׳
3. חקיקה ותקנות בתחום אבטחת מידע בישראל ובעולם – **5** ש׳
4. תקן 7799 לניהול אבטחת מידע – **5** ש׳
5. הגורם האנושי – המשתמש, סוגי משתמשים, יריבים ותוקפים, ״הנדסה חברתית״ (Social engineering and Fishing) – **10** ש׳
6. מיקור חוץ (outsourcing) והיבטי אבטחה – **4** ש׳

7. הדרכת עובדים, הגברת מחויבות, מודעות ואחריות המשתמשים – **4** ש׳
8. אבטחה פיזית – **4** ש׳
9. הזדהות, ניהול משתמשים ובקרת גישה – **16** ש׳
10. יישומים ביומטריים בשימוש הממשלה – **10** ש׳
11. תקשורת ורשתות נתונים – **8** ש׳
12. אבטחה והקשחה של מערכות הפעלה WINDOWS - **10** ש׳
13. אבטחה והקשחה של מערכת הפעלה Linux/Unix – **10** ש׳
14. ארכיטקטורה, מידור ופרוטוקולי תקשורת – **8** ש׳
15. אבטחת יישומים ומסדי נתונים SQL ו– ORACLE – **10** ש׳
16. התקני אחסון מרכזיים – **4** ש׳
17. אבטחת תחנות קצה – **4** ש׳
18. אבטחת דואר אלקטרוני וממשקי גישה לארגון – **4** ש׳
19. Web Services – בניית אתרים ואספקת שירותים דרך האינטרנט – **5** ש׳
20. טכנולוגיות ומוצרים באבטחת מידע **30** ש׳ : Authentication Mechanisms, Patch Management, IP Sec Basics, Firewalls, Intrusion Detection Systems, Intrusion Prevention Systems, Honey Pots, AntiVirus, FireWall ועוד.
21. מערכות ERP – **6** ש׳
22. שיקום מערכות המידע והמשכיות עסקית (DRP) – **8** ש׳
23. לוחמת מידע והגנה על תשתיות לאומיות – **10** ש׳
24. קביעת מדיניות אבטחת מידע בארגון ותכנית עבודה שנתית – **8** ש׳
25. מנהל אבטחת מידע – תפקידו ומיקומו בארגון (כולל סדנא לטיפול בהתנגדויות) – **12** ש׳
26. חקירת מחשב וחקירת רשת – **10** ש׳
27. היבטי אבטחת מידע במשרדי הממשלה (החלטות ממשלה, הגופים האחראים ואכיפה; היבטי אבטחת מידע בליווי פרוייקטים ובנוהל מפת״ח; הפקת לקחים מדוחות מבקר המדינה; היבטים ייחודיים במחשוב ממשלתי) – **40** ש׳
28. פרוייקט גמר – **60** ש׳

בקרת גישה למחשב המרכזי ולמחשבים האישיים

נוהל מס׳ 12

מבוא

נוהל זה מגדיר אחד משני מעגלי האבטחה הפיזית, שמטרתה לאבטח את יחידת המחשב המרכזי המעבדת מידע בסיווג "**חסוי** ".

יישום הנחיות בפרק זה יתנו מענה הולם לאבטחת מערכות מידע בסיווג "**חסוי**", וכן **מערכות מידע בלתי מסווג** שסווגו כבעלות **חיוניות ברמה בינונית.**

הערה: במקרה והמידע מסווג כ"חסוי", אך לחיוניותו וחיוניות מערכות המידע נקבעה רמת חיוניות אמצעית (או גבוהה), יידרש המשרד ליישם **מעגל אבטחה היקפית חיצונית.**

הגדרות

אבטחה פנימית – מכלול האמצעים אשר נועדו למדר בין מרכיבי מערכת יחידת המחשב המרכזי, לבין עובדי המשרד וזרים.

ההתייחסות בנוהל זה תהיה למרכיבי יחידת המחשב הבאים:
אולם ההפעלה,
ספריית מצעי המידע (מידיה) המגנטיים/אופטיים,
חדר תקשורת,
חדר ההקלדה,
חדר אמצעי קלט/פלט,
חדרי המכונות או מיזוג אוויר וכוח,
קווי התקשורת בתחום יחידת המחשב.

אזור ממודר של מערכות המידע והתקשורת – סביבת העבודה בה ממוקמים מחשבים ומשאבי מחשוב אחרים (כגון: ספריות, נתבים, שרתים, יחידות אל פסק ומיתוג ראשי למערכות הנ"ל, מרכזיות מחשבים וטלפוניה וכד'). כאמור, סביבה זו:

א) תהיה ממודרת בפני עובדי המשרד שאינם נמנים על בעלי התפקיד הנדרשים לשהות בתחום זה.

ב) בכלל זה נמנים, נוסף על מי שצוינו בסעיף א' לעיל, גם בעלי תפקיד אחרים, כגון: ספקים, יועצים, אנשי תמיכה טכנית, תחזוקה, ומוזמנים אחרים.

ג) נוכחותם ב"אזור הממודר" של הרשומים מעלה, תהיה מותנית בצירוף של שני התנאים הבאים יחדיו:

(1) מקום ומשך שהייתם אושרו מראש כנחוצים, על ידי אחד מאלה: מנהל מערכות מידע, מנהל תקשורת, הממונה על אבטחת מידע, הממונה על ביטחון, בעל תפקיד אחר שאושר ע"י הממונה על אבטחת מידע.

(2) כל מבקר נדרש להיות בעל אישור מהימנות ברמת "חסוי" לפחות.

מבנה יחידת מחשב - בניין/ים, חדר/ים המיועד להצבת כלים (טכנולוגיית המידע), של המשרד.

מטרות הנוהל

נוהל זה בא לפרט את כלל אמצעי האבטחה הפיזית בהם יש לנקוט באבטחה פנימית של יחידת מחשב מרכזית המעבדת, אוגרת או מפיקה מידע בסיווג "חסוי" ומעלה.

אחראי על ביצוע הנוהל

אחריות ניהולית: מנהל אגף מערכות מידע.

אחריות ביצוע: מנהל חדר מחשב.

גוף הנוהל

יחידת מחשב מרכזי במשרד המעבד מידע בסיווג "חסוי" תתוכנן ותיבנה על פי עקרון ההפרדה והמידור, הנדרשים בין מרכיבי המערכת השונים. המידור יבוצע באמצעות בניה או מחיצות אשר להן יש מעברים המבוקרים באמצעים: פיזיים, אלקטרוניים או אנושיים. קצין הביטחון יסייע בידי הממונה על אבטחת מידע באפיונים של האמצעים הנדרשים. החדר יהיה נעול בכל עת.

הימצאות בעלי תפקידים ביחידת המחשב המרכזי תהיה באזורים הנדרשים להם מתוקף תפקידם בלבד.

בעלי תפקיד ומוזמנים אחרים, שאינם עובדי המשרד, יהיו מלווים מרגע כניסתם לאזור הממודר של מערך המידע, בכל משך שהותם בו, עד צאתם מאזור זה!

שיטות ההוצאה או ההכנסה של אמצעי אחסון מידע במבנה יחידת המחשב המרכזי, ניודו בין מרכיבי יחידות המחשב השונים, יעוגנו בנהלים הפנימיים של המשרד.

חדרי מיזוג וכוח יהיו מופרדים לחלוטין מיחידת המחשב המרכזי. הגישה אליהם תהיה דרך פתחים נפרדים.
בכל האמצעים לבקרת גישה, יוחלפו הקודים אחת לשלושה חודשים לפחות, או לאחר עזיבת עובד את המשרד או את תפקידו, וזאת באחריות מעקב של הממונה על אבטחת מידע.
להגברת רמת הביטחון, מומלץ להתקין **אמצעי זיהוי ביומטרי** לבקרת הכניסה ליחידת המחשב המרכזי.

יש להציב שילוט תואם, במקומות בולטים מחוץ לחדר המחשב, כדי להאיר את תשומת ליבם של גורמים השוהים באזור חדר המחשב כי הכניסה והשהייה בחדר מותרת למורשים בלבד.

ביחידת מחשב מרכזית, תותקן ותופעל מערכת גילוי והתראה מרכזית. סדרי אבטחה, התקנת מערכות הגילוי וההתרעה והפעלתן, יתואמו עם מנהל אגף הביטחון. מערכת הגילוי תופעל בתום הפעילות במתקן המחשב. דרכי התגובה במקרה של גילוי פעילות חריגה תקבענה ע"י קצין הביטחון.
אזור המפעילים, בקרי תהיל"ה, שרתי המשרד ושרתי פרוייקט תהיל"ה יהיו ממודרים. תותר בו שהיה ונוכחות של עובדים בלבד. אורחים או עובדי משרד אחרים ישהו במקום רק בנוכחות עובד של היחידה.

<u>יחידת מחשב מרכזי תמוקם במבנה הבנוי מחומרים כדלהלן:</u>

א. קירות חיצוניים - עשויים להיבנות מחומרים אלה:

1. **לבנים** - עובי מינימלי **20** סנטימטר.
2. **בלוקים** - עובי מינימלי **20** סנטימטר.
3. **בטון יצוק** - עובי מינימלי **10** סנטימטר.
4. **קיר גבס** - לא יאושר כקיר חיצוני למבנה יחידת מחשב.
5. **קיר עץ** - לא ישמש כקיר חיצוני למבנה יחידת מחשב.

ב. קירות פנימיים* - עשויים להיבנות מחומרים אלה:
*** אין הכוונה כאן למחיצות בחלל הפנימי של חדר המחשב**

1. **לבנים** - עובי מינימלי **10** סנטימטר.
2. **בלוקים** - עובי מינימלי **10** סנטימטר.
3. **בטון יצוק** - עובי מינימלי **10** סנטימטר.
4. **קיר גבס** - קיר גבס פנימי יהיה בן שתי דפנות, כאשר ביניהן תוכנס רשת פלדה מגולוונת. עובי מינימלי של סריגי הרשת יהיה **5** מילימטר. הסריגים יעוגנו לרצפה, לתקרה ולכל דופן אפשרית.
5. **קיר עץ** - לא ישמש כקיר פנימי לחדר יחידת מחשב.

חדר יחידת המחשב המרכזי ייבנה ללא חלונות ויהיה בעל מספר מינימלי של כניסות ויציאות, הכרחיים בלבד.

ביחידת מחשב המרכזי הממוקמת כיום, מתוך אילוץ, בבניין בעל חלונות, יש **להתקין בחלונות סורגים.** הסורגים יהיו עשויים מפלדה מגולוונת, מרותכים בכל הצלבה, וסריגיהם בעלי חתך של **12 מילימטר,**

לפחות. הם יעוגנו בכל היקפם לתוך הקיר, בעומק של **10 סנטימטר**, לפחות. הרווח בין הסריגים לא יעל על **15 סנטימטר**.

א. יש להגדיר **כניסה ויציאה אחת בלבד**, לתנועת העובדים. כל שאר הפתחים ינעלו תמיד באופן שיאפשר מילוט בעת חירום.

ב. מנהל יחידת משק ומשאבים חומריים (בנא"מ) אחראי על תקינות דלתות או פתחים המיועדים למילוט.

גורם בוחן ומאשר
כל שינוי פיזי במבנה יחידת מחשב מרכזי יובא, טרם ביצועו, לעיון ואישור בכתב של הממונה על אבטחת המידע.

גורם מדווח
מנהל מערכות המידע (מנמ"ר) אחראי על דיווח ל"ממונה" אודות שינויים המתוכננים להתבצע במבנה יחידת המחשב המרכזי.

גישה לעמדות עבודה

עמדת עבודה – מסוף המחובר למחשב, מחשב אישי הפועל עצמאית, מחשב אישי המחובר לרשת תקשורת, מדפסת, פקסימיליה ושולחן עבודה.

כל חדר המכיל עמדת עבודה יהיה בכל עת מאויש או נעול. עמדות עבודה המכילות חומר "חסוי ביותר" יכללו לפחות אחד מן האמצעים הבאים:

1) מנגנון נעילה פיזית, בו יעשה שימוש בכל עת שהעמדה איננה מופעלת.
2) אבטחה בתוכנה (בקרת גישה).

מדפסות המפיקות חומר בסיווג "חסוי ביותר" תפעלנה בצורה שתמנע נגישות בלתי רצויה/מבוקרת לחדר וכן תמנע אפשרות לקחת החומר/לצלמו/לקרוא את המודפס בו. מסוף או מחשב יוצבו תמיד בזווית שלא תאפשר צפייה לגורמים הנכנסים לחדר/עוברים בסמוך. עמדת עבודה לא תושאר בלתי מאוישת. משתמש העוזב את עמדת העבודה יוודא נעילתה טרם עזיבתו. כאשר יש יותר ממשתמש אחד בעמדת עבודה, ההוראה חלה על כל אחד מהם בנפרד. כאשר מדפסת מחוברת ליותר ממחשב אחד האחריות האבטחתית לגבי המדפסת תיקבע מראש.

מקורות

נהלי מסגרת – אבטחת מידע רגיש ומערכות מידע. משרד ראש הממשלה, אגף בכיר לביקורת מדינה וביקורת פנימית, מאי 2000.

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

נוהלי אבטחת המידע בעיריית ירושלים ,פברואר 2001.

מידור, זיהוי והרשאות המשתמשים

נוהל מס׳ 13

מטרות הנוהל

זיהוי משתמשי המערכת המרכזית, כתנאי בסיסי למידור חלקי המערכת בין המשתמשים השונים.

אחראי לביצוע הנוהל

משתמשים: יקפידו על יישומן המלא של הנחיות נוהל זה המתייחסות אליהם.

הממונה על אבטחת מידע: יקבע ויפרסם את הפרמטרים לניהול מערכת הסיסמאות המחייבת את כלל משתמשי המשרד. יפקח, יבקר ויאכוף את היישום. קביעת הכללים תבוצע בנפרד, עבור כל מערכת מידע המנהלת מערכת סיסמאות אוטומטית.

מנהל צוות התמיכה: ינחה המשתמשים בהתאם להוראות המחייבות במשרד/במערכת מידע.

מנהלי המאגרים ומנהלי היישומים יישמו הנחיות נוהל זה, כל אחד בתחומו, כמפורט להלן.

גוף הנוהל

אבטחת הפעילות תתבסס על מנגנון האבטחה המובנה במערכת ההפעלה. יש להפעיל את מירב האופציות שהמנגנון מספק.

לכל משתמשי מערכות המידע יוקצו עם הצטרפותם למערכת, סיסמאות אישיות ורק על פיהן תתאפשר הגישה למערכת.

כל אחד ממשתמשי המערכת, ללא יוצא מן הכלל, יוגדר באופן אישי ותקבענה לו הרשאות הבלעדיות לו.

מנהלי המאגרים השונים יהיו אחראים לקביעת ההרשאות של העובדים הכפופים להם. יישום ההרשאות יבוצע בתאום בין מנהלי היישומים לממונים ישירים.

למען הסר כל ספק, מודגש כי הרשאה איננה רק אפשרות הגישה למערכת מסוימת, אלא גם הגדרה מדויקת של הפעילויות שרשאי המשתמש לבצע בכל יישום/מסך: אחזור ו/או עדכון ו/או תוספת ו/או מחיקה.

משתמש/תכניתן הפונה למערכת, יתבקש להזדהות. רק במקרה שהזיהוי עבר בצלחה, יקבל הפונה על המסך את רשימת המערכות/יישומים אליהם הוא רשאי לפנות. הרשימה לא תכלול יישומים אחרים.

זיהוי משתמש יהיה באמצעות שמו (USER ID). במקרה של בעיה בזיהוי המשתמש, תיחסם התקשורת ותוצג הודעה. רק המפעיל האחראי או מורשה אחר מטעמו, יוכלו לבצע שחרור החסימה, אחרי שבדקו את המקרה לגופו.

לא יתאפשר לעבור מיישום ליישום או מסביבת עבודה של פיתוח לסביבת עבודה של ייצור, אלא דרך התפריט הראשי ומערכת הסיסמאות.

פעילות תוכניתנים בסביבת ייצור תוגדר כפעילות חריגה על כל המשתמע מכך.

פעילותם השוטפת של התוכניתנים תתבצע אך ורק ממסופי התוכניתנים הנמצאים באזור יחידת המחשב. ייאסר עליהם להשתמש במסוף המפעילים או בכל מסוף אחר של משתמשים, למעט באירועים חריגים.

קבוצת אנשי הסיסטם תופרד מזו של תוכניתני היישומים בכל הנוגע לרמת ההרשאות יש להימנע מלהעניק לתוכניתני היישום הרשאות ברמה המותרת לאנשי הסיסטם או המפעילים.

באחריות מנהלי המאגרים לבדוק כל משתמש פעם בשנה, לצורך עדכון מפת ההרשאות הביצוע יהיה ביוזמת מנהלי יישומים ובתיאום עם הממונים הישירים.

מנהל היישום יוסיף או ינפה אנשים מן הרשימה רק בהתאם לפניה בכתב מטעם מנהל המאגר.

עזיבת עובד (כולל עובד המועסק ע"י חברת כוח אדם) או העברתו לתפקיד אחר, תועבר מיידית לידיעת מנהל היישום, וזה יבטל את הרשאות הגישה של העובד. אחריות הדיווח חלה על הממונה הישיר ו/או מנהל יחידת משאבי אנוש בארגון.

ככלל, לא תותר עבודה מול המחשב המרכזי בשעות חריגות, סופי שבוע, מועדים וחגי ישראל. במקרים חריגים תותר פעילות באישור מוקדם של מנהל היחידה למערכות מידע.

זיהוי בסיסמא

כל משתמש יוכל להגיע אך ורק אל מאגרים המותרים לו, תוך מזעור אפשרויות חשיפת סיסמאות האישיות. מעבר לזיהוי הפונה אל המערכת ע"י שמו, תתאפשר הפניה רק באמצעות סיסמא. הסיסמא תהווה את החוליה העיקרית בהגנה על הרשאות הגישה.

לכל משתמשי המחשב יוקצו, עם הצטרפותם למערכת, סיסמאות אישיות ורק על פיהן תתאפשר הגישה למחשב. את הסיסמאות לאנשי האגף לשירותי מידע יקצה מנהל הסיסטם. את סיסמאות הראשוניות יקצה מנהל הסיסטם על פי הדרישה של מנהל היישום הרלוונטי.

הסיסמא הראשונית תשמש לצורך כניסה ראשונית חד-פעמית למערכת. עם כניסתו הראשונה לחשבונו במערכת, על המשתמש להחליפה לפני כל פעולה אחרת. מכאן והלאה הסיסמא תוחלף ע"י המשתמש ובאחריותו.

הסיסמא לא תופיע על המסך בעת הקשתה.

חל איסור מוחלט למסור/לחשוף סיסמאות. אין לתלות את הסיסמאות על פתקיות בקרבת המחשב.

ככלל, תוחלפנה סיסמאות אחת לשלושה חודשים. המערכת תכפה את החלפת הסיסמא על המשתמש. המשתמש יקבל התראה על מסך המחשב על סיום תוקף הסיסמא לפחות 7 ימים טרם פקיעתה.

במקרה של הקלדת סיסמא שגויה, תחסם התקשורת ותוצג על כך הודעה במסך. המערכת תאפשר שלושה ניסיונות כניסה, לאחר מכן תחסם התקשורת לחלוטין. חידוש הגישה של המשתמש אל המערכת יתאפשר רק אחרי קיומו של בירור ובקשת חידוש באמצעות מנהל היישום. במקרה הצורך יועבר המקרה לידיעת הממונים הרלוונטיים.

אחת לרבעון תתבצע פעילות ביטול או הקפאת משתמשים שלא עשו שימוש במשאבי המחשוב, במשך תקופה שתוגדר בזמן הבדיקה. על יחידת כוח אדם להודיע מייד למנהל המחשוב על עזיבת כל עובד.

עם כניסת נוהל זה לתוקף, תבוצע החלפה יזומה של סיסמאות כל משתמשי המערכת, זאת על מנת להבטיח שלכל משתמשי המערכת הוותיקים קיימות סיסמאות העונות להנחיות נוהל זה.

כל חריגה מהוראות נוהל זה, תתאפשר אך ורק לאחר פניה מנומקת בכתב ואישור בחתימה של הממונה אבטחת מידע, ושל מנהל היחידה למערכות מידע. כל המסמכים הללו יתויקו וישמרו בתיק מיוחד אצל ממונה אבטחת מידע.

במקרה של חריגה על רקע של צורך תפעולי ביחידת המחשב עצמה, תהיה דרושה מערכת אישורים כנ"ל, למעט הצורך לקבלת אישורו של יו"ר הוועדה עליונה לאבטחת מידע.

<u>המשתמש יבחר סיסמא שתענה על הדרישות הבאות:</u>

1. ככלל, הסיסמא תהיה קשה לניחוש.
2. הסיסמא תהיה מורכבת משישה תווים (לכל הפחות) של אותיות, ספרות וסימנים.
3. תו זהה לא יופיע בסיסמא יותר מפעמיים.
4. לא יהיו יותר משלושה תווים עוקבים שיופיעו בסדר הרציף שלהם (א'-ב', ספרות, סדר המקשים במקלדת וכו').
5. אין להשתמש בסיסמא בעלת משמעות הקשורה באופן אישי למשתמש כגון: שם העובד, שם בן/בת זוג, מחלקתו, תאריכים בעלי משמעות וכדומה.
6. אין לעשות שימוש במקשים פונקציונליים לאחסנת סיסמאות והפעלתן.
7. אין לחזור על סיסמאות קודמות במשך 4 "הדורות" האחרונים.
8. אין להשתמש בסיסמא שהנה מילה המופיעה במילון, בכל שפה שהיא.

על מנת לאפשר תיקוני טעות בשלב קביעת הסיסמא, יש לאפשר הקלדה פעמיים.

חל איסור מוחלט על מסירת סיסמאות. משתמש מחשב יתודרך על שמירת הסיסמא האבטחתית ועל החובה שלא להעבירה לאחר. משתמש יתודרך להודיע מיידית על חשד של חשיפת סיסמתו.

עלה החשד לחשיפת הסיסמא, יש להודיע על כך לאחראי אבטחת מערכות מידע ו/או הממונה על אבטחת מידע. תיעשה פעולה מיידית להחליפה. תיעשה בדיקה אודות אפשרות לשימוש בלתי מורשה בסיסמא.

הרשאות גישה

ניהול שוטף של הרשאות במערכת המחשב בצורה מרכזית, תוך הפעלת שיקול דעת של מנהלי אגפים וכן אחראים למערכות ממוחשבות במשרד.

כדי לכלול עובד ברשימת המורשים להיכנס למערכת ולתת לו סיסמא, על נאמן אבטחת המידע להחתים את העובד על טופס "הצהרה והתחייבות שמירת סודיות", בו מתחייב העובד לא להעביר לאנשים בלתי מורשים מידע שיקבל, או שימציא בידיו במסגרת עבודתו.

מנהל מערכות מחשוב ירשום את המערכות שאליהם יהיה העובד מורשה לגשת, יפרט אם העובד מורשה לעדכן את הנתונים או רק להציגם ויאשר בחתימתו על גבי הטופס את מתן הסיסמא והרשות לכניסה למערכת לעובד.

כל משתמש או עובד מחשב יוגדר בטבלאות ההרשאה של המחשב. משתמשי יישומים שגם בהם קיימת טבלת הרשאה, יוגדרו בטבלאות השונות ביישום.

במערכות בהן מנהל המערכת הנו עובד המשרד, יעדכן הוא את הרשאות העובד על פי טופס ההצהרה על שמירת סודיות.

ממונה על אבטחת המידע יעדכן את טופס ההצהרה במערכת ההרשאות וישמור המסמך למעקב. כמו כן, הוא יהיה מוסמך להפעיל את שיקול דעתו אודות ההרשאה המתבקשת, ובתאום עם אחראי המערכת, תשונה ההרשאה.

ממונה על אבטחת המידע מוסמך לבטל הרשאות לעובדים שסיימו עבודתם, עברו מתפקיד לתפקיד וכן לבטל הרשאה לעובדים (בהתאם לנתונים המתעדכנים במערכות ההרשאות) או שימוש לרעה בהרשאות שניתנו להם.

מידי שישה חודשים תתבצע בדיקה של ההרשאות, ע״י אחראי אבטחת מערכות מידע ממוחשבות. תוך תאום עם הנוגעים בדבר, ישונו או יבוטלו הרשאות, בהתאם לצורך.

באחריות מנהלי היחידות להודיע על כל שינוי תפקיד, פרישה או כל שינוי אחר, המחייב עדכון הרשאות, בנוסף לשינויים המתעדכנים במערכת כוח האדם.

גישה למאגרים

לא ייגש עובד למידע שאין הוא מורשה לגשת אליו. עיון או שימוש במידע שלא על פי ההרשאה מהווה עבירה וינקטו כנגד העובד צעדים משמעתיים.

עובד שהורשה לגשת למאגרי מידע, חייב לשמור את סיסמתו בסוד ולא לאפשר לאדם אחר להשתמש בה. אם יתברר כי נעשה שימוש שלא כדין במידע תחת הסיסמא של עובד מסוים, ישא העובד עצמו באחריות לכך.

עובד שהורשה לגשת למאגרי מידע, חייב לנקוט בצעדים הדרושים כדי למנוע מאנשים אחרים גישה למחשב בעת שמוצג בו מידע. אין להשאיר מחשב פתוח ללא השגחת העובד המורשה.

ניהול הרשאות הגישה וניהול תחום ההצפנה לא ייעשו על ידי מי שאינם עובדי המשרד או מורשים מטעמו.

מקורות

מכון התקנים ישראלי, תקן 1495 : אבטחת מערכות מידע ממוחשבות, חלק 3.

נהלי מסגרת – אבטחת מידע רגיש ומערכות מידע. משרד ראש הממשלה, אגף בכיר לביקורת המדינה וביקורת פנימית, מאי 2000.

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

נוהלי אבטחת המידע בעיריית ירושלים ,פברואר 2001.

זיהוי ואימות משתמשים באמצעים ביומטריים

נוהל מס׳ 14 (בהכנה)

מטרות הנוהל

בנוהל זה שלא הושלם עדיין, יוצגו מהלכים עליהם החליטה הממשלה לקידום הזיהוי והאימות של המשתמשים בעזרת יישומים ביומטריים.

הגדרות

ביומטריה היא מה שאת/ה, ולא מה שמסמכים מצביעים עליך, או הסיסמא שאת/ה זוכר/ת. ומכאן ניתן להבין שהיכולת להגיע לאימות וזיהוי באמצעות הביומטריה היא גבוהה בהרבה מהיכולות האחרות והכמות המוגבלת של הזיכרון האנושי לזכור סיסמאות מיישומים, חומרות ותוכנות שאנחנו עובדים אתם. היכולות האחרות קלות לזיוף וניתנות להעתקה/העברה ושיטת הזיהוי והאימות הביומטרי נותנת פתרון הולם למגבלות אלו.

גוף הנוהל

א. החלטות הממשלה

יישומים ביומטריים בשירות המדינה
החלטת ממשלה מספר תמ/66 מיום 16.12.2002

מחליטים:

א. צוות בהשתתפות נציגי המשרד לביטחון הפנים - משטרת ישראל, שב״כ, משרד האוצר, משרד המשפטים, משרד הפנים, משרד הביטחון, צה״ל וראש האגף לביקורת המדינה במשרד ראש הממשלה (מרכז הצוות), יבחן את הצורך והאפשרות, תוך התייחסות לאיזון הנדרש בין התכלית לעקרונות אחרים כגון הגנת הפרטיות, לשימוש ביישומים ביומטריים בשירות המדינה, למניעת הונאות ולשיפור האבטחה במשרדי הממשלה ותאגידים ממשלתיים.

הצוות יעבוד בתיאום עם צוות החשב הכללי במשרד האוצר, האחראי על מערכת פיתוח ותחזוקה למחשוב הציבורי ולכרטיסים החכמים בממשלה.

ב. הצוות יבדוק את היישומים הביומטריים התקניים הקיימים, ויקבע כללים מנחים למשרדי הממשלה לאימוץ ישומים ביומטריים.

ג. הצוות יבחן כל יישום לגופו על ידי המשרד הנוגע בדבר ובהתחשב בצרכיו הייחודיים.

ד. אין בהחלטה זו כדי לעכב כל עבודה המתבצעת לקידום השימוש ביישומים ביומטריים במשרדי הממשלה, לרבות קבוצות העבודה הבינמשרדיות המקדמות את התכנית ליישום אפליקציות ביומטריות בנושא עובדים זרים, או ברשויות אכיפת החוק.

ה. הצוותים הבינמשרדיים העוסקים בקידום השימוש ביישומים ביומטריים במשרדי הממשלה, יעדכנו את הצוות הבינמשרדי, כאמור בסעיף א׳ לעיל, על ההתקדמות בעבודתם.

ו. הצוות הבינמשרדי לעניין השימוש ביישומים ביומטריים בשירות המדינה ידווח על מסקנותיו והמלצותיו מידי שישה חודשים לוועדת השרים לענייני תיאום, מינהל וביקורת המדינה.

יישומים ביומטריים בשירות המדינה

החלטת ממשלה בק/12 מיום 15.06.2003

מחליטים:

א. בהמשך להחלטה מס' 2858(תמ/66) מיום 2.1.2003, לרשום את דו"ח הביניים של הצוות הבין משרדי לעניין יישומים ביומטריים בשירות המדינה, כדלקמן:

1) בקרות ביומטריות בכניסות לישראל

יש מקום לשלב יישומים ביומטריים בתהליכי ביקורת הכניסה לישראל, במעברי הגבול: בים, ביבשה (כולל מעברים שטרם נפתחו) ובשדות התעופה. הצוות בוחן טכנולוגיות רלבנטיות לכל אחד מהמעברים.

2) א) מרכז מידע בנושאים ביומטריים

רפא"ל תקים במסגרתה מרכז מידע לטכנולוגיות, ליישומים ולתוצאות הבדיקה שלהם. מידע זה יועמד לרשות נציגי הממשלה.

ב) מרכז בחינה למוצרים ביומטריים

בהתאם לסטנדרטים רלבנטיים ממקורות חוץ, ישאף הצוות להכין תקנים ישראלים למוצרים ביומטריים. גורמי הממשלה יקיימו בדיקה, לגבי כל יישום שיש כוונה להשתמש בו, כדי לייעל את התהליך, למזער הוצאות, ולאפשר שיתוף מידע בין הגורמים.

הכוונה להגיע לרשימת מוצרים מאושרים, אשר גופים ממשלתיים יוכלו להשתמש בהם בעתיד, מבלי להזדקק לבדיקות משלהם.

3. אמצעים ביומטריים לזיהוי משתמשים במערכות ממוחשבות

נציג מלמ"ב במשרד הביטחון יכין בתוך חודש ימים נייר מטה שיפרט העקרונות לשימוש באמצעים ביומטריים, לבקרת כניסה למערכות ממוחשבות.

4) יישומים ביומטריים ב"תעודת הזהות החכמה"

יש לשלב ב"תעודת הזהות החכמה" המופקת בימים אלה, אמצעי זיהוי ביומטריים ולהקשיח את המעבד. ללא אמצעים ביומטריים, זיוף התעודה ושימוש בה לפעולות לא חוקיות, יהיו קלים. בנושא זה יש לדעת הצוות לקבל החלטת ממשלה.

5) מאגר תמונות ביומטריות בממשלה

משרד המשפטים (רשמת מאגרי מידע) יכין נוהל בין משרדי, שעניינו שימוש בצילומים דיגיטליים, הנעשים על ידי גורמים ממשלתיים והעמדת מאגרי התמונות לשימוש המשרדים.

התמונות שיצולמו בעתיד, יהיו באיכות שתאפשר שימוש ביומטרי.

ב. הצוות הבין משרדי יכין בתוך ששה חדשים הצעה מתואמת לגבי יישומים ביומטריים שיוטמעו בחלק מהמסמכים שבאחריות משרד הפנים במגמה להגביר את יכולת הזיהוי והאימות של נושאיהן.

ג. הממונה על התקציבים במשרד האוצר, ביחד עם מרכז הצוות הבינמשרדי, יגבשו מסגרת תפעולית להפעלת מספר פרויקטים מובילים בממשלה (PILOT). הפרויקטים יהיו בתחומים הבאים:

1) פרויקטים בתחום שיפור בקרת הכניסה לישראל ובמעברי קו התפר, לרבות הכללת אנשים מנועי כניסה לישראל.

2) פרויקטים לזיהוי עובדים זרים לישראל.

3) פרויקטים למניעת הונאות ולהגברת אפשרויות הזיהוי של מקבלי תשלומים מהמדינה.

4) פרויקטים בתחום בקרות כניסה למערכות ממוחשבות.

ד. מרכז הצוות הבינמשרדי ימסור דיווח לועדת השרים בתוך שלושה חודשים. הדיווח יכלול פירוט תכניות העבודה בתחומים השונים, לרבות יעדים, תקציבים ומקורות המימון ולוחות זמנים לביצוע.

יישומים ביומטריים בשרות המדינה –
תיקון החלטה מס. 444 (בק/12) מיום 3.7.2003

חלטה בק/47 מיום 26.01.2004

מ ח ל י ט י ם:

לתקן את החלטה מס. 444(בק/12) מיום 3.7.2003 כדלקמן:

א. במקום סעיף א.(2)א. שענינו מרכז מידע בנושאים ביומטריים, יבוא:

"מכון התקנים הישראלי (מת"י) יקים במסגרתו, מרכז מידע לטכנולוגיה ליישומים ביומטריים ולתוצאות הבדיקה שלהם. המידע יעמוד לרשות נציגי הממשלה, ללא תמורה".

ב. במקום סעיף א.2(ב) שענינו מרכז בחינה למוצרים ביומטריים - יבוא:

"בהתאם לתקנים רלבנטיים שנקבעו בעולם, יקבע הצוות ליישומים ולתוכנות ביומטריים, הפועל בהתאם להחלטה מס. 2858(בק/66) מיום 2.1.2003. אילו מהם יחולו, בשינויים המתבקשים, בישראל. מכון התקנים הישראלי יקיים בדיקות של מוצרים ותוכנות ובהתאם להחלטות הצוות, יפעל לאימוץ תקנים כחוק.

מוצרים ותוכנות שימצאו מתאימים, כאמור לעיל, יעמדו לרשות גורמי הממשלה, מבלי שיהיה צורך לקיים לגביהם בדיקות נוספות."

דיווח מעקב אחר מצב ביצוע החלטה מס. 444(בק/12)
מיום 3.7.2003 - יישומים ביומטריים בשירות המדינה

החלטה בק/48 מיום 26.01.2004

מחליטים:

א. ועדת השרים רושמת לפניה את דו"ח יו"ר הצוות ליישומים ביומטריים בממשלה מיום 6.1.2004 אשר הוגש ליו"ר ועדת השרים.

(הדו"ח נמצא במזכירות הממשלה).

ב. לעניין סעיף מידע במאגרים, ובמעברי "מרחב התפר" - ש.ב.כ ומלמ"ב במשרד הביטחון יכינו עד 31.3.2004 הנחיות למינהלת מרחב התפר בעניין הגנה על המידע.

ההנחיות יועברו לאגף לביקורת המדינה במשרד ראש הממשלה.

ב. יו"ר ועדת השרים מודה לצוות ליישומים ביומטריים בממשלה ולעומד בראשו, על דיווח הביניים שהוצג בפני הועדה ומודיע, כי ועדת השרים תתכנס לישיבה נוספת לקבלת דיווח נוסף ומעודכן, בהתאם לצורך."

תעודת זהות ומסמכי מסע עם מזהים ביומטריים

החלטה מספר בק/82 מיום ה באדר ב התשס"ה-16.3.2005

מחליטים:

בהמשך להחלטות מספר **2858(תמ/66)** מיום 2.1.2003 ומספר **444(תמ/12)** מיום 3.7.2003:-

א. תעודת זהות

1) משרד הפנים יכין עד 30.9.2005, תזכיר חוק, שיכלול את שינויי החקיקה הנדרשים להכללת מזהים ביומטריים ב"תעודת הזהות החכמה".

הכנת תזכיר החוק כאמור, לא תעכב את תהליך הטיפול בהנפקת תעודת הזהות החכמה.

2) המזהים הביומטריים שיקבעו על-ידי משרד הפנים, יהיו על-פי תקני I.S.O ותקנים מחייבים אחרים.

ב. דרכון ומסמכי מסע אחרים

1) משרד הפנים יכין עד 30.9.2005, תזכיר חוק, שיכלול את שינויי החקיקה הנדרשים להכללת מזהים ביומטריים בדרכונים ובמסמכי מסע אחרים.

2) מזהים אלה יותאמו לדרישות הממשל של ארה"ב והאיחוד האירופי, ויהיו בהתאם להנחיות הטכניות של I.C.A.O ולפי תקני I.S.O ו-N.I.S.T, בהתאם לעניין.

3) לוח הזמנים להנפקת הדרכון הישראלי, ייקבע בהתחשב בלוחות הזמנים המקבילים, שיקבעו בענין על-ידי הממשל בארה"ב ובאיחוד האירופי.

4) משרד הפנים ומשטרת ישראל, יתאימו את מערכות המחשוב של ביקורת הגבולות, לבדיקת אימות הזהות באמצעות המזהים הביומטריים.

5) משרד ראש הממשלה יהיה שותף לתהליך החקיקה, בכל הנוגע לנושא טביעות אצבע.

ג. הנתונים הביומטריים שיילקחו מאזרחי ישראל ותושביה בשלב הרישום למערכת, ישמרו במאגר מרכזי, ולא ייעשה בהם שימוש, אלא בהתאם להוראות שיקבעו בחוק.

ד. משרד הפנים, בשיתוף משטרת ישראל, יערכו ניסוי מבוקר להנפקת תעודות זהות ודרכונים, הכוללים מידע ביומטרי, במסגרת הניסוי שעורך החשב הכללי (פרויקט ממשל זמין) ובמימונו, בהנחלת בתי-המשפט או בפרויקט אחר, בהתאם לכללים שיקבעו על-ידי הצוות הבינמשרדי לעניין יישומים ביומטריים.

ה. הצוות הבינמשרדי לעניין יישומים ביומטריים, יעקוב אחר ביצוע החלטה זו, וידווח על-כך לוועדת השרים.

תשלום קצבאות זיקנה ושארים - מערכות מידע ובקרה

החלטה מספר בק/85 מיום ד בניסן התשס"ה-13.4.2005

מחליטים:

1. נוהל מימשקים של מערכות מידע

א. הוועדה הבינמשרדית המיוחדת לאיתור ולמניעת תשלומים חריגים או כפל תשלומים, המתבצעים באמצעות משרדי הממשלה והמוסד לביטוח לאומי, שמונתה ביום 13.3.2005 על-ידי החשב הכללי (להלן - הוועדה), תכין נוהל למימשקים בין מערכות המידע של המוסד לביטוח לאומי, משרד הפנים (מינהל האוכלוסין), משרד הביטחון, צה"ל ומשרד הרווחה (להלן המשרדים).

ב. הנוהל יבטיח שהמוסד לביטוח לאומי, והמשרדים שנציגיהם חברים בוועדה, יקבלו מידע חיוני לקביעת זכאות לקיצבאות, לשיעורן ולאימות הצהרות התובעים.

ג. הנוהל גם יבטיח שהמשרדים יוודאו שבסיסי הנתונים המשמשים אותם, יהיו זהים.

ד. נוהל המימשקים יוכן בהתאמה להוראות חוק הגנת הפרטיות - מאגרי מידע.

ה. נציגי המשרדים הנזכרים בסעיף א' לעיל, יצורפו לוועדה.

ו. הוועדה תמסור דו"ח על פעולותיה לוועדת השרים לענייני ביקורת המדינה, לא יאוחר מ-31.7.2005.

2. איתור זכאים

א. המוסד לביטוח לאומי יגיש לוועדת השרים תוכנית למימוש זכויות לקיצבאות שארים של אלמנות ויתומים, וכן דמי מחייה ותוספת קיצבת ילדים כשארים, המבוססת על תיאום עם קרנות הפנסיה הגדולות, מינהל הגימלאות במשרד האוצר ומעסיקים גדולים, וכן על מידע ממוחשב אודות התלמידים, שיעביר לו משרד החינוך התרבות והספורט.

ב. המוסד לביטוח לאומי יכין תוכנית ביניים לאיתור זכאים לקיצבאות זיקנה, שלא מימשו את זכאותם.

ג. דיווח בנושאים הנ"ל יימסר לועדת השרים עד 31.7.2005.

3. ב ק ר ה

א. המוסד לביטוח לאומי ידווח על התקדמות העבודה וההחלטות של שלושת הצוותים שלהלן, אשר מנכ"ל המוסד לביטוח לאומי הודיע על הקמתם.

להלן פירוט צוותי העבודה לשיפור הבקרה במוסד לביטוח לאומי, ותיאור פעולתם:

1. הצוות לשיפור הבקרה הכספית, בראשות חשב המוסד, שיגבש מערכות בקרה ממוחשבות ושיטות ל"בקרת עומק", אשר יסיים את עבודתו עד 31.12.2005.

2. צוות הבקרה לשיפור תהליכים באגפי הגימלאות, בראשות הסמנכ"ל לגימלאות, שיגבש שיטות בקרה ממוחשבות, ושיטות ל"בקרת עומק".

3. צוות בקרת תקינות, המשותף למינהל הגימלאות ולמינהל הכספים של המוסד, שיסיים את עבודתו עד 30.4.2005.

ב. המוסד לביטוח לאומי ידווח על התקדמות תכנון בקרת הכנסות אוטומטית, שאמור להסתיים לא יאוחר מ-31.3.2006.

ג. המוסד ידווח על חיבור מערכת התשלומים והחובות של תשלומי קיצבאות זיקנה ושארים, למערכת הכספים הכללית של המוסד. לפי דיווח מנכ"ל המוסד, תחובר המערכת במהלך מאי 2005, והיא תנוהל על-פי כללים חשבונאיים ודו"חות כספיים נכונים.

ד. דיווח מפורט לגבי סעיפים א'-ג' לעיל יועבר לועדת השרים עד 31.7.2005.

4. שימוש באמצעים ביומטריים

א. המוסד לביטוח לאומי ידווח עד 31.7.2005, על תוצאות הניסוי להפעלת טכנולוגיה ביומטרית לזיהוי על-פי טביעת אצבע, שמנכ"ל המוסד לביטוח לאומי הודיע על הפעלתו בסניף רמלה, בשיתוף העובדים, למשך שלושה חודשים, עד סוף יוני 2005. הדיווח יכלול את מסקנות המוסד בנוגע לשימוש בטכנולוגיה זאת, לבדיקת ביצוע תשלומי גימלאות כדין.

ב. המוסד לביטוח לאומי, בהתייעצות עם הצוות הבינמשרדי לענין יישומים ביומטריים, יכין תוכנית למניעת הונאות במוסד לביטוח הלאומי. התכנית תכלול לוח זמנים והצעה תקציבית ליישומה, ותתחשב בכללים המחייבים שנקבעו לגבי "תעודת הזהות החכמה".

המוסד ידווח על הכנת תוכנית זו לוועדת השרים עד 31.7.2005.

ביצוע ההחלטות הנ"ל יביא בחשבון את ממצאי ביקורת מבקר המדינה בדו"ח 55ב'.

ב. הנחייה לבחירת פתרון ביומטרי : אצבעות סרוקות ופנים

1. חפש פתרון שיכול לרשום 10 אצבעות במהלך אחד.
2. רצוי לאמץ פתרון ביומטרי שמאפשר מינושה ואימג'.
3. וודא כי הפתרון מאפשר לשמור תמונה מלאה של טביעות אצבע וליצור מינושה אם צריך.
4. וודא כי הפתרון הוא IDMS ויש בו גם התאמה לזהוי פנים על פי piv 2 .
5. אמץ מודל רב תכליתי של זיהוי ביומטרי כולל זיהוי פנים לאזורים בעלי סיווג בטחוני גבוה.
6. דרוש לבחון את השעורים של שגויים false non-match בבדיקה של אחד לאחד ואחד לרבים
7. וודא כי התמונה הינה בעלת איכות גבוהה כדי לאפשר זהוי ביומטרי טוב יותר.
8. וודא כי הפתרון שומר על ביומטריית הפנים בפורמט שיהיה קל לתוכנות זיהוי פנים לבצע בו סריקה

ג. עקרונות למימוש מערכות ביומטריות במשרדי ממשלה

המסמך נועד לספק קווים מנחים לפרויקטים ביומטריים ללא תלות בטכנולוגיה הנבחרת או בספק המערכת . ההנחיות המופיעות במסמך זה ייבחנו מעת לעת כדי להתאימן להתפתחויות בשוק אך כאמור הן תקפות ללא קשר למוצר כזה או אחר . חלק א' של המסמך כולל את ההנחיות עצמן וחלק ב' כולל הסברים להנחיות אלו.

חלק א'

1. עקרונות עבודה בתחום הטכנולוגי :

1.1. יש להימנע באופן גורף ממערכות ביומטריות הפועלות בשיטת ONE TO MANY ולהעדיף שיטה של ONE TO ONE . במקרים חריגים בהם אין אפשרות לממש זאת יינתן פתרון ייחודי של ONE TO MANY המשלב הנחיות אבטחה נוספות .

1.2. מערכות זיהוי ביומטריות המיועדות לצורכי אבטחה ובטחון נדרשות לכלול מנגנון אבטחה אמין נוסף (כגון כרטיס חכם) על מנת להבטיח את שרידות המערכת בפני ניסיונות זיוף ומרמה עתידיים .

1.3. יש להעדיף מנגנון ביומטרי המאפשר בדיקת רישום כפול במערכת על מנת למנוע מצב של אדם יחיד הרשום בזהויות רבות . במלים אחרות זהו בעצם חיפוש ONE TO MANY הנעשה על בסיס הנתונים . חיפוש זה לא חייב להיות באותה טכנולוגיה בה נעשה שימוש שוטף . יתכן מצב שבו השימוש השוטף נעשה בטכנולוגיה אחת והחיפוש של זהות כפולה בטכנולוגיה שונה . אין בדרישה זו סתירה לסעיף 1.1 כי מדובר בחיפוש שאין צורך לבצעו בזמן אמת ואין צורך באותה רמה של ביצועים . חיפוש כזה איננו אפשרי בכל טכנולוגיה ביומטרית ולכן ההנחיה היא <u>להעדיף</u> מערכות כאלה ולא <u>לחייב</u> זאת .

1.4. הנתונים המפורסמים ע״י היצרנים לא תמיד משקפים מצבים אמיתיים המתאימים למציאות אצל הלקוחות ולכן בעת אפיון מערכת ביומטרית אין להסתמך על נתוני היצרנים בלבד . יש לבצע בדיקה עצמאית משלימה (פיילוט) ולדרוש מהספק מסמכי בדיקה על ניסויים של גופים עצמאיים . ניסויים אלה צריכים להיות מתועדים ברמת פירוט גבוהה ויש לקבל את התוצאות שלהם רק אם נעשו בצורה תקפה מבחינה סטטיסטית ורלוונטית ליישום המפותח .

1.5. יש לחייב את ספקי המערכות לדבוק בתקינה שתפורסם מעת לעת ע״י הגורמים המוסמכים לכך ולפסול פתרונות קנייניים .

1.6. בעת בחירת הטכנולוגיה הביומטרית יש לוודא את איכות השילוב (אינטגרציה) בינה לבין מערכות תשתית קיימות כדי למזער את סיכוני הפיתוח ככל האפשר .

2. <u>עקרונות עבודה בתחום התפעולי</u> :

2.1. הזיהוי הביומטרי הינו אמצעי טכנולוגי אחד מיני רבים הנדרש לתת מענה לצורך ארגוני תוך השתלבות והתאמה לתהליכי עבודה , מערכות מידע , כ״א ואמצעים נוספים הקיימים בארגון .

2.2. תכנון מערכת ביומטרית מחייב התייחסות להיבטי תפעול ותחזוקה יחד עם התייחסות לרמת מפעילי המערכת ואוכלוסיית המשתמשים .

2.3. המערכות הביומטריות נדרשות להיות ״פתוחות״ לקליטת טכנולוגיות חדשות ושדרוג תפעולי ללא מגבלות של ספקים וחוזים עסקיים . בהיבט המעשי הנחיה זו מחייבת שמירה של נתונים גולמיים (כגון תמונת טביעת האצבע בנוסף לתבנית הביומטרית) , עמידות בתקינה רלוונטית ופסילה של פתרונות קנייניים של יצרן כזה או אחר . לעיתים יהיה צורך לשלב MIDDLEWARE או אמצעי אחר כדי להבטיח זאת .

2.4. יש לגבש תפיסה תפעולית מתאימה בשלבים מוקדמים ככל האפשר לגבי הזדהות ראשונית של משתמשי המערכת טרם רישומם במאגר הביומטרי . נוהל כזה נועד להבטיח את איכות המאגר הביומטרי .

2.5. יש להתייחס לנתונים ביומטריים כאל בסיס נתונים רגיש ולחייב כל מערכת להירשם כחוק אצל רשם מאגרי המידע שבמשרד המשפטים . הרישום צריך להיות בהתאם למקובל לגבי מאגרי מידע בתוספת הנתונים הבאים :

2.5.1. תאור המערכת

2.5.2. גודל בסיס הנתונים לאורך חיי המערכת

2.5.3. סוג הטכנולוגיות שנעשה בהן שימוש

2.5.4. יצרני המערכת ותת המערכת הביומטרית בפרט

2.5.5. תהליכים עיקריים במערכת בדגש על חיפוש ONE TO MANY המתבצע בה

2.6. רמת האמינות הטכנולוגית של המערכת הביומטרית הינה מרכיב קריטי בכל יישום ביומטרי ויש לזכור שנכון להיות מערכות ביומטריות רבות אינן בשלות לשימוש רחב היקף .

3. <u>מיפוי צרכים בתחום הזיהוי הביומטרי :</u>

כדי ליצור שפה אחידה בין משרדי הממשלה השונים בתחום הביומטרי וכדי לתת כלים אחידים בקביעת שיקולי התכנון ימופו הפרוייקטים הביומטריים לפי ארבעה קריטריונים עיקריים :

3.1. מיפוי עפ"י צורך תפעולי

בסעיף זה תסווג המערכת לאחת מחמש קטגוריות בהתאם לרשימה הבאה :

3.1.1. זיהוי ורישום במעברי גבול (פנימיים וחיצוניים).

3.1.2. בקרת כניסה למתקנים ואזורים ממודרים.

3.1.3. בקרת גישה למערכות מחשב.

3.1.4. זיהוי חד ערכי למשתמש לצורך קבלת שירות משרד ממשלתי.

3.1.5. זיהוי חד ערכי של אוכלוסייה המטופלת ע"י גורמי ביטחון ואבטחה.

3.2. מיפוי עפ"י רמות סיכון וסיווג אבטחתי

בסעיף זה תסווג המערכת לאחת מארבע קטגוריות בהתאם לרשימה הבאה:

3.2.1. מערכות ביומטריות לפעילות ברמת סיכון גבוהה - אלה יוגדרו כמערכות ביומטריות המחייבות מספר מעגלי אבטחה נוספים אשר ימנעו מיריב ברמה של מודיעין זר לתקוף את המערכת לצורך ביצוע פעילות עוינת או לצרוך פגיעה בתקינות המערכת . מדובר בתקיפה ע"י גופים בעלי יכולת טכנולוגית גבוהה ונכונות להשקיע מחקר , זמן וכסף בתקיפת המערכת .

3.2.2. מערכות ביומטריות מועדות לתקיפה - אלה יוגדרו כמערכות ביומטריות המחייבות מעגלי אבטחה נוספים אשר ימנעו ממשתמשי המערכת לתקוף אותה לצורכי זיוף , הונאה ופגיעה בשלמותה . בסיווג זה תיכללנה כל המערכות הנמצאות בסיכון מצד משתמשי המערכת כלומר מערכת שהאוכלוסייה העושה בה שימוש מועדת לנסות לפרוץ אותה בהיקפים גדולים . מדובר באוכלוסייה שאיננה בעלת יכולת טכנולוגית גבוהה אולם יש לה מניע חזק לתקיפת המערכת .

3.2.3. מערכות ביומטריות לפעילות ברמת סיכון רגילה - אלה יוגדרו כמערכות ביומטריות המחייבות מעגלי אבטחה נוספים (לפחות אחד) אשר ימנעו מגורמים פליליים לתקוף את המערכת לצורכי זיוף , הונאה ופגיעה בשלמות המערכת . במקרה זה מדובר על אוכלוסיית משתמשים שרובם המכריע לא ינסה לפרוץ את המערכת כלומר ניסיונות הפריצה הם מיעוט .

3.2.4. מערכות ביומטריות ללא רמת סיכון - אלה יוגדרו כמערכות ביומטריות היכולות לפעול באופן עצמאי ללא מעגלי אבטחה נוספים עקב העדר סיכון ונזק במקרה של

תקיפה ונפילת המערכת (יישום ביומטרי לצורכי נוחות תפעול) . במקרה זה יש לוודא שלא תהיה "סחיפה" לאורך הזמן לשימושים אחרים .

3.3. מיפוי עפ"י היקף וסוג האוכלוסייה המשתמשת

בסעיף זה תסווג המערכת לאחת משלוש קטגוריות בהתאם לרשימה הבאה :

3.3.1. מערכת "פתוחה" : מערכת ביומטרית רחבת היקף המשמשת אוכלוסייה גדולה ומגוונת (כדוגמת מעברי גבול) .

3.3.2. מערכת "סגורה" : מערכת ביומטרית מצומצמת בהיקפה המשמשת עובדי ארגון מוגדר לצרכים מוגדרים (כדוגמת בקרת כניסה למתקן או למחשב) .

3.3.3. מערכת ייעודית : מערכת ביומטרית מצומצמת בהיקפה המשמשת לצרכים ייעודיים ומבצעיים .

3.4. מיפוי על פי תדירות השימוש

תדירות השימוש יכולה להשפיע על בחירת הטכנולוגיה הביומטרית ועל מערכי ההדרכה וההטמעה . בסעיף זה תסווג המערכת לאחת משתי קטגוריות בהתאם לרשימה הבאה :

3.4.1. מערכת בשימוש תכוף : מערכת שניתן להניח שיפור ברמת השימוש לאורך הזמן , כלומר המשתמשים מאומנים יותר בשימוש בה ככל שעובר הזמן .

3.4.2. מערכת בשימוש נדיר : מערכת המחייבת בחירת טכנולוגיה ביומטרית ידידותית במיוחד .

יש להגדיר את הצרכים באופן מפורט ובהתאם לסיווגים השונים ורק לאחר מכן ניתן יהיה להתאים מערכת ביומטרית טובה ואמינה יותר ובהשקעה כלכלית נכונה .

חלק ב'

4. עקרונות עבודה בתחום הטכנולוגי – הסברים :

4.1. ס' 1.1- באופן בסיסי יש שני סוגים של מערכות ביומטריות . סוג אחד מבצע זיהוי , כלומר משווה את הדגימה הנלקחת מהאדם מול כל בסיס הנתונים (או חלקו) ומוצא את הרשומה שיש לה התאמה טובה ביותר לדגימה (ONE TO MANY) . במצב זה יתכן ונקבל יותר מתשובה אחת , כל אחת עם ציון התאמה אחר . הסוג השני לא מבצע זיהוי אלא אימות של זהות מוצהרת , כלומר משווה את הדגימה מהאדם לרשומה בודדת בבסיס הנתונים (ONE TO ONE) . במצב זה מתקבלת תשובה של כן/לא על בסיס סף השוואה מוגדר . יש פער ניכר בביצועי המערכות השונות וזהו הבסיס להנחיה שיש להימנע ככל האפשר ממערכות ביומטריות הפועלות בשיטת ONE TO MANY ולהעדיף שיטה של ONE TO ONE . הנחיה זו באה עקב רמת בשלות טכנולוגית נמוכה של מערכות ביומטריות רבות .

4.2. ס' 1.2 - הכללה של מנגנון אבטחה נוסף כגון כרטיס חכם תבטיח שהמערכת תמשיך להיות רלוונטית גם אם תתפרסם תקיפה כנגד המנגנון הביומטרי . פרסום פומבי של תקיפה כנגד הטכנולוגיה הביומטרית לא יחייב בניית מערכת חדשה והוצאה כלכלית כבדה . שימוש בכרטיס חכם מאפשר עדכון של מנגנון האבטחה ושל מודל האבטחה אם יש סימנים לפריצתו . במקרים מסוימים השימוש בכרטיס חכם מתחייב גם לצורך שמירת פרטיות כי אין צורך במאגר ביומטרי . מקרה אחר המחייב כרטיס חכם הוא בכל מצב בו תשתית המיחשוב והתקשורת איננה מאובטחת מספיק או שהיא חשופה לתקיפה .

4.3. ס' 1.3 - אחת הבעיות שמנגנון הזדהות נדרש להתמודד איתן היא רישום של אותו אדם במספר זהויות . חיפוש ONE TO MANY הנעשה על בסיס הנתונים יציף מצבים אלה

ויאפשר למנוע זיופים. אין צורך לבצע חיפוש כזה בזמן אמת ואין צורך לדרוש ממנו את אותם ביצועים שנדרשים מהמנגנון הביומטרי הרגיל . חיפוש כזה יגלה מספר מסויים של מועמדים שציון ההתאמה שלהם גבוה מספיק כדי להחשידם . מועמדים אלה צריכים להבחן ע״י גורמי אבטחה כדי לסנן התראות שווא ולוודא שאכן יש רישום שגוי במאגר. שימוש בחיפוש מעין זה יעזור גם לאתר שגיאות מפעיל ולא רק ניסיונות הונאה .

4.4. ס׳ 1.4 - למערכות ביומטריות יש מדדים לביצועים אותם ניתן להציג במגוון גדול של צורות . המדדים הראשיים המקובלים הם :

4.4.1. קבלה שגויה של אדם לא מורשה (FAR) FALSE ACCEPTANCE RATIO

4.4.2. דחייה שגויה של אדם מורשה (FRR) FALSE REJECTION RATIO

4.4.3. חוסר אפשרות הרשמה למאגר (FTA או FTE) FAIL TO ENROLL/ACQUIRE

המשמעות של שגיאת FAR היא פגיעה בביטחון והמשמעות של שתי השגיאות האחרות היא טיפול ידני בחריגים , כלומר פגיעה באיכות השרות . הנתונים המפורסמים ע״י היצרנים נועדו להציג את המערכת שלהם באור חיובי ויתכן פער בין דפי הנתונים למציאות בשטח . יש לקבל מהיצרנים את מירב הנתונים הטכניים על המוצר כולל תהליכי הבדיקה , גודל המדגם ועמידות המוצר כנגד ניסיונות תקיפה מוכרים של המערכת . יש לדרוש בדיקה של גופים עצמאיים ולא להתבסס על הבדיקה של היצרנים עצמם .
תהליך ה-pilot נועד יותר לבחון את תפעול המערכת ופחות את נתוני ה-FAR ו-FRR . נתונים אלה קשים לבדיקה (במיוחד FAR) והפיילוט נועד בעיקר להציף בעיות תפעול . FRR גבוה יכול להתברר במסגרת כזו .

4.5. ס׳ 1.5 - אין כיום תקינה רחבת היקף לתחום הביומטרי אולם יש לצפות להופעה של תקינה כזו במשך הזמן . יש מספר ניסיונות ליצור תקינה של תאימות בין יצרנים שונים של ציוד ביומטרי כגון התקינה שפורסמה ע״י ICAO . כמו בכל תחום אחר גם כאן יש להעדיף בצורה מוחלטת תקינה מסודרת על פני פתרונות קנייניים גם אם הם מוצלחים מבחינה טכנולוגית . זו איננה המלצה ייחודית לתחום הביומטרי אך היא תקפה כאן באותה מידה למרות שכיום התקינה עדיין בחיתוליה .

5. עקרונות עבודה בתחום התפעולי- הסבר

5.1. ס׳ 2.3 – שמירה של נתונים גולמיים צריכה להיבחן היטב – האם יש מימשק מתועד לכך , האם היצרן יכול להוכיח את קיום התכונה הזו , האם זה נעשה בעבר ועל ידי מי , האם היצרן מתחייב להעביר את המידע גם ליצרנים מתחרים וכו׳ .

5.2. ס׳ 2.4 - ההנחיה לגיבוש תפיסה תפעולית של הזדהות ראשונית נובעת מהסיבה שתיעוד או סיסמאות אינם קשורים בצורה חזקה לאדם כלשהו , לעומת המערכת הביומטרית שבה אין אפשרות להחליף ״מפתח״ ונתוני הזהות הביומטרית קשורים בצורה חזקה וחד-ערכית לאדם מסוים . כתוצאה מכך, אם יש טעות ברישום (כתוצאה משגיאה או כתוצאה מניסיון הונאה) הטעות מקובעת וקשה לאדם שנפגע מכך להוכיח אחרת .

5.3. ס׳ 2.5 – מאגר ביומטרי צריך לעמוד בכל הנדרש ממאגר מידע בהיבט המשפטי אך יש צורך גם לתעד מספר מאפיינים טכנולוגיים של המאגר כדי להבטיח את שמירתו והגנתו כנגד שימוש לרעה .

ד. צילום תמונת פנים – סטנדרטים לצילום

כללי

תמונות פנים (פורטרט) של אדם, משמשים מזה כמה עשורים כאמצעי לזיהוי \ הוכחת זהות אדם. תמונות אילו, הוכנסו לסטנדרטים שונים במרוצת השנים ("תמונת פספורט", Mugshot וכד'). כיום יכולות תמונות הפנים לשמש מגוון רחב של אפליקציות לזיהוי, ובעיקר זיהוי ביומטרי המשתמש בתמונת הפנים (טביעת פנים) לצורך זיהוי אדם .

בעת לקיחת תמונת הפנים, אנו ננסה להגדיר את אופן הצילום ושמירת התוצאות על מנת שנוכל להשתמש בתמונות אילו לצורך זיהוי ביומטרי באמצעות תמונת הפנים, בהינתן שאין כיום יצרן אחד או טכנולוגיה אחת שנבחרה לצורך ביצוע הזיהוי, ובהתחשב בעובדה כי קיימים כיום כמה יצרנים (Vendors) של טכנולוגיית זיהוי פנים, אנו ננסה להגדיר איכות צילום שתתאים לרוב הטכנולוגיות הקיימות על מנת שלא נהיה מוגבלים בבחירת ספק הטכנולוגיה בשלב מאוחר יותר.

ראוי לציין כי יש בעולם כמה ניסיונות להגיע לסטנדרט ביומטרי עולמי (NIST) אולם נכון לרגע זה אין סטנדרט שמחייב את היצרנים השונים.

עולם הזיהוי הביומטרי (זיהוי פנים) מבדיל בין שתי סוגי תמונות לביצוע הזיהוי :

1. צילום מלא – תמונת צבע מלאה ברזולוציה מספיקה הכולל את כל הפנים, כל השיער (במידת האפשר), כמו כן את הצוואר והכתפיים באותו צילום. צילום זה הינו הצילום אותו נאכסן במאגר מידע.
2. תמונה קנונית - תמונה הנגזרת מהתמונה המלאה, בשחור לבן או צבע, בעלת מאפיינים גיאומטריים מדויקים לביצוע זיהוי פנים ממוחשב, תמונה זו הינה חסכונית במקום אבל עדיין מאפשרת זיהוי פנים, תמונה זו בדחיסה מתאימה ניתנת לאחסנה על כרטיס חכם, או בכל מקום בו אנו צריכים "לחסוך" במקום אחסנה דיגיטאלי כלשהו .

היקף

מסמך זה יגדיר את הדרישות הספציפיות לצילום תמונת פנים, דחיסה, ושמירה על המידע.
אין במסמך זה כל התייחסות לשאלת האכסון על כרטיס חכם בהיבט של אכסון תמונה מול אכסון תבנית .

הגדרות

עומק צבע : מספר הביטים הנדרש להגדרת פיקסל, ומגדיר גם את גווני האפור שניתן להציב בכל פיקסל.
גווני אפור : תמונה בעלת רכיב 8 ביט (ידוע גם כתמונה שחור לבן)
JPEG : צורת דחיסת מידע פורסמה בשנת 1993 בתקן ISO 10918-1
JPEG 2000 : צורת דחיסת מידע פורסמה בשנת 2000 בתקן ISO 15444

תנאי צילום

צילום אובייקט :

1. הצילום יכיל תמונת פנים מלאה (כל הפנים)
2. זוויות הצידוד וההגבהה לא יעלו על +\- 5 מעלות לכל צד או למעלה ולמטה.
3. הבעת הפנים חייבת להיות טבעית , ללא חיוך, שני עיניים פתוחות, פה סגור.
4. הראש חייב להיות ממורכז במרכז התמונה כאשר האף נמצא באמצע התמונה.
5. במידה והשיער ארוך מאוד ניתן לא לכלול את כולו בתמונה.
6. גובה העיניים יהיה במרחק של כ 60-70% מהקצה התחתון של התמונה.
7. הראש המצולם יתפוש כ 80% מסל התמונה.
8. הכתפיים חייבות להיות בזוית ישרה למצלמה.
9. הפנים לא יהיו מכוסות , ויהיו גלויות וברורות למצלמה .

10. במידה והאובייקט מרכיב משקפיים בעלת מסגרת עבה מאוד או משקפיים גסות יש להנחות אותו להוריד את המשקפיים ולצלם בלי משקפיים בכלל .

רקע :

אחד הפעולות הראשונות בזיהוי פנים הינו גזירת הפנים משאר התמונה, לכן חשיבות הרקע המצולם דרמטית לביצועי הזיהוי .

1. חייב להיות ניגוד ברור בין הפנים לבין הרקע.
2. הרקע חייב להיות חלק ללא הפרעות (שולחן כסא וכד׳)
3. הצבע המועדף כצבע רקע הינו אפור .

תנאי תאורה :

1. אין להשתמש במקור אור בודד (כגון פלאש) , שימוש במקור אור בודד גורם ל״עיניים אדומות״.
2. קשתית העין חייבת להיות בהירה וגלויה .
3. יש להשתמש בלפחות שלושה מקורות תאורה מאוזנים בעוצמתם .
4. יש להימנע ככל הניתן מהסתרה או צל על ארובות העין, במידת האפשר יש להגביר את התאורה הצידית על מנת לא לקבל ״צל״ על הפנים ובמיוחד על ארובות העיניים.
5. האור חייב להיות ״מפוזר״ על הפנים ללא הבזקים.
6. תאורה מוחזרת (Reflector) הינה המומלצת ביותר .
7. רמת התאורה לא תפחת מ 500 LUX ולא תעלה על 1250 LUX .

רזולוציה :

1. הפוקוס חייב להתמקד בשתי העיניים צוואר ומצח, לפעמים זה יגרום לטשטוש הרקע, דבר זה אינו מפריע כלל. יש להתעלם ממנו.
2. בין שתי העיניים יהיו לא פחות מ 120 פיקסלים.
3. יש להשתמש ברזולוציה של לפחות 800X600 על מנת להשיג תאימות VGA מלאה.
4. לא מומלץ להשתמש ברזולוציה גבוהה מדי, דבר שיקטין את סך גודל הראש במסגרת .
5. מספר הביטים לא יפחת מרמה של 24 ביט RGB .

מקורות:

החלטות ממשלה.

תקנים של ארגון התעופה הבינלאומי.

החלטות הצוות הבינמשרדי – יישומים ביומטריים בממשלה.

בקרה ופיקוח לוגי

נוהל מס׳ 15

מטרות הנוהל

לפרט את הבקרות הלוגיות השונות במערכות ממוחשבות, ודרכי הפיקוח באמצעותן.
הקנית יכולת לעמוד על תופעות חריגות.

הגדרות

בקרה לוגית – ניטור שוטף ממוחשב אחר הפעילות במערכת הממוחשבת, תוך התמקדות באירועים חריגים או רגישים.

פיקוח לוגי - מעקב אחר פעילויות במחשב גם לאחר ביצוע הפעילות ובהשהיית זמן כלשהו.

אחראי לביצוע הנוהל

מנהל יחידת המחשב יוודא פעילותה התקינה של מערכת ה״לוגים״.

ממונה על אבטחת המידע יטפל באירועים חריגים המטופלים באמצעות מערכת ה״לוגים״.

גוף הנוהל

יוגדרו במערכת פעולות חריגות או רגישות, באחריות הממונה על אבטחת המידע, ובתאום עם כל נודעים בדבר. ההגדרה הנ״ל תכלול ניסיונות סרק לכניסה למערכת וכן ניסיונות לבצע פעולות בלתי מורשות אחרות.

במערכת יישמר LOG של כל הפעילויות באמצעות תוכנה ייעודית, לתקופה של שלושה חודשים אחרונים, לכל הפחות.

ממונה על אבטחת המידע יוכל לבחון דוחות המערכת בהתאם לצורך. ייבדקו ניסיונות כושלים להציב סיסמא, שמות משתמש לא פעילים שנעשה בהם שימוש וכדומה.

בעת הבדיקה האמורה תיבחן בין היתר גם הפעילות הקשורה בעובדים שנעדרו מן העבודה, אך שם המשתמש שלהם היה בשימוש.

בבדיקה תהיה גם התייחסות לשעות העבודה ולמספר הכניסות של כל עובד.

הגדרת הפעילויות החריגות תיבדק ותתעדכן לפחות פעם בשנה.

מנהל הרשת יבדוק וינתח את ה״לוגים״ באמצעות כלים ממוכנים פעם בשבוע ויעביר הממצאים החריגים באופן מיידי לממונה על אבטחת המידע ואל מנהל מערכות המידע.

ממונה על אבטחת המידע, בהתאם עם מנהל מערכות המידע, יערוך בירור מיידי ודחוף לגבי הממצאים החריגים שאותרו ויישם פעילויות נגזרות כנדרש.

ממצאים המעידים על פעילויות חריגות שבוצעו בכוונת תחילה על ידי העובדים/גורמי חוץ הפועלים במשרד, יועברו בדחיפות ובדיסקרטיות לגורמי ההנהלה ויובילו לטיפול משמעתי בהתאם.

מקורות

מכון התקנים הישראלי, תקן מס' 1495 : אבטחת מערכות מידע ממוחשבות.

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

נוהלי אבטחת המידע בעיריית ירושלים ,פברואר 2001.

קבלת מערכת מידע חדשה

נוהל מס׳ 16

מבוא

חשיבות רבה קיימת לבדיקת מערכות חדשות במשרד טרם הכנסתן לפעולה שוטפת. הקפדה על הכללים המפורטים בנוהל זה יבטיחו כי נעשו מירב הפעולות להבטחת רמת אבטחה נאותה במערכת החדשה.

מטרות הנוהל

להבטיח כי דרישות אבטחת המידע ממערכת חדשה ייושמו, יתועדו וייבחנו טרם קבלת המערכת ותחילת השימוש בה.

להבטיח תאימות של מערכות המידע במשרד לנוהלי האבטחה של המשרד טרם קבלתן.

להבטיח כי קבלת מערכות לשימוש במשרד יבוצע בצורה מסודרת על מנת למנוע כשלים ולצמצם את מידת ההפרעה לפעילות השוטפת.

הגדרות

קבלת מערכת – ההחלטה להטמיע ולהשתמש במערכת במשרד, לאחר בדיקתה ואישורה בהתאם לצורכי ודרישות המשרד.

גוף הנוהל

כל מערכות המידע החדשות (מערכות שנרכשו או פותחו) וכמו כן שדרוגים של מערכות קיימות ייבדקו ויאושרו על מנת לאשר פורמלית את שימושם במשרד.
קבלת המערכת תבוצע על פי תהליך כתוב לקבלת מערכת, אשר יפרט את הפעולות שיש לבצע, הדרישות מן המערכת והקריטריונים המדויקים לאישור או דחיית המערכת.
בעת רכש מערכת מידע חדשה, ניתן לבצע את תהליך קבלת המערכת לפני החלטה סופית על קניה והטמעת המערכת במשרד. לדוגמא, ניתן לבחון מערכות של כמה חברות בפיילוט על מנת להחליט איזו תאושר ותתקבל.
החוזה בין משרד וספקי המערכות יציין בבהירות כי על משרד לבחון את המערכות ויגדיר את המחויבות של הצדדים במקרה והמערכת תיכשל במבחני הקבלה.

תוכנית לקבלת מערכת
האחראי על בדיקת המערכת יכתוב תוכנית לקבלת המערכת .להלן נושאים בהם יש להתחשב במהלך כתיבת תוכנית לקבלת מערכת:
התוכנית תכלול את הדרישות הארגוניות והטכניות מן המערכת.
על הספק לתאר את אמצעי האבטחה שבמערכת כולל את מערך ההרשאות.
באם יש במערכת שימוש בזיהוי משתמש פנימי – על בסיס הנתונים של הסיסמאות להיות מוצפן.
גם למנהל המערכת לא תהיה יכולת צפייה בסיסמאות, אלא רק להחליפן בעת הצורך.
לפני תחילת הבדיקה, ממונה אבטחת המידע יקבל הסבר על המערכת ורק באישורו תחל הבדיקה.

על התוכנית לכלול רשימה של הגורמים המעורבים בשלבים השונים של תהליך קבלת המערכת, כולל גורמים פנימיים במשרד וכן גורמים חיצוניים (ספק המערכת וכו'). לכל גורם יפורט התפקיד והאחריות שלו במהלך התהליך.

היקף הטמעת המערכת לאחר קבלתה יוגדר בתוכנית (לדוגמא הטמעה הדרגתית של מודולים שונים, או מערכת שתוטמע בהדרגה בחלקים שונים של המשרד).

למטרת ביצוע בדיקות לקבלת המערכת, תותקן המערכת בסביבת בדיקה אשר דומה ככל האפשר למערכת המבצעית.

התוכנית תכלול הגדרה של המשאבים הנדרשים לתהליך קבלת המערכת וכן לתהליך התקנתה והטמעתה במשרד (במידה ואושרה). לגבי כל משאב יצוין איזה גורם אחראי לספקו וכן מתי. פרק ה"דרישות" יתייחס הן לסביבת הבדיקה והן לשלב ההטמעה.

על התוכנית להתייחס למשאבים הבאים:

כוח אדם.

חומרה נדרשת (לדוגמא: מחשבים , שרתים וכו').

תקשורת (רשתות , כבלים וכו').

מאגרי נתונים וכוננ אחסון.

תשתיות וציוד נוסף.

על התוכנית להתייחס לממשקים למערכות אחרות , במידה ויש צורך:

שינויים נדרשים במערכות המושפעות מהמערכת הנבדקת.

דרישות תקשורת לטובת קישור למערכות אחרות.

שינויים נדרשים בציוד סינון ובקרה (נתבים , FW וכו').

קביעת מערך ההרשאות למערכת אשר תכלול הרשאות להפעלתה לחוד ולנתונים לחוד.

בדיקה

שלב הבדיקה מכיל בדרך כלל שלושה סוגי בדיקות:

Unit Testing– בדיקה הכוללת אישור איכות של המערכת עצמה ותקינות עיבוד הנתונים הפנימי.

System Integration Testing – בדיקה הכוללת בחינה של יחסי הגומלין והממשקים של המערכת עם מערכות אחרות.

User Acceptance Tests – בדיקה ברמת המשתמש הבוחנת את המערכת בהתאם לתרחישים המוגדרים על ידי המשתמש – בהתאם לדרישות מן המערכת.

הבדיקות לקבלת המערכת יבוצעו בהתאם לדרישות מוגדרות. על הבדיקות בנושא אבטחת מידע לכסות את הנושאים הבאים:

במהלך Unit Testing

אפשרויות של ניהול משתמשים וסיסמאות.

מנגנוני בקרה ומעקב.

מנגנוני הרשאות ובקרת גישה.

מבחני קיבולת ועמידה בעומסים.

היבטי זמינות ועמידות נגד התקפות Denial of Service.

התאוששות מתקלות.

אפשרויות של מערכת גיבוי להמשכיות מתן השירות.

בדיקות חדירה ופריצה.

אבטחת קבצי המערכת וקוד המקור.

מנגנוני אימות נתונים (Input/Output Validation).

במהלך Integration Testing

השפעה על רמת האבטחה במערכות אחרות.

אינטגרציה עם מערכות אבטחה קיימות ומתוכננות (לדוגמא מערכות מרכזיות לניהול משתמשים וכו').

תאימות למערכות אחרות במשרד.

התאמה לסטנדרטים נפוצים.

במהלך User Acceptance Testing

התאמה לכל הדרישות והתרחישים.

קלות שימוש.

קלות ניהול.

תהליך הבדיקה יבוצע בסביבת בדיקה ייעודית.

מבחני האבטחה יבוצעו בשיתוף מנהל אבטחת מידע. יש למנות נציגים מתאימים לצורך כך.

קבלת המערכת

אין לאשר את המערכת לעבודה בסביבת הייצור ללא אישור כי כל המערכת עברה את כל מבחני אבטחת המידע ועונה על כל הדרישות בתחום זה.

כאשר המערכת החדשה משפיעה על מערכות אחרות במשרד, יש לקבל אישור מבעלי המערכות המושפעות טרם קבלת המערכת.

באחריות ועדת ההיגוי לאבטחת מידע במשרד לאשר קבלת מערכות מידע מרכזיות.

התקנה והתאמה של המערכת

תוכנה או חומרה נדרשת תותקן על הגורם המוסמך לכך באגף מערכות המידע.

נציגים של ספק מערכת, או המחלקה המפתחת יפקחו על ההתקנה בסביבת הייצור בליווי מנהל אבטחת מידע.

שמות משתמש וסיסמאות המסופקים עם המערכת כברירת מחדל יבוטלו. השימוש בשמות משתמש וסיסמאות אלו אינו מאובטח.

התוכנית לקבלת המערכת תפרט את המודולים והרכיבים של המערכת אשר יש להתקין וכן את ההתקנה ההדרגתית של רכיבים נוספים בעתיד.

יש להטמיע אמצעי בקרה מוגברים על פעולת המערכת בתקופה הראשונה של פעילותה.

מערכות ישנות, או גרסאות קודמות של המערכת יישמרו לתקופה של שנה לטובת ביצוע שחזור של המערכת, במקרה הצורך.

עדכון/שדרוג של המערכת הקיימת

בנוסף להנחיות לעיל, יש להתייחס להיבטים הבאים בעת עדכון/שדרוג של המערכת הקיימת:

1) מינוי אחראי/איש קשר אשר לו הסמכות הבלעדית להזמין עדכון/שדרוג של המערכת הקיימת.
2) קבלת פרטי העדכונים שיבוצעו ע"י בית התוכנה.
3) קבלת מידע על שינויים במודולים קיימים לאור העדכונים (פגיעה במערכת הרשאות וכו').
4) קבלת התחייבות ספק שאין שינויים אחרים.
5) בדיקה ואישור תגובת הספק לסעיפים 4-2 לעיל ע"י האחראי לעדכון/שדרוג.
6) כדי שאחראי המערכת הקיימת יוכל להתרשם ממהות השינויים, יש להתקין התוספת/העדכון בסביבת הבדיקה (test).
7) במקרה של שדרוג גרסה, יש לוודא כי שמות משתמש מערכת שננעלו בעבר לא נפתחו שוב בעקבות השדרוג.
8) הבאת העדכון לוועדת הרשאות לאישור הכנסת העדכון למערכת המבצעית ומספור העדכון במספר מזהה (למשל גרסה 4.01). רק עם אישור הוועדה – יש להתקין את התוספת במערכת המבצעית.
9) יש לקבוע רשימת אנשים אשר יעודכנו בדבר העדכונים/שדרוגים שבוצעו במערכת
10) יש לתעד את פרטי ההתקנה – מהות העדכון, אישור הוועדה וכד'. כל זה יתויק בתיק האישי של המערכת. התיק יישמר אצל איש הקשר/האחראי על עדכונים.

מקורות

נוהלי אבטחת מידע של רשות הדואר, דצמבר 2002.

הטמנות תוכנה / חומרה במערכות מידע ממוחשבות

נוהל מס' 17 (בהכנה)

הגדרות:

התקנה – הוספת תוכנה ו/או חומרה למערכת ע"פ רצון הבעלים/משתמש ולתועלתו.

הטמנה – הוספת תוכנה ו/או חומרה למערכת שלא ע"פ רצון הבעלים/משתמש, ללא ידיעתו ולתועלתו של גורם זר.

גוף הנוהל

בנוהל זה לא נקבעו עדיין האמצעים לזיהוי והסרה של הטמנות תוכנה / חומרה.

יעדי ההטמנה:

- חשיפת מידע
- שתילת מידע
- שיבוש מידע
- הפרעה זמנית לשירותי המידע
- הרס מידע
- שילוב של יותר ממטרה אחת.

מאפייני הטמנת תוכנה

- הטמנת תוכנה בתוך מערכת ההפעלה
- הטמנת תוכנה בתוך תוכנת מדף
- תוכנת הטמנה ייעודית (כגון: תוכנות PUSH באינטרנט)
- שקיפות מלאה מול משתמשים

מאפייני הטמנת חומרה

- הוספת רכיב בתוך כרטיס מוכלל קיים
- הוספת כרטיס מוכלל חדש
- הוספת מכשיר חדש במערכת
- החלפת רכיב/כרטיס/מכשיר קיים באחר

מאפיינים נוספים

1) הטמנה דוממת:
- ממתינה לאירוע פנימי במערכת
- ממתינה להפעלה חיצונית

2) הטמנה פעילה:
- לפי ערכים קבועים מראש
- לפי ערכים מוכתבים באופן דינמי מבחוץ

3) רכיב פולט
4) רכיב משדר (אודיו/וידאו)
5) רכיב צובר (על זיכרון עצמאי/דיסק)
6) רכיב משולב – צובר ומשדר

גורמים יוזמי ההטמנות:

- מדינות
- יצרני חומרה
- מפתחי תוכנה
- ספקי שירותי תמיכה טכנית
- מתחרים
- גופי טרור
- חוקרים פרטיים

מקורות:

הנוהל הוכן בסיוע מר אהוד אבנר.

אבטחת פעילות פיתוח ותחזוקה של מערכות מידע

נוהל מס׳ 18

מטרות הנוהל

הגדרה של שיטת אבטחת המידע בפיתוח מערכות מידע חדשות. הדבר כולל תשתית, יישומים של המשרד ויישומים שפותחו בידי משתמשים. למנוע אובדן נתוני-משתמשים במערכות יישומים, הסגלת (שינוי) נתונים אלה או שימוש בהם לרעה.

הגדרות

תכנון מערכות מחשוב – מכלול השלבים במחזור חיים של מערכות מידע עד לשלב הכתיבה.

המידע במערכת יסווג על פי הסיווגים הבאים:

1. בלתי מסווג
2. חסוי
3. חסוי ביותר

לפירוט הסיווגים ראה נוהל מתאים.

סביבת עבודת פיתוח – אזור ״לוגי״ או מחשב נפרד המשמשים למטרות פיתוח.

מסמכים ישימים:

א. נהלי הרשות להכוונת מידע ביטחוני בשב״כ – 1994
ב. נהלי היחידה לביקורת ואבטחת מידע רגיש במשרדי הממשלה – 2000
ג. נהלי אבטחת מידע של משרד האוצר
ד. נוהל מפת״ח, גרסה מעודכנת

אחראי לביצוע הנוהל

האחריות לקבלת אישור על פיתוח מערכות מידע חלה על מנהל הפרוייקט.
האחריות לביצוע הנוהל חלה על מנהל הפרוייקט – עובד המשרד.
האחריות הניהולית חלה על מנהלי יחידות המחשוב אשר באחריותם מתנהלים הפרוייקטים.
האחריות לפיקוח ובקרה מוטלת על אגף הביטחון במשרד.
האחריות לעדכון ושלמות נוהל זה חלה על ממונה אבטחת מידע במשרד.

גוף הנוהל

שילוב מרכיבי אבטחה בשלבי הייזום, איסוף הצרכים, האפיון הראשוני, האפיון המפורט, הכתיבה ומבחני הקבלה הנו הדרך היחידה להבטיח מערכת בעלת אמצעי אבטחה נאותים.

העדר שילוב אבטחה בכל שלבי פיתוח המערכת וניסיון לבנות אותה בשלבים מאוחרים יותר כרוך בעלויות גבוהות, בפתרונות לא מלאים ולעתים אף בחוסר יכולת לאתר פתרון כלשהו.

חל איסור לפתח מערכת ו/או לבצע שינויים ותיקונים בסביבת הייצור. כל פיתוח מערכת, תיקונים ושיפורים יתבצעו בסביבת פיתוח בלבד. שימוש בסביבת הייצור תתבצע רק בליווי גורם משרדי האחראי לאותה מערכת.

נוהל זה משלב בתוכו הנחיות רבות מהתקן הישראלי מס׳ 7799 – חלק 1, **ניהול אבטחת מידע: קובץ כללים לניהול אבטחת מידע**, ופרק 10 **פיתוח ותחזוקה של מערכות.**

ניתוח וניסוח של דרישות אבטחה

בניסוח דרישות המשרד למערכות חדשות, או לשיפור המערכות הקיימות, יפורטו דרישות הבקרה. הדרישות יביאו בחשבון את הבקרות האוטומטיות שיש לשלב במערכת, ואת הצורך בתמיכה בבקרות שאינן אוטומטיות. שיקולים דומים ייעשו כאשר מעריכים את חבילות התוכנה ליישומי המשרד. ההנהלה עשויה להחליט להשתמש במוצרים שנעשתה להם הערכה נפרדת ושאושרו בנפרד. דרישות האבטחה ואמצעי הבקרה ישקפו את הערך העסקי של הנכסים המעורבים, ואת הנזק העסקי הצפוי במקרה של כשל אבטחה או היעדר אבטחה. המסגרת להערכת דרישות אבטחה ולזיהוי בקרות שיענו לדרישות אלה, היא הערכת סיכונים וניהול סיכונים. (ראה נוהל מתאים).

אבטחה במערכות יישומים

תכנון מערכות היישומים, לרבות יישומים שנכתבו על ידי המשתמש, יכלול בקרות מתאימות ונתיבי ביקורת או יומן פעילויות. אמצעים אלה יכללו מתן תוקף לנתוני הקלט, העיבוד הפנימי ונתוני הפלט. ייתכן שיהיה צורך בבקרות נוספות למערכות המעבדות מידע רגיש, רב ערך או קריטי למשרד, או שיש להן השפעה על נכסים כאלה. בקרות כאלה ייקבעו על סמך דרישות אבטחה והערכת סיכונים.

מתן תוקף (validation) לנתוני קלט

לנתוני הקלט למערכות יישומים יינתן תוקף, כדי להבטיח שהם נכונים ונאותים. ייבדקו נתוני קלט של עסקאות, נתוני מצב (כגון שמות ומענים, שיעורי מס וכד') וטבלאות פרמטרים (כגון מחירי מכירה, שערי חליפין וכו'). יישקלו הבקרות שלהלן:

א. בדיקות כפולות או אחרות לקלט, כדי לגלות שגיאות אלה:
   1. ערכים החורגים מהתחום,
   2. תווים לא תקפים בשדות נתונים,
   3. נתונים חסרים או לא שלמים,
   4. חריגה כלפי מעלה או כלפי מטה מגבולי נפח הנתונים,
   5. נתוני בקרה לא מאושרים או לא עקביים

ב. סקירות תקופתיות של תוכן השדות העיקריים או של קבצי נתונים עיקריים,כדי לאשר את תקפותם וכלילותם (integrity).

ג. בחינת מסמכי קלט המודפסים על נייר כדי לגלות כל שינוי לא מורשה בנתוני הקלט (כל השינויים ב מסמכי קלט צריכים להיות מאושרים).

ד. נהלי תגובה לשגיאות מתן תוקף.

ה. נהלי בדיקה לסבירות נתוני הקלט.

ו. הגדרת אחריות של כל העובדים המעורבים בתהליך הכנסת הנתונים.

בקרת העיבוד הפנימי

אזורי סיכון
נתונים שהוכנסו נכון, עלולים להשחת על ידי שגיאות עיבוד או בגלל פעולות שיבוש מכוונת. כדי לגלות מקרי שיבוש כאלה, ישולבו במערכות בדיקות מתן תוקף. תכנון היישומים יבטיח שיושמו הגבלות שימזערו את הסיכון להתרחשות מקרים של כשל עיבוד, שיובילו לאובדן הכלילות (integrity). יישקלו נושאים כגון:

א. השימוש בפונקציות הוספה ומחיקה בתוכניות, ומיקומן של הפונקציות האלה, לעשיית שינויים בנתונים.

ב. הנהלים למניעת ריצה של תוכניות בסדר לא נכון או ריצה אחרי כשל או לפני עיבוד.

ג. השימוש בתוכניות הנכונות להתאוששות אחרי כשל, כדי להבטיח עיבוד נכון של נתונים.

בדיקות ובקרות

הבקרות הדרושות ייקבעו לפי אופי היישום ולפי ההשלכות העסקיות של השחתת נתונים. להלן דוגמות לבדיקות שניתן לשלב:

א. בקרות שיח או אצווה, כדי להתאים מאזנים של קבצי נתונים אחרי עדכוני עסקאות,
ב. בקרות יתרה, כדי להשוות יתרות פתיחה עם יתרות סגירה קודמות, כלומר:
   1. בקרות ריצה – לריצה (run to run controls),
   2. סיכומי עדכון קבצים (file update totals),
   3. בקרות תוכנית לתוכנית (program to program controls)

ג. מתן תוקף לנתונים שנוצרו על ידי המערכת
ד. בדיקות כלילות (integrity) של נתונים או תוכנות שנטענו מהמחשב המרכזי למחשבים מרוחקים או להפך
ה. סיכומי גיבוב (hash totals) של רשומות וקבצים
ו. בדיקות שיבטיחו שתוכניות היישומים רצות בזמנים הנכונים
ז. בדיקות שיבטיחו שתוכניות רצות בסדר הנכון ומסתיימות במקרה כשל, ושהמשך העיבוד מעוכב עד שהבעיה נפתרת.

אימות – זהות מסרים

אימות-זהות מסרים היא טכניקה המשמשת לגילוי שינויים לא מורשים בתוכנם של מסרים אלקטרוניים, או השחתתם. אפשר ליישם את הטכניקות על חומרה – התקן אימות-זהות מסרים פיזי, או על התוכנה – אלגוריתם לאימות-זהות מסרים. יישקל השימוש באימות-זהות מסרים ליישומים שקיימת לגביהם דרישת אבטחה להגן על כלילות התוכן של המסרים, כגון העברת כסף אלקטרוני או החלפת נתונים אלקטרוניים דומים. תיעשה הערכת סיכוני אבטחה כדי לקבוע אם דרוש אימות-זהות מסרים וכדי לזהות את דרך היישום הנאותה ביותר.
אימות-זהות מסרים אינו מיועד להגן על תוכנם של מסרים מחשיפה לא מורשית. אמצעי נאות היכול לשמש באימות-זהות מסרים הוא טכניקת הצפנה.

מתן תוקף לנתוני פלט

לנתוני פלט ממערכת יישום יינתן תוקף כדי להבטיח שעיבוד המידע המאוחסן הוא נכון ומתאים לנסיבות. מערכות בנויות בדרך כלל על ההנחה שאם נעשה מתן תוקף נאות, אזי האימות והבדיקה של הפלט יהיו תמיד נכונים. הדבר אינו תמיד כך. מתן –תוקף לפלט יכול לכלול:

א. מבדקי סבירות כדי לקבוע אם נתוני הפלט הגיוניים,
ב. התאמת בקרות ספירה,
ג. הספקת מידע מספיק למקראה או למערכת עיבוד כדי לקבוע את הדיוק (accuracy), השלמות, הדייק (precision), והסיווג של המידע,
ד. נהלים לתגובה על תוצאות בדיקת מתן התוקף,
ה. הגדרות האחריות של כל העובדים המעורבים בתהליך הפקת הפלט.

בקרות הצפנה

מטרה: להגן על החיסיון, המהימנות או הכלילות של המידע.
מערכות הצפנה וטכניקות הצפנה ישמשו להגנת מידע הנחשב מידע בסיכון, ושבקרות אחרות אינן מספקות לו הגנה הולמת.

מדיניות השימוש בבקרות הצפנה
ההחלטה אם הצפנה היא פתרון נאות, תהיה חלק מתהליך רחב יותר של הערכת סיכונים ובחירת בקרות. כדי לקבוע את רמת ההגנה שתינתן למידע, תיעשה הערכת סיכונים. אחר כך אפשר יהיה להשתמש בהערכה הזאת כדי לקבוע אם להשתמש בבקרת הצפנה, איזה סוג בקרה ייושם ולאילו מטרות ותהליכים של הארגון.
המשרד יפתח מדיניות לגבי השימוש שלו בבקרות הצפנה להגנת המידע שלו. מדיניות כזאת דרושה כדי להגדיל למקסימום את התועלת וכדי להקטין למינימום את הסיכונים הכרוכים בשימוש בטכניקות הצפנה אלה. בפיתוח המדיניות, יישקלו עניינים אלה:

א. גישת ההנהלה לשימוש בבקרות הצפנה במשרד כולו, לרבות העקרונות הכלליים שינחו את ההגנה על המידע,
ב. הגישה לניהול מפתחות, לרבות שיטת הטיפול בהתאוששות של מידע מוצפן במקרה של אובדן מפתחות, העמדתם בסיכון, או השחתתם,
ג. תפקידים ואחריות, כגון מי אחראי:
   1. ליישום המדיניות,
   2. לניהול מפתחות

ד. איך לקבוע את הרמה הנאותה של ההגנה המבוססת על הצפנה,
ה. התקנים שיאומצו כדי להשיג יישום אפקטיבי בכל המשרד (איזה פתרון ישמש לכל תהליך).

הצפנה

הצפנה היא טכניקה היכולה לשמש להגנת חיסיון של מידע. יש לשקול את השימוש בה להגנת מידע רגיש או קריטי.
על סמך הערכת סיכונים, מזהים את רמת ההגנה הדרושה, תוך התחשבות בסוג ובאיכות של אלגוריתם ה הצפנה המשמש, ובאורך מפתחות ההצפנה שישמשו. כשמיישמים את מדיניות ה הצפנה של המשרד, יבוא בחשבון דרישות החוק הרלבנטיות וההגבלות הלאומיות העשויות לחול על טכניקות ההצפנה, בחלקי העולם השונים, וכל הקשור בזרימת מידע מוצפן החוצה גבולות של מדינות. נוסף על כך יובאו בחשבון הבקרות המופעלות על יבוא יצוא של טכנולוגיות הצפנה.
לזיהוי רמת ההגנה הנאותה, רצוי להיוועץ במומחה, שיבחר מוצרים מתאימים שיספקו את ההגנה הרצויה ויבטיחו יישום של מערכת מאובטחת של ניהול מפתחות. נוסף על כך, ייתכן שיהיה צורך בייעוץ משפטי באשר לחוקים ולתקנות העשויים לחול על השימוש שהארגון מתכוון לעשות בהצפנה.

חתימה ספרתית

חתימות ספרתיות (דיגיטלית) מספקות אמצעי להגנת האותנטיות והכלילות של מסמכים אלקטרוניים. למשל, אפשר להשתמש בהן בסחר אלקטרוני כאשר יש צורך לאמת מי חתם על מסמך אלקטרוני, ולבדוק אם התוכן של המסמך שונה לאחר החתימה.
ניתן להשתמש בחתימה ספרתית בכל צורה של מסמך המעובד באופן אלקטרוני, כגון לחתימה על תשלום אלקטרוני, על העברת כספים, על חוזים והסכמים. אפשר ליישם חתימות ספרתיות באמצעות טכניקת הצפנה המתבססת על זוג מפתחות שהיחס ביניהם חד ערכי, שאחד מהם משמש ליצירת חתימה (המפתח הפרטי), והאחר משמש לבדיקת החתימה (המפתח הציבורי).
יש להקפיד להגן על החיסיון של המפתח הפרטי. סודיותו תישמר, מפני שכל מי שיכול לגשת אליו, יכול לחתום על מסמכים, וכך לזייף למעשה את חתימתו של בעל המפתח. נוסף על כך חשוב להגן על כלילות של המפתח הציבורי. הגנה זאת ניתן להשיג על ידי השימוש באישור (התעדת) מפתח ציבורי (ראה בהמשך).
יש לשקול מה סוג אלגוריתם החתימה שישמש, ומה איכותו, ומה אורך המפתחות. מפתחות הצפנה משמשים לחתימות ספרתיות צריכים להיות שונים מהמפתחות המשמשים להצפנה. כשמשתמשים בחתימות ספרתיות, יובאו בחשבון כל התקנות הרלבנטיות המתארות את התנאים שבהם חתימה ספרתית מחייבת על פי דין. למשל, במקרה של סחר אלקטרוני, חשוב לדעת את מעמדן החוקי של חתימות ספרתיות. ייתכן שהשימוש החתימה אלקטרונית יצריך תמיכה של חוזה או הסכם המפרט את היות החתימה האלקטרונית מחייבת, אם מסגרת החוק אינה מספקת. רצוי לקבל ייעוץ משפטי באשר לחוקים ולתקנות העשויים לחול על השימוש שהארגון מתכוון לעשות בחתימות ספרתיות.

שירותי אי-הכחשה

שירותי אי-הכחשה (no-repudiation services) ישמשו כאשר עשוי להיות צורך ליישב מחלוקות באשר להתרחשות או אי-התרחשות של אירוע או פעולה, כגון מחלוקת לגבי השימוש בחתימה ספרתית על חוזה אלקטרוני או על תשלום אלקטרוני. שירותים אלה יכולים לספק ראיות שיוכיחו אם אירוע מסוים התרחש או אם פעולה מסוימת נעשתה. אפשר למשל להכחיש באמצעותם, משלוח הוראות עם חתימה ספרתית בדואר אלקטרוני. שירותים אלה מבוססים על שימוש בטכניקת הצפנה וחתימה אלקטרונית.

ניהול מפתחות

הגנת מפתחות הצפנה
ניהול מפתחות הצפנה הוא חיוני לשימוש אפקטיבי בטכניקות הצפנה. כל העמדה בסכנה או אובדן של המפתחות עלול להוביל לסיכון חיסיון, אותנטיות או/וגם כלילות של מידע. תהיה מערכת ניהול שתתמוך בשימוש של המשרד בשני סוגים של טכניקות הצפנה, שהן:

א. טכניקות מפתחות סודיים, כאשר שני צדדים או יותר, חולקים ביניהם את אותו מפתח והוא משמש הן להצפנה והן לפענוח של מידע. מפתח זה צריך להישמר בסודיות מאחר שכל מי שיכול לגשת אליו, יכול לפענח את כל המידע שהוצפן באמצעותו, או להכניס מידע אל מאושר.

ב. טכניקות מפתחות ציבוריים, כאשר לכל משתמש יש זוג מפתחות: מפתח ציבורי (שמותר לגלות אותו לכל אחד) ומפתח פרטי (שיש לשמור בסודיות). טכניקות של מפתחות ציבוריים יכולות לשמש להצפנה וליצירת חתימות ספרתיות.

כל המפתחות יוגנו מפני הסגלה והרס, ומפתחות סודיים ופרטיים צריכים הגנה מפני חשיפה לא מורשית. למטרה זאת יכולות לשמש גם טכניקות הצפנה. תהיה הגנה פיזית לציוד המשמש ליצירת מפתחות, לאחסונם ולגניזתם.

תקנים, נהלים ושיטות
מערכת ניהול מפתחות תתבסס על קבוצה מוסכמת של תקנים, נהלים ושיטות אבטחה, כדי:

א. לחולל מפתחות לשיטות הצפנה שונות וליישומים שונים,
ב. לחולל ולקבל אישורים מפתחות ציבוריים,
ג. להפיץ מפתחות למשתמשים מיועדים , לרבות המידע איך להפעיל אותם עם קבלתם,
ד. לאחסן מפתחות, לרבות המידע איך משתמשים מורשים יקבלו גישה למפתחות
ה. לשנות או לעדכן מפתחות, לרבות כללים הקובעים מתי יש להחליף מפתחות ואיך הדבר ייעשה,
ו. לטפל במפתחות שהועמדו בסכנה,
ז. לבטל מפתחות, לרבות המידע איך לסלק או לשתק מפתחות, כגון כאשר הם הועמדו בסכמה או כאשר משתמש עוזב את הארגון (במקרה כזה יש לגנוז גם את המפתחות),
ח. לאושש מפתחות שאבדו או הושחתו כחלק מניהול המשכיות של העסק, כגון לאישוש מידע מוצפן,
ט. לגנוז מפתחות, כגון עבור מידע שנגנז או שנעשה לו גיבוי,
י. להשמיד מפתחות
יא. לרשום ביומן ולערוך מבדקים לפעילויות הקשורות בניהול מפתחות.

כדי להקטין את ההסתברות של העמדת מפתחות בסכנה, יהיו להם תאריכים מוגדרים של הפעלה וביטול, כך שניתן יהיה להשתמש בהם רק לתקופה מוגבלת. תקופה זו תהיה תלויה בנסיבות השימוש בבקרת ההצפנה ובסיכון המשוער.
ייתכן שיהיה צורך לשקול קביעת נהלים לטיפול בדרישות לגישה למפתחות ההצפנה, הנובעות מהחוק. למשל, ייתכן שיהיה צורך לפענח מידע מוצפן כדי להציגו שראיה במשפט.
נוסף על עניין הניהול של מפתחות פרטיים וסודיים, יש לשקול גם הגנת מפתחות ציבוריים. אדם יכול לזייף חתימות ספרתיות על ידי החלפת מפתח ציבורי של משתמש, במפתח שלו. המענה לבעיה הזאת הוא שימוש באישור (התעדת) מפתחות ציבוריים. האישורים (התעדות) יופקו באופן הקשור קשר חד-ערכי בין מידע המתייחס לבעל זוג המפתחות הפרטי/ציבורי, לבין המפתח הציבורי. לכן חשוב שתהליך הניהול המחולל את האישורים האלה, יהיה אמין. תהליך זה מתבצע בדרך כלל על ידי רשות התעדה, שרצוי שיהיה ארגון מוכר הפועל לפי נהלים ואמצעי בקרה מתאימים, כדי לספק את רמת הנאמנות הדרושה.
תוכנם של הסכמים או חוזים ברמת השירות, עם ספקים חיצוניים של שירותי הצפנה, כגון עם רשות התעדה, יכסה את נושאי החבות, אמינות השירותים וזמני תגובה להספקת השירות.

אבטחת קבצי מערכת

מטרה: להבטיח שפרויקטים של טכנולוגיות מידע (IT) ופעילויות תומכות ינוהלו באופן בטוח. הגישה לקובצי המערכת תהיה מבוקרת. האחריות לקיים את כלילות המערכת תוטל על היחידה לניהול המשתמשים או על קבוצת הפיתוח שמערכת היישום או תוכנת היישום שייכת לה.

בקרת תוכנה תפעולית
תהיה בקרה של יישום תוכנה במערכות תפעוליות. כדי למזער את הסיכון של השחתת מערכות תפעוליות, יישקלו הבקרות שלהלן:

א. עדכון הספריות של התוכנית התפעולית ייעשה רק על ידי אדם שמונה על ידי ההנהלה והוסמך לנהל ספריות.
ב. אם אפשר, תוכניות תפעוליות יכללו רק קודים בציעים (executable).
ג. קוד בציע לא יופעל במערכת תפעולית אלא לאחר שעמד בבדיקה בהצלחה והתקבל על ידי יחידת ניהול משתמשים, ואחרי שעודכנו הספריות של תוכניות המקור.
ד. ייעשה רישום ביומן לצורך מבדק, לכל העדכונים שנעשו בספריות של התוכניות התפעוליות.
ה. גרסאות קודמות של התוכנה יישמרו כאמצעי למקרה חירום.

תוכנה שנרכשה מספק והמשמשת במערכות תפעוליות, תתוחזק ברמה הנתמכת על ידי הספק. כל החלטה לשדרג לפי גרסה חדשה, תביא בחשבון את האבטחה של הגרסה החדשה, כלומר דרישות אבטחה חדשות או מספר בעיות האבטחה המשפיעות על הגרסה הזאת, וחומרתן. טלאים (patches) ייעשו בתוכנה רק אם הם יכולים לסייע לסלק או להפחית את מספר נקודות התורפה באבטחה.
גישה פיזית או לוגית תינתן רק לספקים, למטרות תמיכה, לפי הצורך, ובאישור ההנהלה. פעילויות הספק ינוטרו.

הגנת נתוני הבדיקה של המערכת
נתוני בדיקה יוגנו ויבוקרו. בדיקות מערכת ובדיקות קבלה דורשות בדרך כלל נפח נתונים גדול שהוא קרוב ככל שניתן לנתונים התפעוליים. יש להימנע מהשימוש במסדי הנתונים של המערכת התפעולית המכילים מידע אישי. אם משתמשים במידע כזה, יש לטשטש את אפשרויות הזיהוי האישי לפני השימוש. להגנת הנתונים התפעוליים, אם הם משמשים למטרות בדיקה, יופעלו הבקרות שלהלן:

א. נהלי בקרת הגישה, המתייחסים למערכות יישום תפעוליות, יתייחסו גם למערכות יישום בדיקות,
ב. יהיה אישור נפרד בכל פעם שמעתיקים מידע תפעולי למערכת יישום בדיקה,
ג. מידע תפעולי יימחק ממערכת יישום הבדיקה מיד עם השלמת הבדיקה,
ד. ההעתקה והשימוש במידע תפעולי יירשמו ביומן כדי לספק נתיב ביקורת.

בקרת גישה לספריית תוכניות מקור
כדי להקטין את האפשרות להשחתת תוכניות מחשב, תקוים בקרה קפדנית על הגישה לספריות של תוכניות מקור, כמפורט להלן:

א. אם אפשר, ספריות תוכניות המקור לא יוחזקו במערכות תפעוליות,
ב. לכל יישום ימונה אחראי על הספריות,
ג. צוות התמיכה של טכנולוגיית המידע לא יקבל גישה חופשית לספריות תוכניות מקור,
ד. תוכניות שבפיתוח או תחזוקה, לא יוחזקו בספריות של תוכניות המקור,
ה. עדכון ספריות של תוכניות המקור והנפקת תוכניות מקור לתוכניתנים, ייעשו רק על ידי הממונה על הספרייה ועל פי אישור של מנהל התמיכה בטכנולוגיית המידע ליישום מסוים,
ו. דוחות התוכניות יישמרו בסביבה בטוחה,
ז. יתוחזק רישום ביומן של כל הגישות שנעשו לספריות תוכניות המקור,
ח. גרסאות ישנות של תוכניות מקור יגנזו, והתאריכים והזמנים שבהם הן היו פעילות, יהיו מצוינים בבירור, יחד עם כל התוכנה התומכת, בקרת העבודות, הגדרות הנתונים והנהלים,
ט. תחזוקה והעתקה של ספריות תוכניות המקור, תיעשה רק תחת נהלים קפדניים של בקרת שינויים.

אבטחה בתהליכי פיתוח ותמיכה

מטרה: לקיים את האבטחה של התוכנה והמידע של מערכת היישום.

סביבות פרויקטים ותמיכה יהיו נתונים תחת בקרה קפדנית. מנהלים האחראים למערכות יישומים, יהיו אחראים גם על אבטחת הפרויקט או סביבת התמיכה. הם יבטיחו שכל השינויים המוצעים למערכת נסקרו, כדי לוודא שאין הם מסכנים את האבטחה של המערכת או של סביבת התפעול.

נהלי בקרת שינויים

כדי להפחית למינימום מקרים של השחתת מערכות מידע, תופעל בקרה קפדנית על ביצוע שינויים. יאכפו נהלים רשמיים לבקרת שינויים. הם יבטיחו שנוהלי אבטחה ובקרה לא יועמדו בסכנה, שתוכניתני התמיכה יקבלו גישה רק לחלקי המערכת שהם צריכים לגשת אליהם לצורך ביצוע עבודתם, ושהתקבלו אישור רשמי והסכמה רשמית לכל שינוי. שינוי תוכנת יישום יכולה להשפיע על הסביבה התפעולית. נוהלי בקרת שינויים תפעוליים ויישומים ישולבו ככל שהדבר מעשי. התהליך יכלול:

א. קיום של רשומה ובה רמות הרשאה מוסכמות,
ב. וידוא שהשינויים הוצעו על ידי משתמשים מורשים,
ג. סקירת בקרות ונוהלי כלילות כדי להבטיח שהם לא יועמדו בסכנה על ידי השינויים,
ד. זיהוי כל תוכנת המחשב, המידע, ישויות מסד הנתונים והחומרה, הדורשים תיקון,
ה. קבלת אישור רשמי להצעות מפורטות, לפני תחילת העבודה,
ו. וידוא שהמשתמש המורשה קיבל את השינויים לפני כל יישום,
ז. וידוא שהיישום מתבצע באופן שימזער הפרעות לארגון,
ח. וידוא שתיעוד המערכת מעודכן עם השלמתו של כל שינוי ושהתיעוד הישן נגנז או מסולק,
ט. תחזוקת בקרת גרסאות לכל עדכוני התוכנה,
י. תחזוקת נתיב ביקורת של כל הבקשות לשינוי,
יא. וידוא שתיעוד התפעול ונוהלי המשתמש שונו לפי הצורך כדי להיות נאותים,
יב. וידוא שיישום השינויים ייעשה בזמן הנכון ולא יפריע לתהליכי העסק הקשורים בו.

ארגונים רבים מקיימים סביבה שבה המשתמשים בודקים תוכנה חדשה, והסביבה נפרדת מסביבת הפיתוח ומסביבת הייצור. הדבר מאפשר בקרה על תוכנות חדשות ומאפשר קיומה של הגנה נוספת למידע תפעולי המשמש למטרות בדיקה.

סקירה טכנית של שינויים במערכת ההפעלה

את מערכת ההפעלה צריך **לשנות תקופתית**, למשל כדי להתקין גרסה חדשה של תוכנה או טלאים. כשמתרחשים שינויים, יש לסקור את מערכות היישומים ולבדוק כדי לוודא שאין לכך השפעות שליליות על ההפעלה או על האבטחה. התהליך יכלול:

א. סקירה של נוהלי הבקרה והכלילות של היישום כדי לוודא שהם לא הועמדו בסכנה על ידי השינויים במערכת ההפעלה.
ב. וידוא שתוכנית התמיכה השנתית והתקציב כוללים את הסקירות ואת בדיקות המערכת הנדרשות עקב השינויים במערכת ההפעלה.
ג. וידוא שנשלחה הודעה בזמן, על דבר השינויים במערכת ההפעלה, כדי לאפשר עריכת סקירה לפני יישום השינויים.
ד. וידוא שנעשים שינויים נאותים לתוכניות הרציפות הארגונית.

הגבלת שינויים לחבילות תוכנה

לא רצוי לבצע שינויים (הסגלות) בחבילות תוכנה. בחבילות תוכנה קנויות רצוי להשתמש בלי לשנותן, ככל שניתן, וככל שהדבר מעשי. כאשר נראה שיש צורך חיוני בשינוי חבילת תוכנה, יישקלו עניינים אלה:

א. הסיכון שבקרות ותהליכי כלילות מובנים, יועמדו בסכנה.
ב. השאלה האם יש לקבל את הסכמת הספק.
ג. האפשרות לקבל את השינויים הדרושים מהספק, כעדכון תוכנה תקני.
ד. ההשלכות הנובעות מכך שהארגון הופך להיות האחראי להמשך התחזוקה, עקב השינויים שהוכנסו.

אם נראה שהשינויים חיוניים, תישמר התוכנה המקורית, והשינויים ייעשו על עותק שיזוהה בבירור. כל השינויים ייבדקו בדיקה מלאה ויתועדו, כך שניתן יהיה ליישם אותם שוב על שדרוגי התוכנה בעתיד.

ערוצים חשאיים וקודים טרויאניים
ערוץ חשאי יכול לחשוף מידע באמצעים לא ישירים ונסתרים. אפשר להפעיל אותו על ידי שינוי פרמטר נגיש הן על ידי אלמנט מאובטח והן על ידי אלמנט לא מאובטח של מערכת מחשוב, או על ידי השכנת מידע בתוך זרם נתונים. קוד טרויאני מיועד להשפיע על המערכת באופן שאינו מאושר ואינו ניתן להבחנה בקלות, ושאינו נדרש על ידי הנמען או המשתמש של התוכנית. ערוצים חשאיים ו קודים טרויאניים מתרחשים רק לעתים רחוקות במקרה. אם יש חשש להתרחשותם, יישקלו אפשרויות אלה:

א. רכישת תוכנות רק ממקור בעל מוניטין,
ב. קניית תוכנות בקוד מקור, כך שניתן לאמתו,
ג. שימוש במוצרים מוערכים (evaluated),
ד. בחינה של קוד המקור כולו לפני הכנסתו לשימוש תפעולי,
ה. אחרי התקנתו של הקוד – בקרת גישה אליו ובקרת השינויים הנעשים בו,
ו. לעבודה של מערכות עיקריות – העסקת צוותים שנאמנותם הוכחה.

פיתוח תוכנה על ידי קבלני שירות
אם מוציאים את פיתוח התוכנה אל מחוץ למשרד (קבלנות שירות), יישקלו עניינים אלה:

א. סידורי רישוי, הבעלות על הקוד, וזכויות קניין רוחני,
ב. אישור האיכות והדיוק של העבודה המתבצעת.

מנהל היחידה המזמינה את הפרוייקט (כל פרוייקט), יציג את הפרוייקט, לאחר אישור מסמך הייזום ולפני התחלת שלב האפיון, בפני אגף הביטחון וממונה אבטחת מידע שיקבע את סיווג המערכת, האמצעים הנדרשים לאבטחת המערכת, הן בתחום החומרה, התוכנה והאבטחה הפיזית הנדרשת.
ממונה אבטחת המידע במשרד יקבע את הרשאות לשימוש במערכת.

במידה והוחלט לסווג את המערכת מרמת "חסוי" ומעלה, יחתמו כל גורמי הפיתוח, במידה והם עובדי חברה חיצונית, על טופס לשמירת סודיות.

גורמי הפיתוח יעברו במידת הצורך הדרכה ייעודית לאבטחת מידע.

לפרוייקט ימונה נאמן אבטחת מידע, שיהיה אחד ממנהלי הפרוייקט, שידווח בסיום כל שלב ממחזור החיים של הפרויקט על הפעולות שנעשו בתחום אבטחת המידע בפרוייקט עפ"י הנחיות הממונה. לקראת שלב הרצת הניסוי (pilot), יערכו מבחני קבלה אבטחתיים וביקורת של הממונה ורק לאחר אישורו תעבור המערכת לסטטוס של עבודה בשגרה.

במסגרת האפיון ייכתבו נהלים ייעודיים למערכת ולמשתמשים, וזאת בהנחיית ממונה אבטחת מידע.

לגבי מערכות שסיווגן "סודי ביותר", יש לפנות לנוהל מיוחד בנושא המצוי במשרד האוצר.

היבטים טכניים של אבטחת המידע

איסור שינוי לא מבוקר - חל איסור על ביצוע שינוי בנתונים, בתוכנה יישומית, בתוכנה, בתשתית ובחומרה, אלא אם הדבר נעשה באופן מאובטח ומבוקר בהתאם להנחיות מפורשות של ממונה אבטחת מידע.

שיוניים טכנולוגיים – כל שינוי במפרטים הטכניים או הטכנולוגיים של המערכות, אשר עשוי לשנות את מצב אבטחת המידע.

מקורות

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

נוהלי אבטחת המידע בעיריית ירושלים, פברואר 2001.

מכון התקנים הישראלי, תקן 7799: ניהול אבטחת מידע.

נוהלי עבודה – אגף לשירותי מידע ומחשוב, משרד הבריאות, פברואר 2000.

נוהלי אבטחת מידע של רשות הדואר, דצמבר 2002.

טיפול במסמכי קלט/פלט

נוהל מס׳ 19

מטרות הנוהל

צמצום הסיכון אשר בחשיפת מידע מסווג המצוי במסמכי קלט/פלט, באמצעות טיפול אבטחתי הולם.

אחראי לביצוע הנוהל

ממונה אבטחת מידע ינחיל, יטמיע ויאכוף יישום הנחיות נוהל זה.
עובדי המשרד, בעלי המידע או המשתמשים בו, יוודאו טיפול אבטחתי נאות, כמוגדר בנוהל זה.

גוף הנוהל

לכל פלט המופק במחשב יקבע סיווג על פי סיווג המאגר. הסיווג יקבע על פי כללי סיווג מאגרים (ראה נוהל מס׳ **2-** ״מיפוי וסיווג של מידע רגיש ומערכי מידע״).
במקרים מיוחדים ניתן להקל ברמת סיווג פלט באישור מנהל המאגר, או באישור מנהל היחידה המפיקה את הפלט.

הסיווג יופיע בראש הדף. הסיווג יבוצע לפי המפתח הבא: ״**בלתי מסווג**״, ״**חסוי**״, ״**חסוי ביותר**״.
יש לרשום את סיווגו של מידע בסיווג ״חסוי״, ״חסוי ביותר״ בלבד. אין צורך לרשום את סיווגו של מידע ״בלתי מסווג״.
במסמכים המסווגים ״חסוי ביותר״ יופיע הכיתוב ״מכיל מידע מוגן לפי חוק הגנת הפרטיות – המוסר שלא כדין עובר עבירה״.

כל עותקי דו״ח מחשב המכילים חומר ״חסוי ביותר״ ימוספרו ויצוין מספר העמודים בכל עותק.
פעולה זו תיעשה באופן ידני והמספור יופיע בדף הראשון ובדף האחרון של כל עותק.

גורם המפיץ מסמכים בסיווג ״חסוי ביותר״, ינהל רישום מדויק בו מפורטים נמעני המסמכים, כותרותיהם, תאריכי ההפצה, שם המפיץ, מספרו של העותק ומספר העמודים בו.
הרישום ייעשה ביומן מיוחד לכך. הרישום ישמר למשך שנתיים לפחות.

כל טיוטא או תדפיס יופקו, יטופלו ויועברו רק ע״י גורמים שהוסמכו לכך. חומר זה יימצא רק ברשותם, בחדריהם או באתרי פעילותם.
עובד שהוסמך לקבל דו״ח מחשב מסווג, ישתמש בדו״ח לצורכי העבודה ולא ימסור אותו לעובד אחר במשרד, אלא אם אישר מנהל היחידה בו הוא עובד את המסירה.

לגורמים חיצוניים מוסמכים יועבר חומר כתוב במעטפות סגורות.
מסירת מידע לגופים ואנשים מחוץ למשרד, תיעשה לפי הנוהל מס׳ **19** – ״העברת מידע והוצאתו״.

חומר מסווג (״חסוי״ או ״חסוי ביותר״), אשר איננו בשימוש, יימצא תמיד בארונות נעולים. חומר בלתי מסווג אשר איננו בשימוש, ימצא תמיד בחדר נעול.

חומר עודף או לקוי, יפונה לביעור באחריות אחראי לניהול הרשומות במשרד. פלט שפג תוקפו, יפונה לביעור באחריות המשתמש בו.
גריסת חומר וגניזתו (שוטף או תקופתי) תבוצענה בהתאם להוראות חוק הארכיונים ולהנחיות האחראי לניהול רשומות. (ראה נוהל מס׳ **22** – ביעור רשומות).

על מדפסות שתפקנה חומר מסווג (״חסוי״, ״חסוי ביותר״), יחולו עליהן כללי המידור וההגנה שנקבעו למסופים לחומר בסיווג זה.

חומר המסווג כ״חסוי ביותר״ יופץ כשהוא ארוז ומצורפת אליו תעודת משלוח למעקב ההפצה.
התהליך יכלול החזרת אישור לשולח.

מסמכי קלט (מסמכי מקור שנועדו להקלדה), יסווגו ויטופלו כמפורט בהנחיות המתייחסות לפלט.

מקורות

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

נוהלי אבטחת המידע בעיריית ירושלים, פברואר 2001.

חוק ההגנה על הפרטיות התשמ"א – 1981 ותקנותיו.

ניהול ואבטחה של אמצעי אחסון מגנטיים ואופטיים

נוהל מס׳ 20

מטרות הנוהל

אמצעי אחסון מגנטיים ו/או אופטיים והאפשרות לשחזר מתוכם מידע בקלות יחסית, עלולים להוות מפגעי אבטחה החמורים, אלא אם כן, ננקוט אודותם באמצעי אבטחה נאותים.

מניעת חשיפת חומר חסוי המאוחסן במצעים מגנטיים ו/או אופטיים.

אחראי לביצוע הנוהל

ממונה אבטחת מידע ינחה, יטמיע ויבקר יישום הנחיות נוהל זה.
מנהל חדר מחשב יישא באחריות ביצוע הנחיות נוהל זה, בסיוע מנהלי היחידות מהן משונעים מצעים מגנטיים ו/או אופטיים אל ו/או מחוץ למשרד.

גוף הנוהל

מצעים המגיעים למשרד מגורם חיצוני, יבדקו כדי לוודא שאינם מכילים רכיבי תוכנה הרסניים כגון וירוסים.

השימוש במצעי האחסון המגנטיים יהי רק ע״י משתמשים מורשים.

הקצאת מצע נושא מידע לשימוש חוזר, מחייבת מחיקת המצע במלואו. יש להקפיד על קיום מלא ומדייק של הנחיה זו.

כעקרון, מצעים נושאי מידע, יועברו בין הגורמים שונים בתוך מארז קשיח המיועד להעברת מצעים מגנטיים. דיסקטים ניתן להעביר בתוך מעטפה קשיחה המיועדת למטרה זו.

המצעים יועברו ישירות, ללא שהיות בדרך. אין להשאיר מצעים ברכב, ללא סידורי שמירה נאותים. אין להשאיר מצעים נושאי מידע ברכב חונה (בייחוד בלילה ליד בתי עובדים).

מצע שנתקבל מגורם חוץ, אין להעביר אותו לגורם חוץ אחר, אלא אם כן סוכם הדבר מראש, והמצע עבר תהליך מחיקה מלא.

בעת ניוד מחשבים, החלפתם או השבתתם – יש למחוק את קבצי המידע הקיימים בדיסק. ביצוע המחיקה יהיה ע״י טכנאי מוסמך. במידת הצורך, לפני מחיקת המידע יש לבצע גיבוי למידע החיוני. תהליך זה יתבצע גם הוא, ע״י טכנאי מוסמך.

מצעים מגנטיים/אופטיים נתיקים (סרטים, קלטות, דיסקטים וכו׳), המכילים חומר מסווג (״חסוי״ או ״חסוי ביותר״), יהיו מאוחסנים תמיד בארון מתכת עם מנעול תליה או בחדר נעול במנעול צילינדר, לכל הפחות.

ככלל, ימצאו אמצעי האחסון מגנטיים ו/או אופטיים נעולים בטמפרטורה רגילה של חדר העבודה מבלי שיהיו חשופים ישירות לקרני שמש, ללחות או לרטיבות. כל זה לפי הוראות היצרן.

מצעים המשמשים למטרות גיבוי יסומנו וישמרו בנפרד – ראה פרק ה׳.

הערה: מידע רשום על מצע מגנטי אינו ניתן למחיקה מוחלטת עקב תכונותיו הפיסיות והכימיות של החומר ממנו עשוי המצע. שיטת כתיבה על כתיבה איננה מעלימה תמיד את המידע הקיים על

המצע. אמצעים טכניים מאפשרים שיחזור וקריאה אחורנית כמה דורות של המידע הרשום על המצע.

מצעים מגנטיים ו/או אופטיים מקולקלים, ובכלל זה דיסקים קשיחים, לא יוצאו מתחומי המשרד, אם נכלל בהם חומר מסווג ("חסוי ביותר"). המצעים יועברו אל ממונה אבטחת המידע אשר ידאג להשמדתם. לפני תחילת התהליך ונקיטה באיזשהו צעד בנושא, יש להביא העניין לידיעתו ואישורו של מנהל מערכות מידע ו/או ממונה אבטחת מידע. הממונה ינהל פרוטוקול לגבי השמדת המצעים הללו.

ההשמדה תתבצע באופנים הבאים:
- מחיקה
- גריסה ע"י מכונת גריסה מיוחדת למדיה מגנטית/אופטית
- שריפה

דיסקים קשיחים מקולקלים אשר מכילים מידע מסווג (חסוי" או "חסוי ביותר"), ואשר הוחלט לתקנם, יטופלו בתיאום עם ממונה אבטחת מידע רק לאחר קבלת אישורו המותנה בכך כי החברה המתקנת התחייבה בכתב לשמור על סודיות מוחלטת ולנקוט באמצעים שהוכתבו מראש על ידי המשרד. טפסי ההתחייבות לשמירת סודיות ישמרו אצל ממונה אבטחת מידע.

העברת מידע מחוץ ליחידה תעשה אך ורק על מצעים חדשים או מצעים של הגוף המקבל.

כל יחידה המוציאה מצעים אל מחוץ לכתליה, תנהל מחברת רישומים. זו תאפשר לנתח בכל עת איזה מידע נמסר, על גבי איזה מצע, למי, מתי, אם המצע עצמו אמור לחזור אל השולח וכן אם אכן חזר אל המשרד. כל זאת בכפוף לחוק הגנת הפרטיות. ברישום תעשה אבחנה בין הוצאת חומר ליחידה אחרת במשרד, לבין הוצאה אל גורם חיצוני.

כל מצעים מגנטיים ו/או אופטיים במשרד יסומנו בסימן בולט ומפורש כרכוש של המשרד. אין להשתמש במצעים ללא סימון המשרד.

כל הקלטות במחשב המרכזי תסומנה במספר רץ, שיזהה אותן חד ערכית. מספור הקלטות יעשה על ידי המפעילים. ספרית הסרטים תוגדר כמקום פיסי נפרד ונעול. תיקבע רשימת מורשי כניסה לאזור.

מקורות

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

נוהלי אבטחת המידע בעיריית ירושלים, פברואר 2001.

חוק הגנת הפרטיות התשמ"א – 1981 ותקנותיו.

מכון התקנים הישראלי, תקן ישראלי 1495 חלק 2 - אבטחת מערכות מידע ממוחשבות – מצעים נושאי מידע..

מכון התקנים הישראלי, תקן ישראלי 1243 – בטיחות אש של מחשבים וציודם ההיקפי.

העברת מידע והוצאתו

א. הוצאת אמצעי נושאי מידע מחוץ למשרד, ב. העברת מידע בין גופים ציבוריים, ג. זכות עיון במאגרי מידע

נוהל מס׳ 21

א. הוצאת אמצעי נושאי מידע מחוץ למשרד

מטרות הנוהל

להגדיר הנחיות המאפשרות הוצאת אמצעים נושאי מידע (מסמך, תיק, דיסקט וכד׳) מחוץ למשרד.

אחראי לביצוע הנוהל

באחראיות גורמי המשרד העוסקים במידע על כל סוגיו, לוודא יישומו של נוהל הזה.

ממונה אבטחת מידע יקיים פעילויות להגברת מודעות להנחיות נוהל זה, יבצע בקרה ואכיפה מדגמית.

מנהלים ישירים של העובדים יאשרו הוצאתו של מידע מחוץ למשרד, בכפוף לצורך ו/או דחיפות מקצועית. בנוסף, יתדרכו לגבי הנחיות אבטחת מידע, בסיוע ממונה אבטחת מידע. ככלל, יש לשאוף להוציא מידע מחוץ למשרד מעט ככל שניתן.

גוף הנוהל

על פי החוק, חל איסור למסור מידע של המשרד לגורם חיצוני ללא רשות של גורם מוסמך במשרד.

מידע המכיל ריכוז פרטים לגבי אנשים ומסווג כמידע רגיש עפ״י הוראות חוק הגנת הפרטיות וכן כל מידע אחר של המשרד, יימצא תחת משמורת העובד המחזיק בחומר בכל זמן נתון.

אין להשאיר מידע מהסוג האמור בכלי רכב או בכל מקום אחר ללא השגחה, לרבות מידע הנלקח למקומות ציבוריים, משרדי חברות אחרות וכדומה.

מידע יילקח בתוך מעטפות סגורות, קלסרים הסוגרים באמצעות גומייה שתימנע נפילתם של דפים או תיקים. אין לשאת מידע בלתי ארוז.

המידע הנלקח לבתיהם של עובדים ייארז בתום יום הפעילות ולא יוותר חשוף או נגיש לאורחים/מבקרים/מנקה וכדומה.

לא יוציא עובד מידע מתחומי המשרד לכל מטרה שהיא בטרם יקבל אישור הממונה עליו להוצאת המידע ובטרם תודרך בעניין סדרי אבטחת המידע אשר עליו ליישם.

כל מקרה חריג, תקלה או אירוע הנוגעים או העלולים להשליך על אבטחת המידע, ידווחו באופן מיידי על ידי הגורם המחזיק במידע, לממונה אבטחת מידע וכן למנהלו הישיר של העובד.

ב. העברת מידע בין גופים ציבוריים

מטרות הנוהל

הגדרת סידורי העברת מידע בין גופים ציבוריים בהתאם לדרישות חוק הגנת הפרטיות.

אחראי לביצוע הנוהל

מנהל המאגר ינהל, יישם ויבקר יישום הנחיות נוהל זה.
ממונה אבטחת מידע יסייע בהגדרת הדרישות ובמתן פתרונות מקצועיים.

גוף הנוהל

מסירת מידע לגופים ציבוריים תיעשה לפי הכללים הבאים, המפורטים להלן:

כל פניה להעברת מידע בין גופים ציבוריים, תעשה רק על פי דרישות החוק. הדבר אמור הן במקרה שהמשרד הוא הגורם הפונה והן במקרה בו הפניה מופנית אל המשרד.

בעת מסירה של מידע לגוף ציבורי אחר, על מנהל מאגר המידע לנקוט בפעולות אבטחה ובקרה ולדאוג כי השימוש במידע על ידי המערכת המקבלת יהיה לכל הפחות שווה ברמת האבטחה לזו הנהוגה במשרד.

על גבי דוחות מודפסים יופיע הנוסח הבא בכל עמוד "מכיל מידע מוגן לפי חוק הגנת הפרטיות – המוסרו שלא כדין עובר עבירה".

עם גמר השימוש בדו"ח חלה על מקבל הדו"ח האחריות להשמיד את הדו"ח או להחזירו לממונה על אבטחת מידע. השמדת הדו"ח משמעה גריסתו במגרסת נייר או מסירתו למחזור במפעלי נייר באמצעות החברה בעלת הזיכיון.
על גבי סרטים מגנטיים, קלטות, דיסקטים ותקליטורים תודבק מדבקה ועליה נוסח הבא:
"מידע מוגן לפי חוק הגנת הפרטיות".

ועדת היגוי לאבטחת מידע תהיה מוסמכת לקבוע, אלו משאבי מידע לא יימסרו לטיפול בידי גורמי חוץ על פי המבחנים הבאים:

(1) מידע רגיש אשר זמינותו, שלמותו ואמינותו חיוניים באופן קריטי לניהולה התקין של המשרד.
(2) חשש סביר שגורם החוץ עלול להימצא במצב של ניגוד עניינים.
(3) שיקולים אחרים שתציג הנהלת המשרד.

מקבל המידע יחתום על התחייבות שלא למסור את המידע לגורם שלישי ולהשתמש בו אך ורק למטרה שנמסרה בבקשת המידע. עם גמר השימוש בדו"ח, ידאג מקבל המידע להשמדת הדו"ח או להחזרתו.

מנהלי מאגרים המעבירים דרך קבע מידע לגופים ציבוריים מסוימים, ידאגו לקיומה של התקשרות בה יישמו עקרונות האבטחה, בקרת הגישה ורישום המידע בהתאם לדרישות החוק והנהלים. עותק מהתקשרות זו ימצא אצל מנהל המאגר.

כל העברת מידע מן הסוג הנדון טעונה אישור בכתב של היועץ המשפטי במשרד.

בקשה להעברת מידע מגוף ציבורי ומתן האישור יבוצעו בכתב על גבי טופס בקשה. מתן האישור ע"י הגוף המוסר יינתן על גבי טופס התשובה. אין לאשר את העברת מידע ללא טפסים אלה הממולאים כיאות.

על הטפסים יחתמו הגורמים המורשים בשני הגופים (המוסר והמקבל) וכן היועצים המשפטיים של גופים אלה.
ממונה אבטחת המידע יקבל דיווח על העברות מידע מן הסוג האמור.

אם מידע מועבר דרך קבע, על הגוף מקבל המידע לדווח לרשם מאגרי המידע.

ג. זכות עיון במאגרי מידע

מטרות הנוהל

להסדיר מימוש "זכות עיון" במאגרי המידע הממוחשבים המכילים נתונים אודות הפרט, תוך מניעת מסירת מידע למי שאינו זכאי לקבלו.

גוף הנוהל

כל פניה של אזרח או גורם אחר, למימוש זכות עיון, תובא באופן מיידי לידיעת מנהל מאגר הרלוונטי.

זכות העיון מותנית בכך שאין איסור חוקי על מימוש זכות העיון. לדוגמא: חוק הנוער – טיפול והשגחה.

מנהל המאגר יביא את הבקשה לידיעת היועץ המשפטי של המשרד ובמקביל לממונה על אבטחת המידע.

במקרה של ספק, יעדכן ממונה על אבטחת המידע את המשנה למנכ"ל המשרד אודות קיומה של הבקשה והבעיה הקשורה אליה.

כל הטיפול ייעשה על בסיס הטופס המיוחד המיועד לנושא. פניה שתגיע בכל דרך או אופן אחר, יידחה הטיפול עד למילוי הטופס כיאות, ורק אז יחל בה הטיפול על פי כל יתר ההנחיות.

את התשובה לפונה יעביר מנהל המאגר באמצעות הטופס המיועד לכך.

למען הסר ספק, מובהר בזאת כי עובד במשרד לא ישלוף נתונים ממאגר מידע בין אם הוא ממוחשב ובין שאיננו כזה, אלא אם הוסמך לכך לצורך תפקידו בלבד.

טיפול בבקשה לעיון במידע ייעשה תוך תיאום עם המטפל הישיר במבקש.

מקורות

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

נוהלי אבטחת המידע בעיריית ירושלים, פברואר 2001.

חוק הגנה על הפרטיות התשמ"א – 1981 ותקנותיו.

רישום המאגרים

נוהל מס׳ 22

מטרות הנוהל

להנחות באשר לקביעת המאגרים שהנם ״מאגרי מידע״ על פי החוק, וסדרי רישומים אצל רשם מאגרי המידע שבמשרד המשפטים.

הגדרות

״מידע״ – נתונים המתייחסים לעובדות/לפרטים אודות פרטיו של אדם.

״מאגר מידע״ לפי חוק – הנו מאגר הכולל מידע אודות הפרט ומתייחס לנתונים על אישיותו של אדם, מעמדו אישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו מקצועית, דעותיו ואמונתו. אוסף של נתוני מידע (כמשמעו בחוק) המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד מחשב.

אחראי לביצוע הנוהל

ביצוע נוהל זה באחריות מנהל היחידה בה מוצב המחשב, מנהל מאגר מידע וכן הממונה על אבטחת מידע.

ממונה על אבטחת המידע יסייע במתן פתרונות מקצועיים לעמידה בדרישות החוק כמפורט.

גוף הנוהל

כל מאגר מידע הכולל נתונים אודות הפרט, הנו מאגר כמשמעותו בחוק. גם מאגר מידע הכולל רשימות שמיות בלבד, אולם כותרתו מצביעה על פרטים, מצב או עובדה שהחוק מגדירם כ״מידע״, הנו מאגר כנ״ל. במידה של ספק, יש לפנות לממונה אבטחת מידע במשרד.

כל אחראי לתפעול מערכות מידע כלשהי, ידווח על קיומה לממונה על אבטחת המידע במשרד. הדיווח יכלול פרטים אודות המערכת ואת אמצעי האבטחה עליה. הממונה על אבטחת המידע יבדוק אם המאגר מתאים להגדרת החוק. במידה וכן, יפעל לרישומו במשרד המשפטים. יש לדווח כנ״ל על הקמת כל מערכת מידע חדשה.

לכל מאגר מידע יקבע מנהל מאגר.

מנהל המאגר יחתום על שאלון הרישום של משרד המשפטים, שנמסרו לו ע״י הממונה למערכות המידע במשרד. השאלון יישלח אל רשם מאגרי המידע, ע״י הממונה על אבטחת המידע במשרד.

כל מאגרי המידע הרלוונטיים על פי הגדרות חוק הגנת הפרטיות, יירשמו כנדרש באותו חוק.

בכל מקרה של התלבטות בקשר להתאמת מאגר המידע המסוים אל המוגדר בחוק, יש לפנות לקבלת ייעוץ מתאים, באמצעות הממונה על הפעלת חוק חופש המידע, אצל הגורם המוסמך הרלוונטי.

כל גורם במשרד שמתעתד להקים מאגר נתונים שענינו נתוני פרט, ידווח על כך בדחיפות לממונה על אבטחת המידע אשר ישקול ויבדוק אם יש לרשום את המאגר אצל רשם מאגרי המידע במשרד המשפטים. אם יימצא הצורך, יפעל לרישום המאגר, כנדרש.

בכל מקרה בו השתנו נתונים מהותיים לעומת המצב ששרר בעת רישומו של מאגר מידע, כגון שם מנהל המאגר, מורשי גישה, מטרות וכו׳, יש להודיע בכתב לרשם מאגרי המידע על מנת לשנות את פרטי הרישום.

אצל ממונה על אבטחת המידע והממונה על הפעלת חוק חופש המידע יימצא רישום מדוקדק של כל מאגרי המידע של המשרד הרשומים אצל רשם מאגרי המידע במשרד המשפטים, וכן של כל המאגרים הנמצאים בתהליכי רישום כולל עדכון הסטטוס.

מקורות

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

נוהלי אבטחת המידע בעיריית ירושלים, פברואר 2001.

ניהול מלאי חומרה ותוכנה

הנוהל מס׳ 23

מטרות הנוהל

לקיים הגנה נאותה על נכסי המשרד. שליטה בכמויות החומרה והתוכנה ומקום הימצאותם במשרד ובגופים הקשורים, שתסייע במניעת התקנת תוכנות או עזרים ואביזרים, העלולים לפגוע בכשירות הציוד, במידע או בתוכנות אחרות.

אחראי לביצוע הנוהל

מצבת חומרה ותוכנה תנוהל, תבוקר ותתוחזק ע״י צוות מרכז תמיכה באחריות מנהל סיוע טכני ותקשורת רוחבית, בנושא חומרה, ומנהל צוות תמיכה של יחידת מערכות מידע, בנושא תוכנה.

על מחלקת כוח אדם לעדכן מחלקת מחשוב בדבר שינויים במצבת העובדים.

גוף הנוהל

תהיה התייחסות לכל נכסי המידע הראשיים וייקבעו להם בעלים. הטלת אחריות למתן הדין על נכסים עוזרת להבטיח שנשמרת רמה נאותה של הגנה. יזוהו הבעלים של כל הנכסים הראשיים ותוטל אחריות לתחזוקה ובקרות נאותות. מי שנקבעו להיות הבעלים של הנכס, הם יישארו הנושאים באחריות למתן הדין.

רשימת מצאי של נכסים עוזרת להבטיח שתהיה הגנה אפקטיבית על הנכסים, והן יכולות להידרש גם למטרות אחרות של העסק, כגון בטיחות וגהות, ביטוח או סיבות כספיות (ניהול נכסים). תהליך הכנת מצאי נכסים הוא היבט חשוב בניהול סיכונים. משרד צריך להיות מסוגל לזהות את נכסיו ואת הערך והחשיבות היחסיים שלהם. על בסיס המידע הזה יכול המשרד לספק רמות אבטחה המתאימות לערכים ולדרגות החשיבות היחסיים של הנכסים. תוכן ותתוחזק רשימת מצאי שתכלול את הנכסים החשובים הקשורים לכל מערכת מידע. כל נכס יזוהה בבירור ובעלים וסיווג האבטחה שלו ייקבעו בהסכמה ויתועדו, יחד עם מקומו הנוכחי (חשוב בעת ניסיון התאוששות מאובדן או נזק).

דוגמות לנכסים הקשורים במערכות מידע הן:

א. נכסי מידע: מסדי נתונים וקובצי נתונים, תיעוד המערכת, מדריכי משתמשים, חומר הדרכה, נוהלי תפעול או תמיכה, תוכניות התאוששות, סידורי עתודה לשעת חירום, מידע ארכיוני;

ב. נכסי תוכנה: תוכנות יישום, תוכנת מערכת, כלי פיתוח ותוכניות שירות;

ג. נכסים פיזיים: ציוד מחשבים (מעבדים, צגים, מחשבים נישאים, מודמים), ציוד תקשורת (נתבים, מרכזיות פרטיות, מכונות פקס, משיבונים), מצעים מגנטיים (סרטים ודיסקים), ציוד טכני אחר (ספקים, יחידות מיזוג אוויר), ריהוט;

ד. שירותים: שירותי מחשוב ותקשורת, שירותים כלליים, כגון חימום, תאורה, חשמל, מיזוג אוויר.

צוות מרכז התמיכה ינהל יומן רישום ומעקב בו תפורט מצבת התוכנה וצוות סיוע טכני ינהל יומן רישום בנושא מצבת החומרה.

כל שינוי במצבת, לרבות גריעת ציוד, משלוחו לתיקון או הוספת ציוד חדש, יתועדו ביומן. כמו כן, יש לציין את מיקומו במשרד.

מעת לעת יבצעו צוות מרכז תמיכה וצוות הסיוע הטכני בדיקה בשטח המשרד על מנת לוודא את נתוני היומן בשטח (ספירת מלאי בפועל).

אין לרכוש חומרה או תוכנה ללא אישור הגורם המתאים ביחידה למערכות מידע.

מקורות

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

נוהלי אבטחת המידע בעיריית ירושלים, פברואר 2001.

מכון התקנים הישראלי, תקן 7799 - ניהול אבטחת מידע.

אבטחת רשומות ותעודות רשמיות

נוהל מס׳ 24

מבוא

עיקרה של אבטחת רשומות (רשומות על גבי מצעים מגנטיים, אופטיים, או, על גבי ניירת) הוא בעצם בקביעה ובהתקנה של אמצעי אבטחה ומידור, במטרה למנוע מגורם עוין, או בלתי מוסמך **את השגת המידע** הכלול ברשומות, **או את האפשרות לפגוע באמינותן, בשלמותן, בזמינותן או בשרידותן**, והיא תושג תוך יישום כל הפעילויות האלה:

א. קביעת סיווג מתאים (הנסמך על רמת סודיות/חיסיון המידע ורמת חיוניות המידע).
ב. הגבלת התפוצה **רק** לאנשים אשר צריכים לראות, או, לקבל את הרשומה, לצורך תפקידם הרשמי, וסיווג (מהימנותם) האישי אינו נמוך מסיווג הרשומה.
ג. התקנת כלים, טכנולוגיים ומינהליים, לשמירה תקינה של הרשומות.
ד. הדרכת העובדים העוסקים ברשומות **״ציבוריות רגישות״** לשמירה הולמת עליהן.
ה. קיום בקרות וביקורות על טיב האבטחה, במשך כל מחזור החיים של הרשומות.

הגדרות

״מידע״ - כל תיאור, תוכנית, סיסמה, סמל, נוסחה, חפץ או חלק מהם, המכילים ידיעה, כמשמעה בחוק העונשין, התשמ״א- 1981, או העשויים לשמש מקור לידיעה, לרבות מידע שאינו נכון.

״מידע רגיש״ (לא בטחוני) - כל מידע הנמצא בידי משרדי הממשלה וכל יתר הרשויות הציבוריות (בכל שלבי הטיפול ובכלל זה גם בהעברה, באחסון, או בגניזה), על כל סוג מצע -מידע, אשר הוטבעה או נרשמה עליו אחד, או כמה מהסימנים האלה: **סמל מדינת ישראל**, המילים - ״**מדינת ישראל**״, **שמו של גוף ציבורי, אגפיו, או, יחידות-הסמך** שלו, ושמירת המידע הנ״ל נדרשת בשל היותו, אחד, לפחות, מאלה:

א. מידע אשר פגיעה בסודיותו, בשלמותו, באמינותו, בזמינותו, או, בשרידותו, עלולה לגרום לאחת מהבאות -
1. פגיעה בניהולה התקין של המדינה;
2. פגיעה או שיבוש פעילותם התקינה ומילוי תפקידם של משרדי הממשלה ויתר הרשויות הציבוריות;
ב. מידע המכיל פרטים אישיים המוגנים ע״י החוק להגנת הפרטיות, התשמ״א - 1981 ותקנותיו, התשמ״ה - 1985.
ג. מידע אודות מדיניות הנמצאת בשלבי עיצוב;
ד. מידע הכולל פרטים על משא ומתן עם גוף או עם אדם שמחוץ לרשות;
ה. מידע החייב בשמירה על פי כל דין;
ו. מידע שהוא סוד מסחרי, או סוד מקצועי או שהוא בעל ערך כלכלי, שפרסומו עלול לפגוע פגיעה ממשית בערכו, וכן מידע הנוגע לעניינים מסחריים או מקצועיים הקשורים לעסקיו של אדם, שגילויו עלול לפגוע פגיעה ממשית באינטרס מקצועי, מסחרי, או כלכלי, למעט מידע בנושאי איכות הסביבה, כמפורט בסעיף קטן, 9 (ב) (6) (א) ו- (ב), החוק לחופש המידע, התשנ״ח- 1998;
ז. מידע שהגיע לידי הרשות הציבורית, שאי גילויו היה תנאי למסירתו, או שגילויו עלול לפגוע בהמשך קבלת המידע;
ח. מידע אודות שיטות עבודה ונהלים של רשות ציבורית העוסקת באכיפת החוק, או שיש לה סמכות חקירה, או ביקורת, או בירור תלונות על פי דין, אם גילויו עלול לגרום לאחד מאלה:
1. פגיעה בפעולות האכיפה, או הביקורת, או בירור התלונות של הרשות.
2. פגיעה בהליכי חקירה או משפט או בזכותו של אדם למשפט הוגן.

גילוי או מתן אפשרות לגלות את קיומו או זהותו של מקור מידע חסוי;
ט. מידע הנוגע לענייני משמעת של עובד של רשות ציבורית, למעט מידע בדבר הליכים הפומביים על פי החוק;

״רשומה״ - מידע כתוב בכל צורה שהיא, לרבות מברק, טיוטה (כולל תרשומת ותקציר) מפה, פלט

מחשב, כתב יד, טיוטה, מכתב, שאלון ממולא, תעודה רשמית מברק, פלט פקס, הדפסות (כולל פסולת פלט מחשב), העתקת נייר, נייר פחם משומש, וכדי.

"**תעודה רשמית**" - כל סוג של תעודה המופקת על ידי הממשלה ומוסדותיה, לשם זיהוי, או, קביעת מעמד אזרחי, מקצועי, אישי, וכיוצא בכך או, להקניית זכויות אישיות למיניהן, לרבות **תעודת-זהות, דרכון, תעודת-עולה ואח**', בכל משך חיי התעודה.

"**משך חיי רשומה**" - פרק הזמן שבין הכנת הרשומה לבין מועד ביעורה כדין, על פי קביעת גנז המדינה וכל דין. בכלל זה: כל שלבי ההכנה, ההובלה, האחסון, המסירה הגניזה, ועד תום הביעור.

"**סיווג**" - קביעת רמת **<u>הרגישות</u> או <u>החיוניות</u>** של הרשומה.

"**רשומה רגישה**" - רשומה אשר לתוכנה נקבע סיווג, המחייב את הטיפול בה על פי נוהל זה.

"**חיוניות**" - מימד המאגד בתוכו את מירב השיקולים לשמירת "מידע רגיש" (הצורך בשמירת **זמינות, השלמות האמינות, והשרידות** של המידע, למעט שמירת הסודיות) וכן הוראות כל דין), או לשם ניהולם התקין של הרשויות הציבוריות וניהול תקין של משק המדינה.

"**רשומה חיונית**" - הוספת הכותרת "**חיוני**" בראש כל דף של מסמך רשמי מעלה את רמת החיוניות הבסיסית שהייתה לו, ומקנה לו רמת חיוניות אמצעית, או, עליונה וצורך בנקיטת אמצעים נוספים/ מיוחדים לשמירה איכותית, כמפורט בנוהל זה.

"**מידע בלתי-מסווג" (בלמ"ס)** - מידע אשר עונה על כל התבחינים האלה:

א. אינו רגיש מהיבטי סודיות/מידור וניתן לפרסמו בציבור.
ב. אינו עונה על התבחינים לסיווגי מידע "חסוי", או, "חסוי-ביותר" שלהלן.
ג. פגיעה בזמינותו, באמינותו, או בשלמותו עלולה לשבש את פעילות המשרדים.

דוגמאות ל"מידע רגיש" אשר בדרך כלל ייחשב כ- "בלתי-מסווג".

"**מידע חסוי**" - מידע שפגיעה באמינותו, בשלמותו, בזמינותו, בסודיותו או בשרידותו עלולה לגרום לתקלות כגון אלה:

א. פגיעה או הכבדה על ביצוע תוכניות או פעולות כלכליות, מינהליות, חברתיות, משפטיות ואחרות, של המדינה.
ב. גרימת תקלה לעבודת הגופים הציבוריים שמשמעה עיכוב או ייקור תהליכי עבודה, או, הפרעה בביצוע אכיפת החוק.
ג. חשיפת מידע אישי המוגן על ידי החוק להגנת הפרטיות, התשמ"א- 1981.
ד. הפרת כל דין המחייב שמירה על סודיות (או חיסיון) מידע.

"**מידע חסוי-ביותר**" - **מידע שפגיעה באמינותו, בשלמותו, בזמינותו, בסודיותו, או, בשרידותו עלולה לגרום לשיתוק חלקי, או מלא, של ניהול המדינה או הגופים הציבוריים.** להלן מספר דוגמאות:

א. הקניית יתרון כלכלי מכריע למדינה זרה או לגורם זר.
ב. הכשלת תוכניות או פעולות כלכליות ומסחריות של מדינת ישראל.
ג. חשיפת מידע העלול לגרום לבהלה בציבור.
ד. חשיפת מידע אישי "רגיש", או, "מוגבל", כמשמעו בחוק הגנת הפרטיות, שהינו רגיש ייחודית.
ה. שיתוק מערכות המידע של הגופים הציבוריים.
ו. פגיעה בהיערכות, החלשה, או קריסת מערכות היערכות משק המדינה לשעת – חירום.

מטרת הנוהל

מניעה, או צימצום האפשרות של גורמים פנימיים בארגון, או חיצוניים, המבקשים לשבש את פעילות המשרד התקינה, או מגורמים בלתי מוסמכים אחרים, להשיג שלא כדין את "**המידע הרגיש**" הכלול ברשומות, וכן למנוע או לצמצם את יכולתם של הנ"ל לפגוע בשלמותן, בזמינותן במהימנותן, או בשרידותן של "**רשומות רגישות**".

קביעת האמצעים למידור ולאבטחה, המכוונים להבטיח כי "**המידע הרגיש**" הכלול ברשומות יגיע **<u>רק</u>** אל מי שצריך ומוסמך לקבלו, תוכן הרשומה לא ישונה בכל דרך שהיא, על ידי מי שלא הוסמך לכך, והיא תהיה ראויה לשימוש על פי צרכי הגוף -המונחה, בכל משך זמן שנקבע כאורך חיי הרשומה. (עפ"י כל דין, ובכלל זה חוק הארכיונים, התשט"ו- 1955, ותקנותיו, וכן הנחיות משלימות של גנז המדינה).

קביעת האמצעים והשיטות הנדרשים לשמירה של "**תעודות רשמיות**", ובכלל זה: גלופות, טפסים, וחומרי גלם המשמשים להכנתם, בכדי לצמצם או למנוע את גניבתם, לקיחתם ומסירתם שלא כדין, השחתתם, או כל שימוש אחר שלא כדין.

להורות על ביצוע אבטחת **רשומות רגישות** ותיעוד רשמי לעובדי המדינה ומוסדותיה ולגורמים הקשורים אליהם, בתוך תחומי מדינת ישראל ובחו"ל.

הנוהל אינו מבטל, מחליף, או גורע מהוראות כל דין והנחיות ממלכתיות כגון: חוק הארכיונים ותקנותיו, חוק הגנת הפרטיות ותקנותיו, תקנות שירות המדינה או נהלים פנימיים של המשרדים והגופים השונים, **אלא מוסיף עליהם**.

נוהל זה <u>אינו</u> מיועד להנחות את דרכי הטיפול ברשומות מסווגות-ביטחונית !

אחראי על ביצוע הנוהל

ממונה על אבטחת "מידע-רגיש" (להלן -"הממונה")

ייזום פעילויות הדרכה והסברה בקרב כל העובדים בארגון, על מנת להטמיע את נושא אבטחת המידע, בכלל, ויישום הוראות נוהל זה, בפרט. ינחה כל עובד חדש (בכל מעמד ובכל תפקיד) המתקבל לעבודה במשרד, וימסור לו עותק מנוהל זה. יקיים פעילויות בקרה וביקורת שנתיות, כדי לבחון את אופן יישומו של הנוהל בארגונו. יעביר את ממצאי הבדיקות לידיעת הממונה הישיר.

ביקורת על אבטחת המידע

המבקר הפנימי של המשרד יוסיף את נושא אבטחת הרשומות לתוכנית הביקורת השנתית. אבטחת הרשומות במשרדי הממשלה תהיה נושא לביקורת של "**היחידה**".

אחריות אישית כל עובד אחראי, אחריות-אישית לאבטחת "**הרשומות הרגישות**" המצויות ברשותו, על פי נוהל זה.

אחריות מינהלית כוללת
המנהל-הכללי במשרדי הממשלה ומוסדותיה, אחראי, אחריות כוללת, כי "**רשומות רגישות**" ו"**תעודות רשמיות**" שבאחריות משרדו, יאובטחו על פי הנחיות נוהל זה, ועל פי כל דין.

גוף הנוהל

קביעת סיווג מתאים לרשומה

א. נוכח מספרם הרב של פריטי "**מידע-רגיש**" הקשורים בניהול משק המדינה בניהול הגופים הציבוריים, במידע אישי ("**רגיש**" או "**רפואי-מוגבל**"), או במידע שהוא קניינם של פרטים, או תאגידים, לא ניתן ליחס לכולם אותה מידה של חשיבות ולהקצות לכולם את אותם אמצעי-אבטחה. לפיכך, אנו קובעים סדר עדיפויות לטיפול במידע הנ"ל, בהתאם לערכו של המידע ולמידת הנזק שעלול להיגרם למדינה, לארגון, ולכל אדם, כתוצאה **חשיפתו,** או **מפגיעה בשלמותו, באמינותו, בזמינותו ובשרידותו.**

ב. קביעת סיווג לרשומה נסמכת על פי שני מדדים: **מידת הסודיות/החיסיון של המידע** כן **מידת החיוניות** (הצורך בשמירת זמינותו, שלמותו/אמינותו ושרידותו).

ג. **"הממונה"** יכין רשימה של נושאים מסווגים המטופלים על ידי העובדים בארגונו**.** כל נושא יהיה מסווג על פי מידת הסודיות וכן החיוניות. כל המטפלים במידע רגיש יקבלו (אישית ובצורה ממודרת, עפ"י הצורך) מהממונה, את רשימת הנושאים הנ"ל**.** "הממונה" יעדכן מעת לעת את רשימת הנושאים המסווגים ויפיצה בין הגורמים הרלבנטיים.

ד. **<u>סיווג רמת הסודיות/החיסיון</u>**: יש לסווג את הרשומה, על פי מידת הנזק המירבי שיגרם כתוצאה מחשיפתה למי שלא הותרו לכך, לאחת מתוך שלושת הרמות : **"בלתי-מסווג", "חסוי" ו- "חסוי-ביותר".**

ה. **<u>סיווג רמת החיוניות של המידע</u>**: יש לסווג את הרשומה גם על פי חיוניותה המירבית. משמע, מידת הנזק שעלול להיגרם **כתוצאה מפגיעה בשלמותה, באמינותה, בזמינותה, או, בשרידותה.**

ו. כל שלבי הטיפול ב"**רשומה רגישה**" ייעשו רק על ידי עובדים שהוסמכו לכך על ידי המשרד, לאחר שקיבלו אישור מהימנות מ"**הממונה על הביטחון**" (קב"ט).

ז. בשיקולים לסיווג רשומת נייר **כ- "רגישה"** יש לקחת בחשבון גם את רשימת המכותבים לאותה רשומה, שמא מתוך שמותיהם ו/או עיסוקיהם ניתן יהיה **ל**הסגיר את הנושא הרגיש, גם אם תוכן הרשומה אינו מחייב סיווג רגישות גבוה. **<u>לדוגמא</u>**: זימון לדיון כאשר רשימת המשתתפים עלולה להסגיר נושא רגיש.

שינוי מושגים

בכל מהלך הטיפול בשמירת "**מידע-רגיש**" ייעשה שימוש רק בשמות הסיווג האלה: **בלתי-מסווג" , "חסוי" ו- "חסוי-ביותר",** ולא ייעשה כל שימוש במונחים של בטחון המדינה כגון: "שמור", "סודי" ו- "סודי ביותר".
<u>דוגמאות</u>: **א.** רשומה המכילה "**מידע-אישי**" אודות מצב בריאותו הנפשית של פלוני, תסווג כ- "**חסוי -ביותר**".
ב. רשומה אודות רישום פלילי של אדם מסוים - תסווג כ -"חסוי".

רישומים אישיים
התכתבות בדבר מעמדם האישי של עובדים כגון: פיטורין, רישומים-רפואיים וכד' יסווגו בסיווגים שהוגדרו בנוהל זה.

סיווג צרור רשומות
צרור של רשומות המסווגות בסווגי רגישות שונים **(כולל סיווגים ביטחוניים)**, יסווג לפי הרשומה בעלת **סוג הרגישות הגבוה ביותר** שבצרור.
סווג אמון "לנמען בלבד"

בסיווג אמון "לנמען בלבד" ייעשה שימוש במקרים ובמגבלות אלה:

א. כאשר כותב רשומה רוצה להגביל את תפוצתה ולוודא פתיחת המעטפה רק על ידי הנמען עצמו, יציין על הרשומה ועל המעטפה את ההערה "**לנמען בלבד**". מעטפה זו תפתח על ידי <u>הנמען בלבד</u>, <u>או על ידי הממונה עליו</u>. בהעדרם יש לבקש את רשות השולח שהמעטפה תיפתח על ידי עובד אחר. ככלל, לא יתיר הנמען לעובד אחר פתיחתה של מעטפה, עליה צוין סוג אמון "**לנמען - בלבד**" ושנועדה לו.

ב. מקבל הרשומה אחראי לביצוע הרישומים המתחייבים במידה ומדובר ב"**רשומה רגישה**"

ג. **סווג אמון אינו בא במקום סיווג הרגישות, אלא בנוסף לו !**

בעלי הסמכות לסיווג
א. **<u>רשאים לסווג רשומה בסיווג "חסוי-ביותר"</u> -**
1. עובדים בדרג של ראש אגף ומעלה או עובדים בדרג מקביל וממלאי מקומם.
2. ראשי נציגויות בחו"ל וממלאי מקומם.
3. מנהלי לשכות שרים וממלאי מקומם.

4. ממונים על אבטחת "מידע-רגיש", או ממונים על הביטחון (קב"טים).
5. כל עובד בדרג בכיר שהוסמך לכך ע"י "**הממונה**".
6. עובדי הגופים הציבוריים המטפלים בתוקף תפקידם במידע "**אישי רגיש**" ו-"**מוגבל**", בנושאים האלה: **א)** רפואה [כולל בריאות הנפש], **ב)** אימוצים.

ב. <u>רשאים לסווג רשומה בסיווג "חסוי</u>" -

כל עובדי המשרד שקיבלו מהממונה על הביטחון **(קב"ט)** הכשר מהימנות לרמת "**חסוי**".

הכנת "רשומה רגישה"
א. עורך הרשומה יסמן גם על גבי הטיוטה את סיווגה ואת רשימת התפוצה.

ב. סוג הרגישות של כל רשומה בסיווג "**חסוי**", **או, "חסוי-ביותר**", יסומן בראש כל דף במרכזו.

ג. ה**<u>סיווג "בלמ"ס" לא יצוין על גבי רשומות.</u>** למעט מברקים הנשלחים באמצעי הקשר של משרד החוץ.

ד. בכל רשומה המכילה מידע **רפואי** "**מוגבל**", כמשמעו בחוק הגנת הפרטיות, התשמ"א- 1981 , המופקת עבור גוף ציבורי אחר, יש לקבוע בכל עמוד כותרת **בולטת** בזו הלשון:

"מכיל מידע מוגן לפי חוק הגנת הפרטיות - מוסרו שלא כדין עובר בירה".

ה. מרשומה שסיווגה "**חסוי-ביותר**" יוכנו מספר עותקים שלא יעלה על המספר המירבי ה<u>הכרחי</u> לצורכי המשרד.

ההנחיות שלהלן (סעיף קטן **ו'** עד **יא'**, כולל) הנן **<u>חובה</u>** לרשומות בסיווג "**חסוי ביותר**", ובגדר **<u>המלצה</u>** עבור רשומות בסיווג "**חסוי**" -

ו. ברשומות שסיווגן "**חסוי-ביותר**", או, "**חסוי**" ימוספרו הדפים כלהלן:
1. על העמוד הראשון יצוין (בצד שמאל למעלה):

ברשומה .... דפים עותק .... מתוך ... עותקים

2. בעמודים הנוספים יירשם מספר הדף כמקובל בצד שמאל למעלה, כדלהלן:

עותק מס': .....

ז. בחוברות הכרוכות בצורה שאינה מאפשרת החלפת עמודים, אין צורך בציון מספר העותק בכל עמוד.
ח. דפי הרשומה המסווגת יחוברו במכונת חיבור ("שדכן") ולא ע"י מהדק או סיכה.
ט. רמת סווג של תיקים (לרבות תיקים שוטפים) תוטבע על הכריכה הקדמית והאחורית. על אוגדנים ("קלסר") תוטבע על חזית ועל גב האוגדן.
י. מכתב לוואי, הנשלח יחד עם רשומה בעלת סוג רגישות גבוה, יסווג באותו הסיווג.
י"א. מכתב לוואי, הנשלח בנפרד, יסווג לפי הסיווג של תוכנו.

העתקת רשומה שסיווגה "חסוי-ביותר", או, "חסוי" :
א. <u>העתקה באמצעות מכונת צילום</u>: אין להכין עותקים מיותרים/ עודפים מרשומה שסיווגה "**חסוי-ביותר**", או "**חסוי**".

ב. כאשר צורכי העבודה מחייבים הכנת עותקים (נייר) נוספים לתפוצה פנימית, תבוצע ההעתקה לאחר שהוטבעה עליה החותמת הבאה:

- שם המשרד -
צילום מסמך "ח ס ו י - ב י ו ת ר"
סה"כ הועתקו ממסמך זה ..... עותקים נוספים
תאריך ההעתקה ../../... עותק זה מקבל מספר .....#   נרשם ביומן, דף ..... שורה .....

ג. דין רשומה רגישה שהועתקה או צולמה, כדין רשומה מקורית, בכל הנוגע לסיווגה ולדרכי הטיפול בה.
הרישום של רשומה שסיווגה "**חסוי-ביותר**", או, "**חסוי**" ייעשה על פי הרשומה המקורית, והעותקים הנוספים שהוכנו יסומנו באותיות **ה-א'-ב', כדלהלן:**

מספר העותקים שצולם:
1. עותק 5/ -א מתוך 5 (כמספר העותקים הנוספים שצולמו).
2. עותק 5/ -ב מתוך 5 (כמספר העותקים הנוספים שצולמו).

שכפול רשומת נייר -
על מנת לשמור על עקרון המידור, יבוצע שכפול רשומות המסווגות כ- "**חסוי-ביותר**" על ידי עובד בעל הכשר מהימנות מתאים. העובד יאסוף לאחר השכפול את כל החומר, לרבות חומר פגום וגלופות.

רישום רשומה שסיווגה "חסוי-ביותר"

א. משרד השולח או מקבל רשומות שסיווגן "**חסוי- ביותר**". ינהל רישום של רשומות. הרישום ייעשה "בקובץ - יומן דואר " (יוצא-נכנס).

ב. רישום הדואר הנכנס יבוצע **לפני שייעשה ברשומה טיפול כלשהו**. הרישום יכלול את כל הפרטים המופיעים בדף ה- "קובץ - יומן" הרישום.

ג. במקרה ומתקבלת רשומה מסווגת בציון סוג אמון "**לנמען בלבד**", או אם רשם הדואר לא הוסמך לפתוח מעטפה המכילה רשומה בסיווג "**חסוי-ביותר**", **לפני** שיעיין בה הנמען, חייב רשם הדואר לרשום ביומן הרישום לאחר קבלת הרשומה מהנמען.

ד. באחריות אישית של מקבל רשומה להעביר לרשם הדואר (מזכירות) את הרשומה, או את הפרטים הרלבנטיים לדרכי הרישום - **<u>לפני</u>** שייעשה בה טיפול כלשהו.
ה. רישום הדואר היוצא יבוצע **לפני** המשלוח ויכלול את **כל** הפרטים המופיעים ביומן הרישום. ביומן זה יירשמו גם העותקים שיועברו לתיוק במשרד.

הכנה למשלוח של רשומה (נייר) רגישה -

א. השולח רשומה שסיווגה "**חסוי-ביותר**", יכניסה למעטפה אטומה ובלתי משומשת, יטביע

עליה את חותמת היחידה וידביק עליה סרט הדברה שקוף.

ב. על גבי המעטפה יצוינו: סיווג הרשומה, שם הנמען, תפקידו וכתובתו המדויקת.

ג. דואר רגיש לחו"ל, בעל חסינות דיפלומטית, יוכן למשלוח על פי נהלי משלוח דואר דיפלומטי.

ד. למכתב שסיווגו "**חסוי-ביותר**" ולמכתב בסיווג "**חסוי**" (באם כולל מידע "**רפואי מוגבל**", המוגן בחוק הגנת הפרטיות, התשמ"א- 1981) יש לצרף **תעודת משלוח** במקור. עותק מתעודת המשלוח יתויק אצל השולח, למעקב ולביקורת.

ה. שולח המכתב ידאג לכך שתעודת המשלוח תוחזר לו כשהיא חתומה. לאחר קבלתה יצרף אותה לעותק שברשותו.

ו. באם לא הוחזרה תעודת המשלוח תוך 10 ימים, יבדוק השולח את סיבת העיכוב ויוודא קבלתה.

ז. מותר להשמיד תעודות משלוח כעבור חודש מיום הוצאתן.

משלוח רשומת נייר רגישה בדואר

א. רשומה שסיווגה "**חסוי-ביותר**" תועבר בארץ בשיטות ובאמצעים כדלהלן :

1. במישרין - מידי השולח לידי המקבל (תוך קיום תהליך רישום, כמתבקש).

2. באמצעות בלדר - הנמנה על עובדי משרד. מותנה בכך ש"**הממונה**" בחן ואישר את כל פרטי תהליך זה, והכשיר את הבלדר לתפקידו (אישור מהימנותו וסדרי מסירה מאובטחת). במעמד מסירת הרשומה לנמען, יחתום הנמען על אישור קבלה ויחזירו לשולח.

3. באמצעות בלדר של "רשות-הדואר".

4. תהליך העברת דואר בסיווג "**חסוי-ביותר**" ע"י רשות-הדואר ייעשה ב - **דואר רשום <u>עם</u> <u>"אישור מסירה"</u> !**

5. אסורה לחלוטין העברת רשומות בסיווג "חסוי-ביותר" באמצעות קבלן ! **הממונה**" יתריע בפני **מנהל "היחידה"**, מבעוד מועד, על יוזמות מסוג זה).

6. א. במקרים אשר בהם נדרשת העברת רשומות בעלות חיסיון וחיוניות ברמה גבוהה (כגון: תיעוד ייחודי לצורך הצגתו בדיון בבית-המשפט, מידע אודות החלטות ופרוייקטים כלכליים ברמה מערכתית, בחינות בגרות וכד') - יידרשו להעברתם כל האמצעים הבאים:

1. מיכלים הניתנים לנעילה.
2. ליווי של אדם חמוש אשר ברשותו מכשיר טלפון נייד.
3. רכב ייעודי לליווי .
4. קביעת תוואי נסיעה אקראי בכל העברה.

ב. "**הממונה**" יודיע מבעוד מועד ל"**ממונה על הביטחון**" (קב"ט) על הצורך בהעברת רשומות בעלות חיוניות גבוהה או בסיווג "**חסוי-ביותר**". החל ממתן ההודעה הנ"ל יישא **הממונה על הביטחון (קב"ט)** באחריות להעברה מאובטחת של המידע, ממקום שמירתו במשרד השולח ועד למסירתו, אישית, לידי הגורם שמוסמך לקבלו ביעד. הממונה על הביטחון **(קב"ט)** יעדכן את "הממונה" אודות פעילויות אלה.

על גבי מעטפות המכילות רשומות נייר, או מצעי מידע אחרים (כגון: דיסקט, דיסק מגנטי, אופטי ואחר) אשר מסווגים בסיווג "**חסוי-ביותר**", או שהם **בעלי חיוניות ברמה הגבוהה** (מתוך השלוש הקיימות) תודבק על ידי השולח מדבקה בנוסח כדלהלן:

מדינת ישראל
דואר רשמי

<u>ח ס ו י - ביותר</u>

למסירה ביד או באמצעות רשות הדואר ב"**דואר רשום**" עם אישור מסירה

כל המוצא מעטפה זו מתבקש להעבירה לתחנת המשטרה הקרובה או למשרד ראש הממשלה

רשומה שסיווגה "**חסוי**" תועבר בארץ בשיטות ובאמצעים כדלהלן:

1. באמצעות "רשות הדואר" ע"י מכתב "**רשום**".
2. באמצעות הדרכים שצוינו לעיל בסעיף 35– א' 1 עד 3 (כולל).
3. על גבי מעטפות המכילות רשומות נייר, או מצעי מידע אחרים (כגון: דיסקט, דיסק מגנטי, אופטי ואח') בסיווג "**חסוי**" תודבק על ידי השולח מדבקה בנוסח כדלהלן:

מדינת ישראל
דואר רשמי

<u>ח ס ו י</u>

למסירה ביד או באמצעות "דואר רשום"

סייגים למשלוח דואר באמצעים אלקטרוניים
בשל הצורך בשמירת הסודיות/החיסיון והחיוניות של המידע האגור במערכות המידע של משרדי הממשלה ומוסדותיה, יש להקפיד על יישום הנחיות אלה:

א. העברת דואר המכיל מידע "**חסוי**" או "**חסוי-ביותר**" באמצעות תקשורת אלקטרונית (כגון: טלפון, פקס', מחשב ואח') - מותנית **בקבלת אישור מראש ובכתב מ"הממונה"**.

ב. הפרה של סעיף א' לעיל, עשויה להיחשב כעבירת משמעת חמורה. **תיוק (ידני או ממוחשב):**

א. רשומה שסיווגה "**חסוי**" או "**חסוי-ביותר**" תתויק באחת משתי הדרכים הבאות:
1) בתיק הנושא, ובתנאי שהתיק יסווג ע"י סוג הרגישות הגבוה ביותר של הרשומות בתיק
2) בתיק נפרד, כאשר אין הצדקה לסווג את התיק כולו בסוג רגישות גבוה. במקרה יוכנס לתיק הנושא "טופס מראה מקום".

ב. בעת השימוש בתיוק ממוחשב **יש להשתמש בתוכנה המחייבת סימון של רמת הסיווג** על גבי רשומות בסיווג "**חסוי**" ו-"**חסוי-ביותר**" והמאפשרת, בהמשך, יכולת טובה של איתורן ומעקב אחר הפצתן.

שימור, שמירה, אחזקה ונעילה של "רשומה רגישה":

א. כללית, אין להשאיר חדר-ביטחון, קופה או ארון, בלתי נעולים וללא השגחה של אחד העובדים, שאושרו לכך על ידי "**הממונה על אבטחת המידע**".

ב. רשומות נייר בלתי-מסווגות - בשל העובדה כי בגופים הציבוריים ישנן הרבה רשומות שאין להן רגישות של חיסיון ומאידך יש לרשומות הללו רמה מסוימת של חיוניות, יש להעדיף את שמירתן של כל הרשומות הקיימות במשרדי הממשלה ומוסדותיה בספריות, בתיקיונים או, בארכיבים, אשר תוכננו במיוחד או עוצבו למטרה זו מתוך שיקולים של אבטחה, בטיחות ושימור), למעט רשומות הנמצאות עתה בטיפול .

ג. כאמור לעיל, יתכן כי לרשומות הנ"ל, אין ערך של חיסיון, אך רגישותן נובעת מחיוניותן לניהול התפקיד וליישום יעדי המשרד, ובכדי למנוע תקלות בעבודה, כגון: היעלמות, אבדן, או השחתה (כוח עליון או בזדון), תיעשה שמירת הרשומות בשיטות ובתנאים שיהוו איזון בין חובתו האישית של העובד לשמור על הרשומות שברשותו, לבין הרצון להקל (במידת האפשר) על שגרת העבודה.

ד. להלן הנחיות אודות תנאי השימור של "רשומות רגישות":

1. הרשומות יאוחסנו בארון עץ נעול, או ארון פח נעול, כאשר דלת הכניסה לחדר העובד/ת נעולה, בכל עת שהוא נעדר ממנו.

2. יש לוודא נעילת חלונות בכל עת שבה אין פעילות במשרד.
3. יש לשמור על המסמכים/התיקים בגובה 30 ס"מ, לפחות, מעל הרצפה.
4. אין לאחסן רשומות בקרבת נורות ליבון, או ניאון, מתקן בעירה, מייחם מים או כל מקור חום אחר.
5. אין לאחסן רשומות בקרבת חומרים וכימיקלים דליקים, או מאכלים או בקרבת לוחות חשמל ראשיים, או בקרבת קווי מים ראשיים, מגופים, דודי הסקה וכיוצא בכך.
6. משך הזמן הנדרש **לשימור** כל רשומה יהיה לפי צרכי המשרד ובהתאם לחוק הארכיונים, התשט"ו- 1955

ה. שימור רשומות נייר בסיווג "חסוי" -
1. אחסון: יש לאחסן בארונות פח שעובי הפח יהיה **4** מילימטר, לפחות.או בארון מחוזק בחבקי ברזל, בעלי חתך של **0.8** X **4** סנטימטר, לפחות.
2. נעילה: יש להשתמש במנעול מסיבי אשר יאופיין ע"י "**הממונה על הביטחון** (קב"ט).

ו. שימור רשומות נייר בסיווג "חסוי-חיוני"
רשומות אלה יישמרו בתנאים הזהים לשמירת רשומות בסיווג "**חסוי-ביותר**"

ז. שימור רשומות נייר בסיווג "חסוי-ביותר" -
1. אחסון: בכספת או חדר בטחון אשר נבחנו ואושרו על ידי "**הממונה על הביטחון**".
2. נעילה: ע"י מנעול צירופים (קומבינציה) אשר יאושר ע"י "**הממונה על ביטחון**".

השאלת רשומות או תיקים והעברתם לעיון - חובת רישום :
א. רשומה או תיק, בסוג רגישות "**חסוי**", **או,** "**חסוי-ביותר**" באותו משרד או אתר, לעיון של עובד שאינו נמנה על עובדי המשרד, בעל הרשומה/התיק, יירשמו בעמודה המתאימה ביומן הדואר היוצא. ביומן יצוין גם שמו של העובד שקיבל את הרשומה לעיון. במקרה והרשומה או התיק לא חזרו תוך חודש ימים מיום המשלוח, יבקש המשרד השולח מהעובד להחזירם מיד.

ב. באם זקוק העובד להחזיק ברשומה/התיק תקופה נוספת, אחראי המשרד המשאיל לנהל מעקב חדש עד להחזרת הרשומה/התיק.

ג. הוחזרו הרשומה/התיק, יירשם הדבר בעמודת ההערות ביומן הרישום, ליד השורה בה רשמה העברת הרשומה/התיק לעיון.

ד. השאלת רשומות מסווגות כנ"ל מותרת **רק** לעובדים מוסמכים, אשר קיבלו הכשר מהימנות מתאים, באישור "**הממונה**".

הוצאת "רשומה רגישה" מהמשרד :

א. הוצאת רשומה/תיק שסיווגם: **"חיוני", "חסוי", או"-חסוי-ביותר"** אל מחוץ לכותלי המשרד (גם אם המקבל שייך לאותו משרד) שלא למטרת תפוצה ומשלוח, טעונה **אישור מראש** של הממונה הישיר, או מי שהוסמך על ידו.

ב. אישור לנטילת רשומות/תיקים כנ"ל מחוץ למשרד, אל בית העובד/או לצורכי עבודה לזמן מוגבל בלבד, יינתן **רק אם קיימים סידורי אבטחה נאותים**, שנבדקו ואושרו **מראש** על ידי "**הממונה**".

"הפשרת" רשומה רגישה -

א. **רמת הסיווג שנקבעה למידע אינה קבועה לעד**. ערך המידע לגורמים בלתי מוסמכים, או
הנזק הצפוי מחשיפתו, יכול להשתנות כעבור זמן ועקב שינוי בנסיבות. כתוצאה מתמורות אלו, ניתן, בדרך כלל, **"להפשיר"** את הסיווג, כלומר- להורידו מרמת "**חסוי-ביותר**" ל-"**חסוי**". חשוב לבדוק מחדש, מעת לעת, את רמות הסיווג שנקבעו למידע, במגמה "**להפשירן**".
ניתן גם לבצע פעולת "**<u>התרה</u>**", המאפשרת את חשיפת המידע לציבור, בתנאי שנתקיימו כל הכללים המתירים זאת.

ב. אם סוג הרגישות הגבוה יישאר מעל הצורך, תצטבר כמות גדולה של מידע שתחייב מאמץ אבטחתי ובעיקר לוגיסטי רב. תהליך זה המתווסף לנטייה האנושית להפריז בקביעת סוג הרגישות, מקשה על אבטחת הרשומות הראויות באמת לאבטחה מיוחדת, ומייקר לשווא את העלויות הנדרשות לאבטחת המידע.

ג. בדיקות חוזרות של סיווגים למידע "**חסוי-ביותר**" יש לבצע במשרד שייצר את הרשומה פעם בשנה, לפחות. באם לא נמצאה אפשרות "**להפשיר**" את סיווג הרשומה, היא תיבדק מחדש במועד הבדיקה החוזרת הבאה.

ד. "**הפשרת**" רמת סיווג - תיעשה ע"י הגורם אשר סיווג את הרשומה (משרד, מוסד, היחידה). כאשר המשרד או העובד המטפל ברשומה, מבקשים "להפשיר" את סיווג רגישותה, עליהם לפנות אל הגורם שסיווג את הרשומה, לשם קבלת אישורו.

ה. עד לקבלת האישור, תטופל הרשומה על פי סוג הרגישות שנקבע לה, על ידי מייצר רשומה.

ו. עובד המסווג רשומה אינו רשאי להורות על הורדת סוג הרגישות של רשומה בודדת, כל זמן שלא הורד סיווג הנושא אליו מתייחסת הרשומה (כגון: רמת סיווג הרגישות של פרוייקט כלכלי).

"התרת" "רשומה רגישה"

א. התרת רשומה **(לשם חשיפתה לציבור) תיבחן, בין היתר, על פי האמור בחוק הארכיונים, התשכ"ו- 1966, בחוק חופש המידע, התשנ"ח- 1998 וכל דין.**

ב. "התרת" רשומה מסווגת תיעשה רק לאחר ביצוע עיון ובחינת המידע, אף אם תמה תקופת חיסיונה, כאמור בחוק הארכיונים, התשכ"ז- 1966 (טור ב' בתוספת).

ג. "**הממונה על מסירת מידע לציבור**" (על פי החוק לחופש המידע, התשנ"ח - 1998, ייוועץ בממונה על אבטחת המידע הרגיש, בטרם יבצע "**התרת**" רשומה.

ביעור "רשומות רגישות" :

א. **<u>כללי</u>** - ביעור רשומות המסווגות ברמה "**חסוי**", או, "**חסוי-ביותר**" ייעשה על ידי עובדי המשרד בלבד, הבדוקים מהימנותית ע"י "**הממונה על הביטחון**") לרמת התיעוד. **פעילות הביעור כפופה בלעדית לאישור מוקדם של "הממונה על תיעוד רשומות" כ**י אין להן ערך מיוחד המחייב את שימור הרשומה !

ב. **ביעור רשומות בסיווג " בלמ"ס":** ניתן לפנות לשם מחזור, או, לבער בכל דרך משקית

הנראית למשרד/ארגון כמתאימה, לאחר קבלת **אישור מוקדם של "הממונה על תיעוד רשומות" כי** אין להן ערך מיוחד המחייב את שימורן, בהתאם לחוק הארכיונים, התשט"ו -1955 .

ג. ביעור רשומות בסיווג "חסוי":

1. גריסה - בעזרת מגרסה חשמלית. רוחב רצועת נייר גרוס לא יעלה על **2** מילימטר

2. **פינוי בעזרת קבלן** (שנבדק מהימנותית ע"י "**הממונה על הביטחון**"), ועפ"י הנחיות אבטחתיות משלימות, שיימסרו ע"י "**הממונה**".

ד. ביעור רשומות בסיווג "חסוי-ביותר"

1. גריסה במגרסה חשמלית, בשיטת "**שתי וערב**". גודלו המירבי של שבב נייר גרוס, לא יעלה על 3 X 3 מילימטר.

2. פינוי לביעור באמצעות קבלן (בדוק מהימנותית), על פי הנחיות משלימות של "**הממונה**".

אבטחת "תעודות רשמיות" :

א. מהימנות העוסקים בתיעוד

בכל שלבי הטיפול בתעודה ממלכתית, יועסקו רק עובדים אשר נבדקו מהימנותית על ידי "הממונה על הביטחון (קב"ט)", לפני וכתנאי להעסקה.

ב. אחסון התיעוד

תעודות רשמיות יאוחסנו בכספות חסינות אש, או בחדרי בטחון באופן שיימנע מגורמי - חוץ או עובדי המשרד שלא הותרו לכך, גישה לתיעוד. קביעת התקנים הטכניים תיעשה ע"י "**הממונה על הביטחון**" (קב"ט) בהתאם לנוהל זה.

ג. אבטחת ייצור התיעוד

הממונה הארצי על הביטחון (קב"ט) אחראי ליצירת "סביבה סטרילית" שבה לא תתאפשר קירבה פיזית בין עובדים שאינם נמנים על יוצרי תיעוד מהימנים לבין עובדים אחרים של המשרד, קהל, או נותני שירות, לבין : 1. חומרים להכנת התעודות, 2. תעודות מוכנות 3. מערכי רישום והדפסה ידניים או ממוחשבים המשמשים להפקת תעודות רשמיות.

ד. אמצעי בקרה אלקטרוניים

שמירת תהליך הייצור בכלל זה חומרי הגלם ותעודות בכל שלב, טרם הנפקתם תאובטח גם באמצעי בקרה אלקטרוניים שיקשו מאד או ימנעו כליל אפשרות לקחת התעודות ללא רשות, או לגניבת גלופה, חומר גלם או תעודה מוכנה, וכל ניסיון לביצוע מעשים אלה תינתן אות אזעקה רועשת. הממונה יפעל עפ"י נהלים משלימים שיימצאו בידיו .

ה. ספירה ורישום התעודות

1. יש לנהל רישום (ספירה ובדיקת התאמת כמויות) בכל שלב שבו מועברות התעודות אל מחוץ לאתר וכן בתחילה ובסוף כל יום עבודה. הרישום יתייחס גם לצרור תעודות כאמור בסעיף ה' להלן.

2. כל אי-התאמה בכמויות תחשב כ"אירוע חריג" המחייב דיווח מיידי לגורמים שייקבעו, ול"ממונה".

ו. אריזת התעודות למשלוח

התעודות ייארזו במעטפות חתומות וסגירתן תיעשה על רק ידי גורם מוסמך במשרד תוך הטבעת סמל של משרד הפנים ולצידו מספור סידרתי. פתיחת המעטפה תחייב את קריעתה ובכך יתאפשר זיהוי אמין ומהיר כי המעטפה פתוחה ויש צורך לספור את כל התעודות שבמעטפה, במועדים שנקבעו.

ז. שינוע התעודות

1. "**תעודות רשמיות**" ישונעו על ידי עובדי המשרד שנבדקו מהימנותית ע"י "**הממונה על הביטחון**" (קב"ט). רכב ההובלה יהיה ממוגן כנגד פריצה, ע"י סירוג מסיבי של חלונותיו ונעילה

מסיבית של דלתותיו וכן יישומו הנחיות משלימות של **הממונה**״

2. רכב ההובלה יהיה מאויש על ידי מאבטח חמוש (חימושו יהיה באחריות הממונה על הביטחון) ויפוקח, ב״קשר- עין״, בכל משך הזמן שבין תחילת ההעמסה לבין הפריקה ביעד שנקבע, למניעת טיפול שלא הותר או פגיעה מכל סוג שהוא בתעודות.

3. על המאבטח מוטלת חובה אישית לבחון לעיתים קרובות את שלמות האריזה ולציין ביומן את תוצאות בדיקתו. יומן זה יבוקר שבועית, על ידי נציג הממונה על הביטחון. סימני פגיעה באריזה, או חוסר בפועל ידווחו מיידית לממונה הישיר.

ז. סמכות מינהלית לביעור

בעל הסמכות היחיד במשרדי הממשלה ומוסדותיה, הרשאי להתיר ביעור של תעודות רשמיות במשרדי הממשלה מוסדותיה הינו ״**הממונה על התיעוד והרשומות**״, הפועל בהתאם לחוק הארכיונים, התשט״ו - 1955, והנחיות משלימות של גנז המדינה.

ח. תהליך הביעור

1. ביעור ״**תעודות רשמיות**״ ייעשה בתנאים מבוקרים אשר יבטיחו כי לא יוותרו שאריות ניירת וגלופות פגומים ללא השגחה, תוך ביצוע רישום מדויק לאימות כמויות הפריטים שבוערו.

2. הביעור ייערך בנוכחות ״**הממונה**״ או נציג מוסמך מטעמו. ראה: סעיף 44 להלן.

ט. דיווח

כל אירוע חריג במהלך הטיפול ב״תעודה רשמית״ ידווח **<u>מיידית</u>** ל״ממונה״ (או ל״ממונה על הביטחון״ קב״ט), ולמנהל המשרד.

להלן לקט נושאים המוגדרים כ**מידע- רגיש,** אשר בד״כ ייחשבו כמידע ״**בלתי -מסווג**״

א. מידע אודות פעילויות תרבות והשכלה במשרדים.

ב. מידע אודות תוצאות מכרז, בשלב שנקבע כפומבי, ובלבד שאינו מכיל פרטים חסויים הנוגעים לצנעת מגיש ההצעה, פרט או ארגון.

ג. נושאי מדיניות אשר הנהלת המשרד אישרה את פרסומם.

לנושאים הנ״ל אין רגישות מהיבטי חיסיון, אך עשויה להיות להם רגישות של **חיוניות** (זמינות, שלמות, ואמינות) לניהול הארגון ומשק המדינה, הדורשים אבטחה הולמת.

להלן לקט נושאים המוגדרים כ- ״**מידע -רגיש**״ והמצדיקים, בדרך כלל, את סיווגם בסיווג ״**חסוי**״ (רמת סיווג אמצעית):

א. שלבים לא פומביים במשא ומתן בין משרדי הממשלה או גופים ציבוריים אחרים ושלוחותיהם, לבין גורם אחר.

ב. שלבים לא פומביים של ועדות משרדיות.

ג. מידע על פעילות משרדי הממשלה וגופים ציבוריים שפרסומו עלול לעיכוב פעילותם לייקור העלויות של הגופים, או לפגיעה במחויבויותיהם לתאגידים או לפרטים.

ד. דו״חות של משרדי הממשלה ומוסדותיה, או, של וועדות ממשלתיות שהנהלות הגופים החליטו שאין לפרסמם.

ה. מידע אודות מדיניות הנמצאת בשלבי עיצוב, דיונים פנימיים או ניהול פנימי של גופים-ציבוריים,
לרבות חוות-דעת, תחקיר פנימי, טיוטה, עצה, המלצה, אשר ניתנו לצורך קבלת החלטה וכן תרשומות.

ו. מידע המוגן על ידי החוק להגנת הפרטיות, התשמ״א- 1981 והמוגדר בחוק זה כ- ״**מידע-רגיש**״ או, ״**מידע מוגבל**״, כמשמעם בחוק הנ״ל, אך למעט הנושאים האלה: אימוצים, בריאות הנפש, מחלות מין ומחלת האיידס.

ז. מידע החייב בשמירה על פי כל דין.

ח. מידע אודות השיטות והכלים לאבטחת מידע ״**חסוי**״.

להלן לקט נושאים המוגדרים כ״**מידע-רגיש**״ והמצדיקים, בדרך כלל, את סיווגם בסיווג ״**חסוי-ביותר**״:

א. תוכניות, פעולות ואמצעים כלכליים ומסחריים שיש להם ערך מכריע לניהול התקין של המדינה, ובכלל זה: מקורות המימון וקניות הגומלין של המדינה.

ב. נושאי מחקר, פיתוח וייצור של התעשייה האזרחית בישראל אשר נמסרו לממשלה, מרצון, או כחובה, או שנמצאים בידי הגופים הציבוריים.

ג. תוכניות פעולה ופרטים בנושא רכש כלכלי-מסחרי [לא בטחוני] החיוניים למדינה.

ד. תוכניות לשינויים מכריעים במדיניות הכלכלית של מדינת ישראל.

ה. מידע אודות הכלים והשיטות לאבטחת מידע "**חסוי-ביותר**".

ו. מידע אשר נמסר לממשלה על ידי מודיעים ואשר פרסומו או פרסום מקורות המידע עלול לפגוע בהמשך קבלת המידע (מידע הנמסר על ידי מודיעים לרשויות אכיפת החוק).

ז. מידע בנושאים: אימוצים, בריאות הנפש, מגפות, מחלות מין ומחלת האיידס, המוגן על ידי החוק להגנת הפרטיות, התשמ"א- 1981.

ח. מידע הנוגע למשק **החשמל, הדלק, הגז, המים והתחבורה** (היבשתית והאווירית), אודות: השיטות והכלים הקיימים והמתוכננים לאבטחת המידע ולשמירת חיוניות מערכי המידע, ובכלל זה סדרי אבטחת מערכות השליטה והבקרה בגופים הללו.

ט. מידע אודות תהליכי הרכש, ההובלה והשימור, הנעשים על ידי הממשלה או גוף מטעמה, של מלאי **לשעת חירום**, כגון: תרופות, מזון, דגנים ואחר.

מקורות

נהלי מסגרת – אבטחת מידע רגיש ומערכות מידע. משרד ראש הממשלה, אגף בכיר לביקורת המדינה וביקורת פנימית, מאי 2000.

שימור רשומות אלקטרוניות

נוהל מס׳ 25 (בהכנה)

החלטת ממשלה בק/54 - 29 למארס 2004

א. צוות בהרכב: מנהל האגף לביקורת המדינה במשרד ראש הממשלה (מרכז), גנז המדינה ונציג החשב הכללי במשרד האוצר, יגבש הנחיות מחייבות ברמה הטכנולוגית והארגונית, כדי לאפשר שימורן של רשומות אלקטרוניות הנוצרות על-ידי רשויות המדינה, ולהבטיח גישה אליהן לאורך זמן.

ב. ההנחיות יוטמעו בפרוייקטים רוחביים של מחשוב הממשלה, בכל משרדי הממשלה.

ג. הצוות יבחן את נושא היקף הרשומות האלקטרוניות, שהצטברו בידי משרדי הממשלה השונים במהלך השנים, ונמצאות בסכנת הכחדה בגלל חוסר טיפול נאות, ויגבש תכנית לפעולה מקיפה להצלת רשומות אלה.

ד. הצוות ידווח לוועדת השרים, בתוך שלושה חודשים, על ההתקדמות.

ה. הערות מבקר המדינה בדו״ח 54ב׳ יובאו בחשבון בעת ביצוע ההחלטה.

ו. דיווח יימסר לאגף לביקורת המדינה במשרד ראש הממשלה.

ביצוע החלטה

א. בהמשך להחלטה, התכנס הצוות שמונה על ידי הממשלה לארבע ישיבות.
כדי לאפשר שימור מיידי, הוציא האגף הבכיר לביקורת המדינה מספר ״נהלי הצלה״ כדלקמן.

הנחיות נדונו בישיבות המועצה המייעצת לביקורת מערכות ממוחשבות ואבטחת מידע בתאריכים 07.12.2004 ו-18.01.2005, והועברו גם להערות מנהלי מערכות מידע במשרדי הממשלה וגופים ממשלתיים עפ״י המלצת המועצה.

״נהלי הצלה״ לשימור רשומות אלקטרוניות

נוהל הצלה מספר 1
הנחיות בסיסיות לתחזוקה של אמצעים אופטיים - CD / DVD

עשה:

1. אחוז את התקליטור בשוליו או במרכזו – בחור.
2. יש לכתוב על התקליטור אך ורק בחומר שאינו SOLVENT.
3. שמור על התקליטור נקי, הרחק אותו מסביבה מזהמת.
4. שמור על התקליטור בתוך קופסא מפלסטיק, מיוחדת לשמירה על תקליטור, במצב מאונך, בדומה לספר על מדף.
5. החזר את התקליטור לקופסאות האחסון, מיד לאחר השימוש.
6. פתח קופסא של RECORDABLE DISK רק כאשר הנך מוכן להקליט את המידע.
7. שמור את התקליטורים במקום אפל, קריר, יבש ונקי.
8. יש לנקות תקליטור באמצעות צמר גפן או מטלית בתנועות ישרות, ממרכז התקליטור אל שוליו. חשוב להרחיק מעל התקליטור סימני שומן, טביעות אצבע ורטיבות.
9. ניתן להשתמש בחומרים הר״מ לניקוי הדיסק:
ISOPROPYL ALCOHOL , CD/DVD CLEANING DETERGENT ,METHANOL
10. יש לבדוק את שלמות הציפוי של התקליטור לפני ההקלטה.

אל תעשה

1. לא לגעת בפני התקליטור.
2. לא לקמט את התקליטור.
3. לא להניח תקליטורים המיועדים לאחסון לטווח ארוך, במשך שנים, במצב אופקי.
4. לא להשתמש במדבקות.
5. לא לפתוח קופסאות של תקליטורים RECORDABLE OPTICAL DISCS לפני שהנך מוכן להקלטה.
6. לא לחשוף תקליטור לחום או ללחות.
7. לא להעביר באופן פתאומי תקליטור מטמפרטורה גבוהה לנמוכה, וההפך.
8. אין לחשוף תקליטור למשך זמן רב לאור שמש ולמקור של אור אולטרה סגול.
9. לא לכתוב על השטח המיועד להקלטה של התקליטור.
10. לא לנקות את התקליטור בתנועות סיבוביות.

הנחיות שמירה לטווח ארוך של תקליטורים CD ו-DVD

טמפרטורה לשמירה על מדיות לטווח ארוך תהיה בערכים 4 – 20 מעלות צלסיוס, ובלחות יחסית 20% - 50%.

עפ"י תקן מכון התקנים של ארה"ב NIST 2003.

נוהל הצלה מספר 2
קביעת שם המסמך

בקביעת שם המסמך, לצורכי השמירה והאחזור, יש להקפיד על מבנה אחיד, כדלקמן:

מימין לשמאל:
1. שם פרטי ושם משפחה מלא של מחבר המסמך.
2. תאריך מלא של יצירת המסמך, במבנה DDMMYYYY.
3. שם פרטי ושם משפחה מלא של הנמען.
4. שם המסמך, כפי שמופיע בשורת "הנדון" שבסמך.

סה"כ אורך רשומת שם המסמך עד 234 תווים. תו יכול להיות אות, ספרה, או רווח.

דוגמה לשם רשומה אלקטרונית: יצחק בן אברהם 18032005 יוסי בן נח הצעת תקציב .

שם השולח	תאריך	שם המקבל	הנדון

השדות: שם השולח, שם המקבל, והנדון, יכולים להופיע בעברית או בלע"ז.

מבוסס על נהלי NARA - National Archives and Records Administration, USA

נוהל הצלה מספר 3
שימור דואר אלקטרוני

כללי

רשומות דואר אלקטרוני בהנחיה זו, הינן הודעות המועברות בין מחשבים באמצעות האינטרנט, ויש לשמור אותן משום ערכן.

מטרה

שימור רשומות דואר אלקטרוני משרדי, במתכונת שתאפשר ניהולן ואיחזורן.

חלות ההנחיה

על כל המשתמשים בדואר האלקטרוני המשרדי.

הגדרות

דואר אלקטרוני: מסר שנוצר, נשלח או התקבל במערכת הדואר האלקטרוני המשרדי, כולל צירופים (ATTACHMENTS), אישורי קבלה ואסמכתאות.

צירופים: מסמכים נספחים, המועברים עם הדואר האלקטרוני, כגון: מסמכי טקסט, גיליונות חישובים, קבצי קול, קבצי גרפיקה, קישורים, תמונות, ועוד. הצירופים מהווים חלק מרשומת הדואר האלקטרוני.

אסמכתאות: נתוני משלוח וקבלה, הכוללים את פרטי השולח, המקבל, העתקים לפעולה, העתקים לידיעה, נושא הרשומה, תאריך ושעת המשלוח, ועוד.

אופן שמירה של דואר אלקטרוני

א. ספריות: יש לפתוח שתי ספריות על ה-DESKTOP, אחת לדואר אלקטרוני נכנס, ואחת לדואר אלקטרוני יוצא. יש להעתיק את הדואר לשתי ספריות אלה, מידי יום, כולל הצירופים. בנוסף יש לשמור את המסרים בספריות המתאימות במחשב, על ידי גרירה מה-OUTLOOK לספריות הייעודיות שנפתחו.

ב. שם הרשומה: בנדון (SUBJECT) של כל מסר, יופיעו מעתה: שם משפחה ופרטי של מחבר המסמך; תאריך יצירת המסמך, במבנה YYYYMMDD; שם משפחה ופרטי של הנמען, ונושא המסמך.

ג. רשומות שחובה לשמור: מסרים, הנוצרים או מתקבלים ביחידה, שעניינם משימות היחידה, כולל: מידע ממקורות חיצוניים המהוה חלק מרשומה יחידתית; לוחות זמנים; סדרי יום וסיכומי ישיבות; המלצות; דוחות סופיים, וכל מסמך אחר הרלבנטי לפעילות היחידה.

ד. רשומות שאין חובה לשמור: טיוטות ביניים שאין חשיבות לתיעודן; מידע מרשימות תפוצה חיצוניות; מידע אישי; הודעות ופרסומות. במקרה של ספק, עדיף לשמור, ולא למחוק!

ה. משך שמירת רשומות דואר אלקטרוני וצרופות: הכללים החלים על שמירת רשומות נייר משרדיות וביעורן, חלים גם על רשומות הדואר האלקטרוני וצרופותיו.

במגמה להקטין את אחריות המשתמש לגיבוי, תוטל האחריות לגיבוי הדואר האלקטרוני על מנהל מערכות המידע, הממונה על תחזוקת שרתי הדואר.
במידה ואין ביחידה שרתי דואר, תוטל האחריות לגיבוי על המשתמשים, עד להתקנת שרת דואר ביחידה.

מבוסס על נהלי Government of British Columbia, Canada, ונהלי National Archives of Australia

נוהל הצלה מספר 4
שמירת סטטוס של פורטל - אתרי אינטרנט ממשלתיים

מטרה
תיעוד סטטוס של פורטל שהינה רשומה אלקטרונית.

אתרים שישמרו
האתרים שישמרו הם אלה הנגישים לציבור, בין אם בניהול ישיר של המשרד, או במיקור חוץ (OUTSOURCING). אין הכוונה לאתרים פנימיים או לאינטרא-נט.

מיפרט
תיעוד הסטטוס של הפורטל יכלול את כל המסמכים הזמינים לציבור מהאתר, והנמצאים בשרת של האתר.

אם האתר או המסמכים מתעדכנים באופן דינמי, מבסיס נתונים, יש לציין זאת במסמך השימור, אולם אין צורך לצרף את בסיס הנתונים.

אופן השמירה
שמירת הסטטוס של הפורטל אינה מהווה תחליף לגיבוי האתר, אך צריכה להיות בתצורה הניתנת לקריאה במחשבים אחרים.
שמירת האתר תתבצע על ידי הפקודה "שמירה בשם" מתפריט קובץ, לספריה ייעודית. את תמונת הסטטוס מהספרייה הייעודית יש לצרוב לאחר מכן על תקליטור. ביחד עם התקליטור יש לשמור תדפיסים של האתר ורשימת הקבצים המצורפים לו, מידע על חומרה או תוכנה קנייניות שבאתר, כגון תוכנות למעקב אחר החלטות, הדרושות לשחזור האתר, ומידע לזיהוי התצורה של כל קובץ הכלול בתמונת המצב.

פעולות הכנה
לפני שמירת הסטטוס של הפורטל, יש לוודא קיום גיבוי לאתר, וכי נרשמו הקישורים (LINKS) לאתרים חיצוניים ולקבצים במסמך השימור.

מבוסס על נהלי NARA - National Archives and Records Administration, USA

נוהל הצלה מספר 5
שימור סרטים מגנטיים

כללי

בשירות המדינה קיימים סרטים מגנטים למחשבי MAIN FRAME ומיני מחשבים, לעבודה ולגיבוי. הנוהל יפרט שיטת גיבוי לסרטים המגנטים, שתאפשר אחזור הנתונים שעליהם.

מטרה

ניהול, שימור ואחזור יעיל ומהיר, של הנתונים על גבי סרטים מגנטים.

מיפרט

יש לפתוח ספריה ייעודית במחשב, ולהעתיק לתוכה את תוכן הסרט המגנטי, אחד לאחד: כל בית, גוש (BLOCK) ו-FILEMARK. יש להשתמש בשם הסרט הקיים כשם קובץ הגיבוי, בסיומת TAP.; למשל: BINUY-6.TAP.

לאימות ההעתקה למחשב, יש להכין דוח, המפרט את מספר הבתים, הגושים וה-FILEMARKS. שם הדוח יהיה כשם הגיבוי, בסיומת DOC. ; למשל: BINUY-6.DOC.

את שני הקבצים, ה-TAP וה-DOC, יש לכווץ (ZIP) לקובץ אחד, ולצרבו על תקליטור או DVD. תווית התקליטור/DVD תכיל את שם הסרט השמור, ומהות הנתונים בו.

בתקליטור/DVD יש לאחסן ולטפל כאמור בהנחיות לתחזוקה של אמצעים אופטיים - נוהל הצלה מספר 1: הנחיות בסיסיות לתחזוקה של של תקליטורים CD ו-DVD.

מבוסס על נהלי NARA - National Archives and Records Administration, USA

ביעור רשומות

נוהל מס׳ 26

מטרות הנוהל

הסדרת תהליך ביעור רשומות בהתאם לחוק ולתקנות.
הרשומות הן באחריות המחלקה שבמסגרת עבודתה נוצרו או התקבלו. השמירה והביעור ייעשו על פי רמות הסיווג ובהתאם לכללים המפורטים בקובץ נהלים זה.
לפי סעיף 12 לחוק הארכיונים ותקנותיו: ״לא יבוער במוסד ממוסדות המדינה או ברשות מקומית חומר ארכיוני (רשומות), אלא בהתאם לתקנות״. נוהל זה עוסק בדרכי איתור הרשומות, בתהליך קבלת אישור לביעורן ובביצוע הביעור.

הגדרות

רשומות – חומר ארכיוני במחשב ואחר, כגון: כל כתב על גבי נייר או על גבי חומר אחר וכל תרשים, דיאגרמה, מפה, ציור, תיק, תצלום סרט, תקליט, קלטת, תקליטור, דיסקט וכיוצא באלה, המצויים ברשותו של מוסד ממוסדות המדינה, דהיינו, ביחידה מיחידות המשרד.

גנזך – ארכיון מדינת ישראל.

הגנז – מנהל הגנזך, לרבות כל אדם שהגנז ייפה את כוחו לפעול בשמו או במקומו.

אחראי לניהול רשומות – עובד המשרד, שאחד מתפקידיו לבדוק את רשימות הרשומות לביעור, לאשרן ולהעבירן לאישור הגנז, ולהודיע על אישור הביעור ליחידה המבקשת.

ביעור רשומות – השמדת רשומות, ע״י גריסה / שריפה / מסירה לחברה בעלת זיכיון לפינוי ולגריסת פסולת נייר ממשרד הממשלה, כפי שמתפרסם בהוראות תכ״ם מעת לעת. הגריסה תתבצע במגרסה לפי תקן.

תעודות שגרתיות – תיקים ומסמכים שתקופת החזקתן נקבעה בתקנות (כגון: מסמכים בנושא כספים, אפסנאות ומשק, ענייני עובדים וכו׳).

הודעה על ביעור תעודות שגרתיות (מדף 1365) טופס שנועד להשגת הודעה לגנז המדינה על ביעור רשומות שתקופת החזקתן נקבעה בתקנות.

אחראי לביצוע הנוהל

אחראי לניהול רשומות של המשרד.

גוף הנוהל

ביעור שוטף של רשומות ביחידות המשרד

א. הרשומות המפורטות להלן תבוערנה (ע״י קריעה או גריסה) באופן שוטף: טיוטות למכתבים שנשלחו, העתקים עודפים, פקסים שצולמו, פלטי מחשב עודפים. הרשומות תיגרסנה בנוכחות עובדי היחידה בעלת הרשומות.
ב. במקום שאין מגרסות, על האחראים לקרוע את הרשומות המיועדות לגריסה. אין להשליך את הרשומות בשלמותן לסל אשפה או לשק לאיסוף פסולת נייר.
ג. עם השלמת פעולת הגריסה (או קריעת הרשומות), יש להעביר את שרידי הרשומות שנגרסו לשקים המיועדים לפינוי כפסולת נייר לחברה שזכתה במכרז לפינוי פסולת נייר מכל משרדי הממשלה.
ד. רשומות לא מסווגות תועברנה מידי יום למתקנים המיוחדים לאיסוף פסולת נייר ללא גריסה.

הכנה לביעור שנתי של רשומות ביחידות המשרד

א. אחת לשנה ישלח האחראי לניהול רשומות, לכל יחידות המשרד רשימה מעודכנת של "תעודות שגרתיות", שרשאית כל יחידה לבעור בשנה זו. כמו כן, יביא לידיעת היחידה את שם החברה בעלת הזיכיון לאיסוף ולגריסת פסולת הנייר, כתובתה ואופן ההתקשרות אליה.

ב. לאחר שמנהל היחידה יקבל את רשימת ה"תעודות שגרתיות", יטיל על עובד היחידה להכין רשימה של כל תעודות שגרתיות שהגיע מועד ביעורן. בבקשה יצוינו נושא, תקופה (מ- עד-), וכמות הרשומות המיועדות לביעור.

ג. נתקלה היחידה בקשיים בקביעת הרשומות לביעור, למרות ההוראות שקיבלה, תתייעץ עם האחראי לניהול רשומות, כדי לקבוע אילו רשומות ניתנות לביעור.

ד. לאחר שסיימה היחידה לרשום את פרטי הרשומות, תשלח את הרשימה לאחראי לניהול רשומות במשרד הראשי. על הבקשה יחתום מנהל היחידה, שבתחום אחריותו נוהלו התיקים.

ה. בהגיע הבקשה לאישור ביעור תעודות שגרתיות, יבדוק האחראי לניהול רשומות את נושאי התעודות ואת כפיפותם לתקנות חוק הארכיונים.

ו. אם מצא האחראי לניהול רשומות, כי לא את כל הרשומות ניתן לבער, יודיע על כך בכתב ליחידה המבקשת.

ז. אם מצא האחראי לניהול רשומות המפורטות ברשימה, רובן או חלקן ניתנות לביעור, ימלא טופס הודעה על ביעור וישלח את ההעתקים מספר 1,2,3 של טפסי ההודעה על ביעור תעודות שגרתיות לארכיון המדינה.

ח. לא נתקבלה התנגדות מהגנז בתוך שלושים יום, יראה בכך האחראי לניהול רשומות אישור לביעור. אם התקבל אישור עם ציון התאריך לביעור, ימתין האחראי לרשומות למועד המצוין.

ט. בהגיע מועד הביעור, יודיע האחראי לרשומות למנהל היחידה שביקש את הביעור. ההודעה תכלול:

(1) המועד המאושר לביצוע הביעור

(2) הנחיות לביצוע הביעור

(3) הוראה לכתוב פרוטוקול, המאשר את ביצוע הביעור, שייחתם ע"י מנהל היחידה או ע"י גורם מוסמך אחר, שהיה נוכח בעת הביעור.

י. הפרוטוקול המאשר את ביעור הרשומות, יישלח לאחראי/ת על הרשומות.

ביעור רשומות ע"י העברתן למפעלי נייר

א. על פי תקנות חוק הארכיונים, יש לבער רק רשומות שתקופת החזקתן ותהליך ביעורן נקבעו בתקנות.

ב. נציגי מחלקות הבנא"ם, במחוזות ובמשרד הראשי, ידריכו את העובדים בהוראות המחייבות, בכל הנוגע לארגון ומיון פסולת נייר, המיועדת לפינוי ולגריסה ע"י החברה בעלת הזיכיון.

ג. החברה בעלת הזיכיון תוזמן ע"י הגורם האחראי לפינוי הרשומות כמפורט לעיל.

ד. ביעור רשומות מסווגות שנגרסו ושל רשומות לא מסווגות שרוכזו בשקים המיוחדים לשם העברתם לחברה בעלת הזיכיון יתבצע כדלהלן:

(1) כל יחידה תנקוט באמצעים הדרושים, לשם הפרדה מסודרת בין פסולת רגילה לבין מסמכים המיועדים לביעור שוטף. באמצעות החברה בעלת הזיכיון לאיסוף ולגריסת פסולת נייר.

(2) הרשומות השוטפות (כפי שהוגדרו לעיל), תאוחסנה בשקים סגורים (קשורים בחבל). קשירת השקים תתבצע מיד עם התמלאותם ותהיה באחריות המשרד לפני הפינוי ל"מקום פינוי מרוכז" ולפני הפינוי ע"י החברה בעלת הזיכיון.

(3) השקים ירוכזו באחריות מחלקת בנא"ם במקום מיוחד.

(4) את השקים הסגורים, בהם הרשומות המיועדות לפינוי, ילווה נציג המשרד.

ה. פינוי הרשומות ייעשה כדלהלן –

(1) רשומות לא מסווגות, או מסווגות שנגרסו ביחידה בה נוצרו, תועברנה בהעברה שגרתית של החברה בעלת הזיכיון, ברכב סגור של החברה בעלת הזיכיון.

(2) כדי להבטיח העברה נאותה של רשומות מסווגות, שלא נגרסו, תועבר לחברה בעלת הזיכיון, בקשה בכתב לסדרי העברת חומר מסווג. החברה תשלח רכב מיוחד סגור להעברת רשומות מסווגות. ההעברה והגריסה, מתחילתן ועד סופן, תלווה ע"י נציג המשרד.

ביעור רשומות ממגנזות המשרד

א. על פי תקנות חוק הארכיונים, יש לבער רק רשומות שתקופת החזקתן ותהליך ביעורן נקבעו בתקנות.

ב. מנהלי המגנזות לא יבערו רשומות כלשהן, ללא קבלת אישור ממחלקה שגנזה את הרשומות ומהאחראי/ת לניהול הרשומות.

ג. עם קבלת אישור לביעור הרשומות (כל רשומות המגנזה נחשבות מסווגות לצורך העברה), יודיע האחראי לרשומות על הצורך בהיערכות לקראת ביעור במרוכז מהמגנזה:

- למנהל המגנזה
- לקב"ט המחוזי
- למנהל בנא"ם המקומי
- לחברה בעלת הזיכיון לאיסוף נייר – הפניה לחברה תיעשה על גבי טופס מיוחד, בו יידרש רכב מיוחד סגור, המיועד לפינוי רשומות מסווגות, ותידרש שיטת פינוי מיוחדת ומאובטחת לאורך כל הדרך.

ד. מנהל המגנזה, או עובד אחר שיוסמך לכך, ילווה את פינוי הרשומות. המלווה יקפיד על נוכחות צמודה, מתחילת הפינוי, מתוך המגנזה, ועד לסיום גריסת הרשומות, במתקני הגריסה של החברה בעלת הזיכיון.

ה. בכל מקרה של ביעור תקופתי של רשומות במגנזות, יינתן תדרוך לכל הגורמים השותפים לתהליך. הקב"ט המחוזי ייתן הדרכה בנהלי אבטחה, האחראי על הרשומות ייתן הדרכה בנהלי ביעור. מנהל בנא"ם יהיה שותף לתהליך הפינוי וההעברה.

מקורות

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

חוק הארכיונים ותקנותיו.

תכ"ם: איסוף פסולת נייר, פרק 9.

סיכוני אש, חשמל ומים בחדר המחשב

נוהל מס' 27

מטרות הנוהל

להגן על המחשבים האישיים והציוד ההיקפי מפני מפגעים פיזיים.

אחראי לביצוע הנוהל

ממונה אבטחת מידע ואחראי על כיבוי אש יגדירו, יטמיעו ויבקרו, כל אחד בתחומו, את יישום הנחיות נוהל זה.
משתמשי המחשב ומנהל יחידת המחשב יישאו באחריות ביצוע הנחיות הנוהל.
ייזום הפעילויות הנזכרות בנוהל זה ייעשה ע"י מנהל מתקן מחשב.

גוף הנוהל

חיבור מחשב ו/או יחידה היקפית (מדפסת, כונן חיצוני, "אל פסק" וכדומה) לחשמל ייעשה אך ורק בצורה תקנית .

כל מחשב-שרת ומחשבים שעליהם בסיס נתונים של יישום "חסוי ביותר" או "חסוי" (בתנאי שנפח הנתונים של יישום זה הנו 15 מגה לפחות), יצוידו ביחידת אל פסק.

המחשב המרכזי יהיה מחובר אל מקור המתח, באמצעות יחידת UPS מסוג on line. פעם בשנה יש להזמין בדיקת תקינות מטעם ספק ה-UPS, לגבי תקינות יחידה זו.

יש להרחיק את המחשב האישי מן הקיר למרחק של 15 ס"מ לפחות, בכדי שלא לחסום האוורור.
מחשבים הניצבים על הרצפה יוצבו על משטח מוגבה יציב בגובה של 10 ס"מ לפחות. זאת כדי למנוע פגיעת רטיבות ונוזלים.

אין להניח חפצים על המחשב או על הצג שלו.

אין להביא נוזלים כלשהם לקרבת המחשב, באופן שעלולים להישפך או לסכן את המחשב. יש להיזהר במיוחד מפגיעה במקלדת. חל איסור על ניקוי המחשבים/המדפסות בנוזלים.

מחשבים יוצבו, במידת האפשר, בחדרים סגורים, הניתנים לנעילה.

בחדר המחשב המרכזי יוצבו לפחות 5 מטפי גז הלון 3 ק"ג, בנקודות שיקבעו ע"י האחראי על הבטיחות.

ליד כל ריכוז של ציוד הכולל 6 פריטים (מחשבים ו/או מדפסות) ומעלה, ברדיוס של עד 5 מטרים, יוצף מטף הלון 3 ק"ג. המטף יוצב במרחק שלא יעלה על 10 מטרים מריכוז הציוד הנ"ל.
בכל מקרה, יש להציב מטף שכזה בכל מבנה נפרד, גם אם מצבת הציוד קטנה מן הכמות האמורה.

בתוך חדר השרתים, וכן ליד הדלת מחוץ לחדר המחשב המרכזי, ליד ארון התקשורת, וליד המצעים המגנטיים, יוצבו מטפי גז הלון 5 ק"ג כל אחד.

פעם בשנה תתבצע בדיקת תקינות המטפים, כמו גם בדיקתה של מערכת הכיבוי המרכזית, מטעם החברות המספקות שירותים אלה. פעילות זו תתבצע בתיאום ובאחריות מחלקת בנא"ם. פעם בשנה לפחות יערך תדרוך התנהגות במקרי שריפה, והפעלת אמצעי הכיבוי, לכל העובדים במקום. לצורך זה יוזמן גורם מוסמך ומורשה בתחום זה. התרגול יכלול שימוש בפתחי מילוט שיקבעו מראש ויסומנו. פעילות זו תתבצע באחריות האחראי לכיבוי אש. תרגול של הפעלת אמצעי הכיבוי יערך באחריות האחראי על כיבוי אש, ובהתאם להנחיות המחייבות.

בחדר המחשב המרכזי ייאסר העישון ויוצבו שלטים בהתאם.

כל פעולת בינוי במבנה בו יאוחסן מחשב מרכזי או אמצעי קלט/פלט, תיעשה מחומרים הולמים על פי התקנים הישראלים הרלבנטיים. אחת לשנתיים יזמן האחראי על כיבוי אש, מומחה בטיחות אש לבדיקה כוללת.

כל חיבורי המחשבים והמדפסות אל מקור המתח ייעשו דרך יחידות לקטיעת הזדקרויות מתח.

כל יציאה של קו תקשורת נתונים אל מחוץ לקירות החיצוניים, תוגן באמצעות כולא ברקים. אחת לשלוש שנים לכל היותר תיערך בדיקה שוטפת של הארקות ורשת ההזנה.

מנהל מתקן המחשב הוא שיזם את הזמנת אנשי המקצוע הקשורים לבדיקות המתוארות בנוהל זה, בתאום עם מחלקת בנא"ם. מנהל המתקן ינהל וישמור תיעוד המשקף את הבדיקות שבוצעו, לרבות נתוני תאריכי הבדיקה, שם חברת הספק, שם הטכנאי וממצאיו.

הדרישות הנ"ל נוגעות אך ורק בכל הקשור להגנה על הציוד בלבד ואינן מבטלות את הנחיות הנהלים האחרים הנוגעים להיבטים האחרים של אבטחת המחשב האישי וציודו.

חל איסור להוצאת פריטי מחשב מאתרי המשרד, אלא אם כן ההוצאה מלווה בתעודה מתאימה של גורם מוסמך.

אמצעי אחסון מגנטיים נתיקים (דיסקטים, קלטות וכד')יאוחסנו בארונות הניתנים לנעילה (בהתאם להנחיות היצרן לגבי התנאים הסביבתיים לאחסנתם).

הודעה על נזק/גניבה/אובדן של ציוד מחשב תועבר מייד לממונה אבטחת מידע והוא יעדכן במידת הצורך את קציו הביטחון של המשרד.

בנוסף לנוהל זה, מומלץ להיעזר בתקני בטיחות מתאימים של מכון התקנים הישראלי ובפרט בתקן 1243 – בטיחות אש של מחשבים וציודם ההיקפי.

מקורות

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

נוהלי אבטחת המידע בעיריית ירושלים, פברואר 2001.

גיבוי ושחזור מידע

נוהל מס׳ 28

מבוא

פעילותם של משרדי הממשלה ומוסדותיה וניהולו התקין של משק המדינה מותנים, בעיקר, בקיומו של מידע זמין, לצורך קבלת החלטות וטיפול בענייניהם של אזרחי המדינה. ביצוע גיבוי למידע ו תנאי להשגת שרידות המידע, זמינותו, והיכולת לשחזרו. אלה נדרשים כדי לאפשר למשרד

א. להתאושש בהקדם ממצבי אסון, תוך ביטול או מזעור הנזק (הכספי, או כל נזק אחר).
ב. להשיג את יעדיו כמשרד ציבורי/ממשלתי, המשרת את הציבור.
ג. לקיים את חובתו כנאמן (לציבור, נשוא המידע הקיים ברשותו) לשמירת המידע.
ד. לאפשר את ניהולו התקין של משק המדינה.
ה. ליישם הוראות כל דין המחייב לשמירת מידע רגיש באופן זמין.

נוהל זה משלב בתוכו הנחיות רבות מהתקן הישראלי מס׳ 1495, **אבטחת מערכות מידע ממוחשבות**, חלק **7 - גיבוי מידע ושחזורו**, ומהתקן הישראלי מס׳ 1495, חלק 2 – **אבטחת מערכות מידע ממוחשבות – מצעים נושאי מידע״.**

הנהלים שיפורטו להלן משלימים את הטיפול הנדרש עפ״י נוהל זה ויש לפעול גם על פיהם: **קווים מנחים לאבטחת מידע רגיש ומערכי מידע, אבטחה פיזית, אבטחת התקשורת, אבטחת מידע רגיש בתהליך ״מיקור - חוץ״** (OUTSOURCING).

מטרות הנוהל

קביעת השיטות לגיבוי מידע ושחזורו במערכות המידע במשרדי הממשלה ומוסדותיה, המטפלים ומעבדים ״מידע רגיש״ בסיווג ״חסוי״.

הנוהל יקבע שיטות אחידות לגיבוי מערכות ממוחשבות, על בסיס שלוש רמות חיוניות: **בסיסית, בינונית וגבוהה** [לעניין קביעת רמות החיוניות - ראה נוהל מיפוי ״מידע רגיש״, משאבים ומערכות מידע וסיווגם על פי רמת חיסיון וחיוניות].

הגדרות

מידע (בנוהל זה) **-** מרכיבי המידע (כולם או חלקם)**:** רשומות ממוחשבות, תיעוד ממוחשב, תוכנות למיניהן, נתונים למיניהם.

גיבוי - א. עותק זהה של המידע, שנכתב על מצע נוסף. **ב.** פעולת ההעתקה של המידע למצע נוסף.

תכולת גיבוי - רשימת פריטי מידע הכלולים בגיבוי מסוים.

תדירות פעולות גיבוי - מרווחי זמן הקבועים שבין פעולות הגיבוי.

דור גיבוי - מקומו הסידורי של הגיבוי בסדרת גיבויים עוקבים של אותו סוג גיבוי.

מחזור גיבוי - מספר דורות הגיבוי שנקבע לסוג גיבוי מסוים במשרד.

סבב דורות גיבוי - החלפת דור הגיבוי הקדום ביותר שבסדרת הגיבויים, המהווה מחזור גיבוי, בדור גיבוי חדש.
גיבוי מלא - גיבוי של כל מרכיבי המידע במשרד (ראה הגדרה - ״מידע״) או גיבוי של כל מרכיבי המידע של מערכת מסוימת.

גיבוי חלקי - גיבוי של אחד או יותר מרכיבי המידע.

גיבוי שינויים (שולי) - גיבוי השינויים במידע מאז עריכת הגיבוי האחרון (ראה ציור 1).

גיבוי שינויים מצטבר (דיפרנציאלי) - גיבוי השינויים במידע מאז ביצוע הגיבוי המלא האחרון.

גיבוי רגיל - גיבוי מידע הנערך כשיגרה למערכות הצוברות שינויים במידע.

גיבוי מיוחד - גיבוי מידע, הנערך בנוסף על הגיבוי הרגיל שהמשרד מפעיל כשיגרה והמבוצע בשל נסיבות מיוחדות. לדוגמא: החלפת מערכת הפעלה, גיבוי לאחר שחזור, החלפת דיסקים, או, גיבוי המשקף מצב נתונים לסוף שנת העסקים.

גיבוי חם - עותק גיבוי הנרשם בגישה ישירה, בו-זמנית, עם מועד יצירת השינויים במידע.

גיבוי חם, קרוב לזמן אמיתי - עותק גיבוי הנרשם בגישה ישירה, בזמנים קצובים, בסמוך למועד יצירת השינויים במידע.

גיבוי "חם" באתר המחשב - גיבוי חם הנערך על מצע מידע הנמצא באתר המחשב.

גיבוי "חם" מחוץ לאתר המחשב - גיבוי חם המתבצע על מצע מידע הנמצא מחוץ לאתר המחשב.

גיבוי חם בנייר – אם אין גיבוי חם ממוחשב במשרד, מומלץ לקיים גיבוי חם במשך יום העבודה, **באופן לא ממוחשב**, בסמוך ליצירתו במחשב המרכזי (עותקים של חשבוניות, הזמנות ומסמכים אחרים חשובים). באופן זה יישמר באמצעים לא ממוחשבים המידע הנאגר במהלך יום העבודה, כך שבמקרה של קריסת המחשב יתאפשר שחזור המידע.

שחזור מידע - העתקה של מידע מהמצע שבו נשמר הגיבוי אל מצע אחר המיועד לשימוש המערכת.

שחזור מידע מלא - שחזור של כל מרכיבי המידע במשרד, או שיחזור של כל מרכיבי המידע של מערכת מסוימת.

שחזור מידע חלקי - שחזור של אחד או יותר מרכיבי המידע.

רענון מצעים - שיטה להבטחת תקינות המידע במצעי גיבוי מגנטיים, המיועדים לשמירה לתקופות ארוכות.

אחראי לביצוע הנוהל

הממונה על אבטחת "מידע רגיש" (להלן - "**הממונה**") אחראי, אחריות מקצועית, על הטמעת נוהל זה ועריכת בקרות וביקורות על אופן יישומו, דגש יושם על היבטי אבטחת המידע בכל תהליכי הגיבוי או השחזור.

מנהל מערכות המידע - אחראי, אחריות תפעולית, על יישום הנחיות נוהל זה.

אחראי לעריכת גיבויים - אחראי, תפעולית, על יישום נוהל זה ודיווח למנהל מערכי המידע

המנהל הכללי, אחראי, אחריות מינהלית כוללת, על יישום נוהל זה, ועל ביצוע ביקורות על אופן יישומו.

גוף הנוהל

האחראי לעריכת גיבויים, יבצע גיבוי של כל המידע שברשותו, באופן שיאפשר את שחזור המידע בעת הצורך.

מנהל מערכות המידע יקבע נהלים לביצוע גיבוי עבור כל מערכי המידע שברשותו וימנה "**אחראי**

לעריכת גיבוי ושחזור".

בכל שלבי הטיפול בהכנה של גיבויים, בשחזורם, באחסונם, בהעברתם למיקום אחר (בחצר הגוף או באתרים אחרים), ייושמו הנהלים הבאים:

א. **נהלי אבטחת המידע** הנוגעים למערכות המידע, למצעי המידע, לעובדים המטפלים וחשופים למידע.

ב. **נהלי בטיחות** הנוגעים למערכות המידע ולמצעי המידע למיניהם.

רישום המידע והנתונים המיועדים לגיבוי יתבצע על גבי מצעי מידע ניידים (דיסקט, תקליטון, סרט ואח') - עותק אחד יישמר בסמוך למחשב, והעותקים האחרים יישמרו באזורים **השונים** מאזור מחשב.

ב. **ה מ ל צ ה: יצירת גיבוי על גבי מצע מידע אופטי** [פילם/מיקרו פיש] - המרה של מידע ורשומות, הרשומים בשיטה בינארית לרישום בשיטה האופטית (מיקרופיש).

רקע: הולך ומתרחב השימוש בתהליך שיכונה להלן - "**גיבוי-המרה**", אשר במהלכו מבוצעת המרה של רשומות ממוחשבות (תיקים של חולים, תלמידים, עובדים, לקוחות, ספקים וכיוצא בכך) לפורמט אופטי [מיקרופיש], אשר נשמר כגיבוי במקום מרוחק, לתקופה שנקבעת על פי צרכי המשרד והנחיות כל דין.

יתרון השיטה: מתן יכולת השחזור של המידע לפורמט נייר או טכנולוגי - לאחר עשרות שנים וללא תלות בציוד מחשוב טכנולוגי מיושן [המותיר אותנו עם מצעי מידע שלא ניתן לקרוא אותם !

לסיכום סעיף זה: "היחידה" ממליצה למשרדי הממשלה ומוסדותיה ליישם <u>גם</u> "גיבוי המרה", התאמה לצורכיהם ובעיקר כאשר יש צורך לשמר מסמך ל-4 שנים ומעלה. יש להתייחס לדרישות החוק לשמירת מסמכים, לדוגמא מידע פיננסי שצריך להישמר 7 שנים.

א. משרד שעל פי צרכיו התפעוליים ואופי עבודתו נדרש לספק שירותי מידע רצופים יבצע גם "**גיבוי-חם**" (ראה סעיפים **17** עד **20**, כולל).

ב. יישום "**גיבוי-חם**" יאפשר למשרד להמשיך במתן שירותי המידע, גם במצב של תקלה ללא השהיה (או בהשהיה מזערית) הנגרמת ברצף השירותים, כתוצאה מפעילות שחזור המידע מן המצעים הניידים.

האחראי על **גיבוי ושחזור** יכין נוהל עבור כל סוג גיבוי (תוך היוועצות עם "**הממונה**"). הנוהל יכיל בין היתר את הפרטים הבאים:

א. תכולת הגיבוי;
ב. היקף הגיבוי (גיבוי מלא, חלקי, או גיבוי שינויים);
ג. אמצעי הגיבוי;
ד. מחזוריות ותדירות פעולת הגיבוי;
ה. מספר דורות הגיבוי;
ו. מספר עותקי הגיבוי;
ז. מיקום אחסון הגיבוי;
ח. שיטות שינוע הגיבויים.

בנוסף, יקבע אחראי הגיבוי והשחזור, (תוך היוועצות עם "הממונה") את:

א. השיטה והתהליך לבדיקת אמינות ושלמות הגיבוי;
ב. אופן ניהול יומן גיבויים.
ג. שיטת סימון המצעים.
ד. שם האחראי ליישום הנוהל.

בעת הכנת הנוהל יילקחו בחשבון השיקולים הבאים:

א. רמת חיסיון המידע (**בלמ"ס**, "**חסוי**", "**חסוי-ביותר**"), שנקבעה ע"י "**הממונה**".
ב. תדירות השינויים במידע;
ג. נפח המידע ושטח האחסון הנדרש ומצעי הגיבוי;
ד. משך זמן פעולת הגיבוי;
ה. רמת חיוניות המידע, הנגזרת מהדרישות לזמינות המידע;
ו. הסיכון באובדן המידע והנזק התוצאתי;
ז. בתכנון היישום של גיבוי יש להביא בחשבון את זמן שמירת המידע שהמשרד חייב בו, על פי חוקים ותקנות.

ראה - **חוק הארכיונים**, "**תעודות שגרתיות שמותר לבערן**", מתוך התוספת הראשונה לתקנות בדבר ביעור חומר ארכיוני במוסדות המדינה וברשויות המקומיות [**פורסם - 19.8.86**] .

עבור כל גיבוי ייקבעו בנהלי המשרד, הפרטים האלה:

א. תכולת הגיבוי
ב. היקף הגיבוי (גיבוי מלא, או גיבוי חלקי);
ג. מצעי הגיבוי, מחזור הגיבוי, תדירות פעולת הגיבוי, מספר דורות הגיבוי ומספר עותקי הגיבוי;
ד. מקום האחסון של עותקי הגיבוי;
ה. שיטת השינוע לעותקי הגיבוי.
ו. כללים לטיפול אבטחתי ובטיחותי במצעי המידע.

נוסף על האמור בסעיפים 37 עד 39 (כולל), ייקבעו בנהלים תהליכי בדיקת האמינות והשלמות של:

א. הגיבוי;
ב. יומן גיבויים, כמפורט בטבלת ניהול מצעים, סעיף **41** להלן;
ג. סימון המצעים, כמפורט בטבלת ניהול מצעים, סעיף **41.6** להלן;

ניהול מצעים (הקצאה ורישום):

כללים והנחיות	**מצע -המידע**	**ביצוע בהתאם לרמת החיוניות בסיסית בינונית גבוהה**		
רישום מצעים ומעקב אחריהם ביומני מעקב בשתי רמות רישום: **ברמת הספרייה** (במידה וקיימת במשרד ספריה) ינהל **הממונה על גיבוי ושחזור** רישום של הקצאת המצעים ותנועתם. **ברמת היישום** - האחראי **על גיבוי ושחזור** - ינהל רישום לגבי נושא תכולת המצעים.	לגבי דיסקיות מספיקה רמת הספרייה	- -	+ +	+ +
רישום ביומן המעקב ברמת היישום יכלול את הנתונים האלה: סוג המצע, זיהויו, מיקומו, נושא תכולתו ורמות סיווגו. הערות: **א)** ביומן המעקב תישמר ההיסטוריה של רמות סיווג מצע המידע. **ב)** רצוי מאד לנהל יומן בצורה ממוחשבת.	נייד וקבוע	+	+	+
רישום ביומן המעקב (הספרייה) של מצעים המועברים לגורמים מחוץ לארגון יכלול, נוסף על הפרטים המוזכרים בסעיף **41.2**, גם את הפרטים האלה: הגורם שאליו הועבר המצע, תאריך ההעברה, פרטי המעביר, פרטי המקבל ואישור הקבלה. היומן ישקף את מיקום המצע בכל עת.	נייד וקבוע	+	+	+
רישום ביומן המעקב (הספרייה) של מצעים				

המועברים לגורמים אחרים בתוך המשרד יכלול, נוסף על הפרטים המוזכרים בסעיף **41.2**, גם את הפרטים האלה: הגורם שאליו הועבר המצע תאריך ההעברה, פרטי המעביר, פרטי המקבל ואישור הקבלה. היומן ישקף את מיקום המצע בכל עת.	נייד וקבוע			+
סיווג יומן המעקב ואבטחת הגישה אליו, לפחות ברמת "**חסוי**".		+	+	+
סימון חיצוני של פרטי מצע המידע, באופן שיאפשר את זיהויו.	נייד		+	+
קביעת נוהל להקצאה מחדש של מצעים.	נייד וקבוע		+	+

על פי תקן ישראלי 1495 חלק 2 - גיבוי מידע ושחזורו
מנהל מערכי המידע יבצע גיבויים מיוחדים, לפי צרכיו.

תכנון גיבוי לגיבויים רגילים [א]

תכונה	סוג הגיבוי	רמת החיוניות בסיסית	בינונית	גבוהה
תדירות גיבוי	מלא	אחת לחודש	אחת לשבועיים	אחת לשבוע
	שינויים [ב]	אחת לשבוע	אחת ליום (ג)	אחת ליום (ג)
	שינויים מצטבר [ב]	אחת לשבוע	אחת ליום (ג)	אחת ליום (ג)
מחזור הגיבוי [ד]	מלא	2	4	8
	שינויים [ה]	3	13	6
	שינויים מצטבר [ו]	3	3	3
בדיקת תקינות במהלך ביצוע גיבוי (VERIFY)	מלא	לא חובה	כן	כן
	שינויים			
	שינויים מצטבר			
בדיקת תקינות חודשית - קריאת גיבוי מדגמית [ז]	מלא	2%	5%	8%
	שינויים			
	שינויים מצטבר			
בדיקת שחזור מדגמית מגיבוי	מלא	שנתית 2%	חצי-שנתית 5%	תלת-חודשית 8%
	שינויים			
	שינויים מצטבר			
מס' העותקים הנדרש	מלא	1	2 עותקים של גיבוי אחרון [ח]	3 עותקים של גיבוי אחרון [ט]
	שינויים			
	שינויים מצטבר			

הערות:

(א) הטבלה הנ"ל מחושבת לפי מודל סכמתי, הבנוי מ- 7 ימי עבודה בשבוע ו- 4 שבועות בחודש.
כל משרד יערוך התאמות של הערכים בטבלה, לפי מספר ימי העבודה בשבוע ומספר השבועות בחודש.

(ב) המשרד יבחר אם לערוך גיבוי שינויים, או לחילופין, לערוך גיבוי שינויים מצטבר.

(ג) אחת ליום - הכוונה לימי עבודה.

(ד) המספרים הנמצאים ב- 3 העמודות בסיסית, בינונית, גבוהה מייצגים את מספר דורות הגיבוי הנדרש במחזורי הגיבוי (מלא, שינויים ושינויים מצטבר).

(ה) מספר דורות גיבוי השינויים הנדרש , מושפע מתדירות הביצוע (בהתאמה לרמת החיוניות),
ולפיכך מספר דורות גיבוי השינויים במחזור, מושפע ממספר השבועות שבין גיבוי מלא לגיבוי המלא שאחריו. לדוגמא: ברמת חיוניות בסיסית, פרק הזמן שבין גיבוי מלא אחד למשנהו הוא חודש וגיבוי שינויים נערך אחת לשבוע; לכן, בחודש בן 4 שבועות יבוצעו 3 גיבויי שינויים (הגיבוי המלא הבא יהיה במקום גיבוי השינויים הרביעי).

(ו) מספר דורות הגיבוי נקבע ל - 3 , כדי לא להתבסס על עותק יחיד של גיבוי שינויים מצטבר.

(ז) לכל הפחות קריאת האינדקס הפנימי במצע.

(ח) 2 עותקים, שיאוחסנו האחד בסמוך למחשב והשני באזור סיכון השונה מאזור הסיכון של המחשב.
(ט) 3 עותקים, שיאוחסנו, האחד בסמוך למחשב והשניים האחרים ב 2- אזורי סיכון נפרדים,
השונים מאזור הסיכון של המחשב.

מחזור גיבוי מלא ברמת חיוניות בסיסית

תכנון גיבוי מיוחד - ייעשה בדומה לעקרונות התכנון של גיבוי רגיל, תוך התחשבות במאפיינים המיוחדים שמהם נובע הצורך בגיבוי מיוחד.

ניהול יומן גיבויים:

א. האחראי לגיבוי ושחזור ינהל יומן גיבויים בו ירשמו, עבור כל פעולת גיבוי, הפרטים
הבאים:

1. סוג הגיבוי (ראה הגדרות של סוגי גיבוי בנספח "מושגים").
2. תכולת הגיבוי;
3. מועד ביצוע הגיבוי;
4. פרטי מצעי המידע - סוג, כמות המצעים, סימון, מספר עותקים;
5. תוצאות ביצוע הגיבוי - הצלחה/כישלון, אירועים מיוחדים והגורמים להם
6. מקום אחסון מצעי הגיבוי;
7. זהות מבצע פעולת הגיבוי;
8. זהות מבצע השינוע;

ב. ביומן הגיבויים ירשמו גם פרטי בדיקת הגיבוי האלה:
1. עותק הגיבוי שנבדק,
2. סוג הבדיקה שבוצעה, על פי טבלה - תכנון גיבוי לגיבויים רגילים,סעיפים 3 עד 5
3. תוצאות הבדיקה,
4. זהות מבצע הגיבוי,
5. מועד הביצוע.

בכל אתר שמוחזקים בו מצעי-גיבוי, ינהל **האחראי לגיבוי** רשימת מצאי מעודכנת.

אחסון הגיבוי ושינועו: העברת מצעי מידע המהווים גיבוי, או אחסונם תאובטח, על פי הכללים המחמירים מבין שני ערכים אלה:

1) חיוניות המידע, התוכנות והנתונים;

2) חיסיון המידע המגובה.

בדיקת הגיבוי וניסוי שחזור:

א. המשרד יקבע מסגרת לבדיקת תקינות הגיבוי, במגמה לאמת את אמינותו של הגיבוי (אם ההעתק זהה למקור) ואת שלמותו (אם כל המידע האמור להיכלל בגיבוי אכן כלול בו).

ב. נוסף על כך יבצע **הממונה על הגיבויים** ניסוי שחזור, כדי לוודא שאפשר לשחזר את המידע באמצעות הגיבויים.

ג. הבדיקות והניסויים הנדרשים יבוצעו במועדים קבועים כנקוב בטבלה וכן באופן אקראי.

ד. פרטי הבדיקות והניסויים ותוצאותיהם יתועדו ביומן הגיבויים או ביומן אחר.

ה. לקחים ומסקנות מן הבדיקות והניסויים ישמשו לעדכון ולשיפור של נוהלי הגיבויים.

שחזור המידע

א. הממונה על גיבויים יקבע נוהל לביצוע מהיר ואמין של שחזור המידע, תוך שמירה על כללי הרשאות הגישה למידע הקיימים במשרד.

ב. בנוהל תהיה חלוקת ל**2**- סוגים של שחזור מידע:

1. שחזור מידע מלא, נכון למועד מסוים (ראה מושג בסעיף **22** לעיל).

2. שחזור מידע חלקי, נכון למועד מסוים ראה מושג סעיף **23** לעיל).

ג. כמו כן יתייחס הנוהל לעניינים אלה:

1. המידע הנדרש לשחזור;

2. מצעי הגיבוי הנדרשים ומקום אחסונם, בהתאם לרישום ביומן הגיבויים ;

3. אופן שינוע מצעי הגיבוי בהתאם לנוהל המשרד.

4. הכלים (תוכנות או פקודות מערכת) שבאמצעותם ייערך השחזור.

"גיבוי חם"
משרד שעל פי צרכיו התפעוליים ואופי עבודתו נדרש לספק שירותי מידע רציפים, יערוך "גיבוי חם", בנוסף על הגיבויים הרגילים או כתחליף לחלק ממחזורי הגיבוי.

ב. הבחירה באופן היישום של "גיבוי חם" - מותנית ברמת השרידות והזמינות של שירותי המידע הנדרשים מן המערכת. אפשרויות הביצוע של "**גיבוי-חם**" יהיו עפ"י שיקולי זמן ומקום, ויהיו בהתאם לסעיף **51ג** שלהלן.

ג. אפשרויות הביצוע של גיבוי חם, בהתאם לשיקולי זמן ומקום

שיקולי מקום	**שיקולי זמן**	
	גיבוי-חם	**גיבוי-חם, קרוב לזמן אמיתי**
באתר המחשב	ביצוע גיבוי-חם, לפי המושגים : גיבוי-חם [1] גיבוי-חם באתר המחשב [2]	בצוע גיבוי-חם, עפ"י המושגים : גיבוי חם קרוב לזמן אמיתי [4] גיבוי חם באתר המחשב [2]
מחוץ לאתר המחשב	בצוע גיבוי-חם, עפ"י המושגים : גיבוי-חם [1] גיבוי-חם מחוץ לאתר המחשב [3]	ביצוע גיבוי-חם, עפ"י המושגים : גיבוי-חם קרוב לזמן אמיתי [4] גיבוי -חם מחוץ לאתר המחשב [3]

[1] **גיבוי חם -** עותק גיבוי הנרשם בגישה ישירה, בו-זמנית, עם מועד יצירת השינויים במידע.
[2] **גיבוי-חם באתר המחשב** - גיבוי חם הנערך על מצע מידע הנמצא באתר המחשב.
[3] **גיבוי-חם מחוץ לאתר המחשב** -גיבוי-חם המתבצע על מצע מידע הנמצא מחוץ לאתר המחשב.
[4] **גיבוי חם, קרוב לזמן אמיתי -** עותק גיבוי הנרשם בגישה ישירה, בזמנים קצובים, בסמוך למועד יצירת השינויים במידע.

ד. גיבוי באמצעות תקשורת

1. ביצוע גיבוי באמצעות תקשורת מותנה באישור מראש ובכתב כי של "**הממונה**" כי הוראות נוהל מס' **7** - **אבטחת התקשורת** שולבו בתכנון תהליך הגיבוי, נבחנו באמצעות נתונים גולמיים ונמצאו כעונים על דרישות אבטחת "מידע רגיש" בתקשורת.

2. **<u>אסור לחלוטין</u>** לבצע גיבוי של מידע בסיווג "**חסוי-ביותר**", באמצעות תקשורת, אל מחשב הנמצא מחוץ למשרדי הממשלה ומוסדותיה. לדוגמא : תאגיד סחרי.

3. ביצוע גיבוי של מידע בסיווג "**חסוי**", באמצעות תקשורת, אל מחשב הנמצא גוף שאינו נמנה על משרדי הממשלה ומוסדותיה.

4. בעת עריכת גיבוי באמצעות תקשורת יש לוודא, שרמת אבטחת המידע במתקן מאחסן הגיבוי או במערכת המחשב שלו - **אינה פחותה** מרמת האבטחה במתקן המקור.

ה. בכל אפשרויות העריכה של **גיבוי-חם** ינהל הממונה על הגיבויים יומן גיבויים מוחשב.

ו. הממונה על הגיבויים יקבע שיטה לבדיקת אמינותו ושלמותו של המידע הכלול בכל "**גיבוי-חם**".

גיבויים במחשב המרכזי

מטרת הנוהל

הגדרת שיטות ודרכי שמירת גיבויים של נתונים ותוכנה שיאפשרו התאוששות סבירה ממקרה של פגיעה במאגרי המערכות הממוחשבות.

אחראי לביצוע הנוהל

המפעילים יישאו באחריות הביצוע של יישום הנחיות נוהל זה.
מנהל חדר מחשב וממונה אבטחת מידע יבצעו ביקורות ואכיפה של הנחיות הנוהל.

גוף הנוהל

הגיבוי יכלול אפשרות להתאוששות מלאה ושחזור, במקרה של קריסת מערכת ההפעלה.

המחשב המרכזי יערך גיבוי יומי, שיכיל את כל הקבצים ובסיסי הנתונים בהם יהיה שינוי כלשהו באותו יום. גיבוי זה ישמר למשך שבועיים. הגיבויים המתייחסים לשבוע השוטף ישמרו בחדר הקלטות בכספת חסינת אש ביחידת המחשב.

כמו כן, ייערך גיבוי שבועי מלא וכללי של כל הדיסקים במחשב. גיבוי זה יישמר חמישה שבועות בחדר הקלטות, בכספת חסינת אש.

יש להתייחס לבחירת סוג כספת חסינת האש ומיקומה: לכמה שעות היא צריכה להיות עמידה בפני האש, האם קיימים גלאי אש/עשן במקום? מומלץ למקם את הכספת במקום מרוחק מחדר מחשב בכדי להגביר את רמת האבטחה.

כמו כן, ישמר גיבוי חודשי למשך שנים עשר חודשים. גיבויי שלשה חודשים אחרונים יישמרו באתר מרוחק.

ביחידת המחשב יתנהל רישום מדויק של כל מהלכי הגיבוי, עד שנה לאחור בהתאם לסוג הגיבוי. המאגר הממוחשב של שליטה ובקרה על הגיבוי, יגובה גם הוא.

דרישות הגיבוי מתייחסות הן למאגרי נתונים והן לתוכנות מסוג כלשהו.

מצעים מגנטיים המכילים מידע, אשר יעמדו ללא שימוש במשך שמונה עשר חודשים, יעברו תהליכי רענון, באחריות מנהל היישום.

יש להתייחס לדרישות החוק לשמירת מסמכים, לדוגמא מידע פיננסי שצריך להישמר 7 שנים.

גיבויים במחשב אישי וברשת מקומית

מטרת הנוהל

שמירת גיבויים של נתונים ותוכנה במחשבים, שיאפשרו התאוששות סבירה במקרה של פגיעה במאגרי המערכת.
(נוהל זה אינו מתייחס לשמירת מידע המתחייבת מחוקים ונהלים אחרים, כגון חוק הארכיונים).

אחראי לביצוע הנוהל

מנהל חדר המחשב/מנהל הרשת יהיו אחראיים ליישום הנחיות נוהל זה.
כל משתמש אחראי לביצוע הגיבוי במחשבו, במידת הצורך.
ממונה אבטחת מידע ומנהל יחידת מערכות מידע יבצעו בקרה ואכיפה, כל אחד בתחומו.

גוף הנוהל

חומר הגיבוי יישמר במיקום אשר נקבע מראש ע"י הארגון.
כל יישום בלתי מסווג במחשבים אישיים, יגובה גיבוי מלא בתום כל יום בו עודכן מאגר הנתונים של היישום (2 "דורות"), וכן בגיבוי שבועי (2 "דורות"). הגיבויים השבועיים יוחזקו מחוץ לכותלי החדר בו נמצא המחשב, ובארון נעול.

כל יישום בסיווג "חסוי" יגובה מלא בתום כל יום בו עודכן מאגר הנתונים של היישום (3 "דורות"), כמו כן בגיבוי שבועי (2 "דורות"), וכן בגיבוי חודשי (2 "דורות"). הגיבויים השבועיים יוחזקו מחוץ לכותלי החדר בו נמצא המחשב, בכספת חסינת אש הממוקמת בחדר מאובטח בעל נגישות ממודרת. הגיבויים החודשיים יוחזקו אף הם באותם תנאים כמו הגיבויים השבועיים, אך בחדר אחר.

הנחיות הגיבוי לחומר "חסוי" יחולו גם על חומר של יישום בלתי מסווג, אם היקף הנתונים בישום זה הנו מעל חצי מגה.

כל יישום בסיווג "חסוי ביותר" במחשבים אישיים, יגובה גיבוי מלא בתום כל יום בו עודכן מאגר הנתונים של היישום (4 "דורות"), כמו כן בגיבוי שבועי (4 "דורות"), וכן בגיבוי חודשי (4 "דורות"). הגיבויים השבועיים יוחזקו מחוץ לכותלי החדר בו נמצא המחשב, ואילו הגיבויים החודשיים יוחזקו <u>מחוץ למבנה</u> בו נמצא המחשב. כל הגיבויים יאוחסנו בכספת חסינת אש הממוקמת בחדר מאובטח בעל נגישות ממודרת. יש להתייחס לבחירת סוג כספת חסינת האש ומיקומה: לכמה שעות היא צריכה להיות עמידה בפני האש, האם קיימים גלאי אש/עשן במקום?

הנחיות הגיבוי לחומר "חסוי" יחולו גם על חומר של יישום "חסוי", אם היקף הנתונים בישום זה הנו מעל חצי מגה.

הנחיות נוהל זה באשר לאחסון המצעים באות להוסיף על ההנחיות הכלליות לגבי מצעים מגנטיים, המופיעות בנוהל מתאים. בכל מקרה של אי אחידות בין דרישות שני הנהלים, לחייב הדרישה המחמירה יותר.

מבצע הגיבוי הוא שאחראי על אחסון ונעילה של מצעי גיבוי.
יש להקפיד כי הארון בו מאוחסנים הגיבויים לא יימצא בקרבה יתרה למערכת ההסקה, לא ייחשף לקרינת השמש ולא יימצא ליד מתקני חשמל מרכזיים או ליד ארונות חשמל או צנרת מים.

בכל מקרה בו נעשה גיבוי של יותר מיישום אחד על גבי אותו מצע מגנטי, תחול דרישת הגיבוי לפי היישום בעל הסיווג הגבוה ביותר.
מצעים מגנטיים המכילים מידע, אשר יעמדו 18 חודשים ללא הפעלה, יעברו תהליכי רענון. במידת הצורך ניתן יהיה לקבל סיוע מיחידת המחשב.
מלבד הגיבויים השוטפים, תחזיק יחידת המחשב שני עותקים מעודכנים של כל תוכנה המופעלת במחשבי המשרד. העתק אחד יימצא מחוץ לכותלי המבנה בו שוכנת יחידת המחשב המרכזית.

קבצי עיבוד למתילים יחשבו כקבצים לכל דבר ועניין, ויחולו עליהם כל ההנחיות של נוהל זה.

דרישות הגיבוי מתייחסות כולן לגיבויים חיצוניים (גיבויים ששוכנים על מצע מגנטי חיצוני למחשב כגון דיסקט, קלטת וכו', ולא על הדיסק הקשיח של המחשב עצמו.
האחראי על רשת התקשורת המקומית יהיה אחראי גם על ביצוע הגיבוי במחשב השרת.
אופן השמדת המידע ומועד ההשמדה ייקבעו על פי הנחיית בעל המידע. אחת לתקופה של שלושה חודשים יש לבדוק את אמינות הגיבוי.

בעת החלפת מחשב או השבתתו, יש לפעול באופן הבא:
יש <u>לגבות</u> את קבצי המידע אשר במחשב המוחלף/המושבת, ו/או להעבירם למחשב החדש.

יש למחוק את כל קבצי המידע והתוכנות אשר במחשב המוחלף/המושבת. ביצוע סעיף זה ע"י טכנאי של יחידת מחשוב.

מקורות

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

נוהלי אבטחת המידע בעיריית ירושלים, פברואר 2001.

מכון התקנים הישראלי, תקן 1495 – אבטחת מערכות מידע ממוחשבות, חלקים 2 ו-7.

חוק הארכיונים, **התשט"ו 1955** -, סעיפים **6, 12, 15**.

תקנות הארכיונים (ביעור חומר ארכיוני במוסדות המדינה וברשויות המקומיות) **התשמ"ו - 1986**, סעיפים: **1** עד **18**, כולל).

תקנות הארכיונים (שמירתם וביעורם של תיקי בית המשפט ובתי דין דתיים, **התשמ"ו - 1986**.

תוכניות התאוששות מאסון
(Disaster Recovery Planning–DRP)

נוהל מס׳ 29

מטרות הנוהל

לסכל הפרעות לפעילויות המשרד ולהגן על תהליכים המשרד קריטיים מהשפעת כשלים רציניים או מקרי אסון. להדגיר תהליכי התארגנות לתהליך התאוששות ממקרה של פגיעה חמורה במערכת הממוחשבת.
התוכנית תעזור להקטין נזקים במקרה אסון, להקטין הוצאות ביטוח, לשפר יחסי גומלין והתקשורת בין היחידות במשרד, להגביר המודעות לצורך בהגנת המערכות.

אחראי לביצוע הנוהל

ממונה אבטחת מידע, בסיועו של מנהל היחידה למערכות מידע, יוודאו תחזוקתם השוטפת והתקינה של האמצעים ליישום תוכנית התאוששות וכן יבקרו,יפקחו, יטמיעו ויתרגלו את פעולתה של התוכנית.

ועדת ההיגוי בנושא אבטחת מידע תדון ותאשר את התוכנית וכל שינוי מתבקש בה ותעודכן על ידי ממונה אבטחת מידע באשר לתרגולם, תקלות ופתרונות.

הגדרות

התאוששות – הקמת מערך מחשוב חלופי

תוכנית התאוששות – אוסף נהלים והנחיות המגדירים תהליכים חיוניים לארגון. פעולות הנחוצות להמשך מתן שירותים חיוניים. לוחות זמנים, מערך חלופי, הסכמי שירות וניסוי מערך התאוששות (לתרגול ולוידוא מוכנותו למצב אסון)

מצב אסון – אובדנם או אי-זמינותם של שירותים חיוניים המסופקים ע״י מערכות המידע המשרתות את המשרד.

גוף הנוהל

היערכות להתאוששות

על הממונה על המשרד למנות ועדת היגוי להכנת תוכנית התאוששות למצב אסון ועל האחראי הגיבוי והשחזור (תוך התייעצות עם הממונה על אבטחת מידע) לדאוג לביצוע ניסוי ובקרה על התוכנה ליישומה בעת אסון.

א. הרכב ועדת היגוי לתוכנית התאוששות
מומלץ כי בוועדה יהיו נציגים מיחידות אלה:
1. הנהלה – ישמש כראש צוות
2. תשתיות ומערכות הפעלה
3. מערכות יישום
4. תקשורת
5. מתאמי מחשוב ונציגי משתמשים
6. יחידת קצין בטחון

ב. פעילות הוועדה
1. הצוות יביא בחשבון מצבי אסון העלולים להיגרם בשל כשל טכנולוגי, פגעי טבע ומעשי אנוש, בשגגה או בזדון.

2. הצוות יגדיר מהו מצב אסון ומיהו בעל הסמכות להכריז על מצב אסון.
3. צוות ההיגוי יכין תוכניות התאוששות לכל התרחישים האפשריים בסביבת מערך המחשוב של המשרד, תוך התחשבות בנתוני אירוע אלה:

שיעור נוכחות בעלי תפקידים חיוניים
שיעור הנזק למבנים ולמתקנים
זמינות שירותי תשתית: חשמל, מים, תקשורת.

תוכניות ההתאוששות

תוכניות ההתאוששות שיפותחו על ידי צוות ההיגוי יתייחסו להיבטים אלה:
פעולות להצלת חיי אדם, לצמצום נזקים, להערכת נזקי האסון ולקביעת דרגת האסון, השיקולים אודות הצורך בהכרזת אסון וקביעת הגורם המכריז. <u>להלן פירוט תוכניות ההתאוששות</u>:

א. הקמה של מערכת תשתית להפעלה מידית במטרה להציל חיי אדם ולצמצם נזקי רכוש, כגון: מערכות התראה ואזעקה לגילוי אש או עשן או שניהם, מערכות כיבוי אש אוטומטיות וידניות וציוד עזרה ראשונה.
ב. פיתוח נהלי חירום, הקמת מערך של צוותי חירום, הדרכתם, אימונם וציודם באמצעי עזר.
ג. הקמת תשתית תקשורת עם שירותי ההצלה ותיאום עמם: משטרה, מגן דודו אדום, מכבי אש והרשות המקומית.
ד. לכל תרחיש רלוונטי למשרד יוכנו המסמכים הבאים:
   - רשימה מפורטת של כל הפעולות הנדרשות עד לתחילת ההתאוששות
   - רשימת קריאה: רשימת כל העובדים שנוכחותם חיונית, כתובותיהם ומספרי הטלפון שלהם (לכל עובד ימונה לפחות מחליף אחד).
ה. בעת אירוע, צוות החירום המתאים יעריך את המצב כצעד ראשון, יקבע את דרגת האסון וידאג להעביר את הממצאים לבעל סמכות להכרזה על מצב אסון.

על ממונה אבטחת מידע, בתאום עם מנהל יחידת מחשב, להכין תוכנית כתובות ומפורטות לתפעול והתאוששות.
העתקי תכנית ההתאוששות יימצאו אצל מנהל יחידת המחשב ואצל ממונה אבטחת המידע.

תכנית ההתאוששות תיקח בחשבון את היערכות יחידות המשרד כולן ואת הקשר בין המחשב המרכזי ליחידות השונות אחרי פגיעה חמורה. ההתייחסות לא תהיה רק ליחידת המחשב, אלא גם לאופן הפעילות הרלוונטית ביחידות המשרד מאז הפגיעה ועד לפתרון הקבע.

יוגדר אתר חלופי כפתרון ביניים, כתשובה לתרחיש של אסון מלא שלא יאפשר כלל להשתמש באתר הקבוע.
במידה והאתר המרכזי נפגע מאסון ואינו יכול לתפקד, ייתכן כי יעבור פרק זמן ניכר עד שניתן יהיה להחזירו לעבודה. האתר החלופי יכיל את כל הציוד הדרוש לתפעול "חדר שרתים חירום" כגון מפצלי וכבלי חשמל, כבלי רשת, בוררי מחשבים, תוכנות והתקנות לתפעול שוטף (לבניית מחשבים, מנהלי התקנים, התקנת תוכנות), ציוד היקפי וכו'.

אירוע חירום, יכול שיחייב כוח אדם נוסף, כדי להתגבר על התקלות ולהחזיר את המערכת לתפקוד סדיר. יש לבחון בשלב התכנון, התקשרויות אפשריות עם חברות לאספקת כוח אדם זמני. רצוי לנהל משא ומתן עם היצרנים ועם חברות- שירות, כדי לשריין את שירותיהם למצבים אלה.
יש להקים Helpdesk חירום. יש לחשוב על תחליפים לציוד מחשבי שקשה להחליפו (מערכות ישנות – חומרה ותוכנה).
רצוי לבחון הוספה של נוהל הקובע את הפעולות מול אתר מרכזי שעבר אסון. לדוגמא: ציוד מחשוב שניתן להציל (בעיקר כזה שקשה להחליף), מניעת בזיזה (הצבה של כוחות משטרה), איסוף מדיות מגנטיות, הובלות ציוד שהוצל לאתר התאוששות, בדיקה של חברות חיצוניות לשחזור מידע מציוד שהוצל.

במשרדים קיימים תהליכים מסורבלים מאוד לרכישת ציוד חדש. מומלץ כי במסגרת נוהל כלל משרדי להתאוששות מאסון יוכלל גם נוהל רכישת ציוד המאפשר רכישה ללא בירוקרטיה וללא מכשולים אחרים (רכישת חירום). (חקיקה ?)

מומלץ לשלב נוהל גיבויים לקביעת סטנדרט איכותי כולל אכסון באתרי התאוששות.

יש לקבוע מראש מי יעמוד בקשר עם אמצעי התקשורת במצב אסון, במגמה לעדכן את ציבור הלקוחות של המשרד על שירותים הניתנים במצב חריג.

נוהל התאוששות לאירועים צריך לכלול את הרכיבים הבאים:

א. דיווח: למי ועל ידי מי.
ב. תחומי אחריות ומי האחראי.
ג. באילו מצבים יופסקו שירותי דואר אלקטרוני ואינטרנט.
ד. הסדרי תקשורת ואתראות.

לצוות התאוששות יש לקבוע מראש משימות. בקביעת הצוות יש לקחת בחשבון:

א. נציגות בצוות של כל חלקי המשרד.
ב. באיזה מצבים יכנס הצוות לפעולה.
ג. שרשרת הפיקוד.
ד. הסמכויות שיואצלו לצוות.

אמצעי האבטחה יאפשרו להתמודד עם:

א. מתקפות האקרים
ב. מתקפות וירוסים
ג. מתקפות Denial Of Service
ד. מתקפות "קוד עוין"
ה. זליגת מידע מסווג
ו. בקרת תכני תקשורת - דואר אלקטרוני ואינטרנט.

תרגול ובקרה

אחת לשנה, במסגרת תכנית העבודה השנתית, יערך באחריות משותפת של מנהל יחידת המחשב וממונה אבטחת המידע, תרגול המקיף את כלל היבטי ותחומי התוכנית, לרבות שחזור קבצים מן הגיבויים ושימוש באתר החליפי.
תרגול האתר החליפי יכלול הובלה ושימוש בהעתקי גיבוי של המאגרים השונים.

מהלכו של התרגיל יתועד על ידי ממונה אבטחת מידע אשר בסופו של התרגיל יפיק דו"ח סיכום תרגיל. ממצאיו יועברו לדיון בישיבת ועדת ההיגוי בנושא אבטחת מידע, המסקנות יתועדו, יוטמעו ויתורגלו כנדרש.

ההיערכות למצב חירום צריכה לקחת בחשבון אפשרויות לפגיעה באספקת הכוח, במידע, בגיבויים, ובאמצעים שונים אחרים, את העלויות הכרוכות בהתאוששות, ואת משך הזמן הנדרש להתאוששות שגם לו משמעות כלכלית.

תוכניות התאוששות עלולות להיכשל בבדיקה, לעתים בגלל הנחות שגויות, טעויות, או שינויים בציוד או צוות העובדים. לכן יש לבדוק אותן באופן סדיר, כדי להבטיח שהן מעודכנות ואפקטיביות. בדיקות כאלה יבטיחו גם שכל חברי צוות ההתאוששות ועובדים רלוונטיים אחרים, מודעים לתוכניות.
לוח הזמנים לבדיקת תוכניות התאוששות, יפרט איך ומתי יש לבדוק כל רכיב בתוכנית. מומלץ לבדוק לעתים קרובות כל רכיב ורכיב. כדי להבטיח שהתוכניות אכן יפעלו בשעת הצורך, יש להשתמש במגוון טכניקות, כגון:

א. בדיקות תיאורטיות של תרחישים שונים (דיון בסידורי ההתאוששות של המשרד אחרי הפרעות שונות אפשריות);
ב. תרגילי הדמיה (במיוחד לצורכי הדרכה באשר לתפקידי הניהול שיוטלו על אנשים לאחר אירוע או משבר);
ג. בדיקת התאוששות טכנית (וידוא שניתן לאתחל ביעילות את מערכות המידע);

ד. בדיקת התאוששות באתר חלופי (הפעלת תהליכי המשרד במקביל לפעולות ההתאוששות, באתר מרוחק מהאתר העיקרי);
ה. בדיקת אפשרות ושירותים של ספקים (וידוא ששירותים ומוצרים המסופקים ממקורות חיצוניים, יעמדו בהתחייבויות החוזיות);
ו. תרגילים מלאים (כדי לבדוק שהארגון, העובדים, הציוד והתהליכים יכולים להתמודד עם ההפרעות).

הטכניקות מתאימות לשימוש על ידי כל המשרד, והן ישקפו את אופייה של תוכנית ההתאוששות הספציפית.

תחזוקה והערכה מחדש

פעם בשנה לכל הפחות יעבור ממונה אבטחת המידע על תוכניות ההתאוששות ויבדוק אם קיים צורך בעדכונו.

תוכניות התאוששות יתוחזקו באמצעות סקירות ועדכונים, כדי להבטיח את היעילות הרציפה שלהם. בתוכנית ניהול השינויים של המשרד, יכללו נהלים שיבטיחו שענייני המשכיות מתן השירות זוכים להתייחסות נאותה.
תוטל אחריות לביצוע סקרים סדירים לכל תוכנית התאוששות. אם זוהו שינויים בסידורי המשרד, שאינם באים עדיין לידי ביטוי בתוכנית התאוששות, תעודכן התוכנית. תהליך רשמי זה של בקרת שינויים, יבטיח שהתוכנית המעודכנת מופצת ומוחזקת באמצעות סקרים סדירים של התוכנית השלמה. מצבים העשויים להצריך עדכון תוכניות, הם למשל, רכישת ציוד חדש, או שדרוג של מערכות תפעוליות ושינויים של:

א. צוותי העובדים,
ב. מענים או מספרי טלפון,
ג. האסטרטגיה העסקית,
ד. מיקום, אפשרויות ומשאבים,
ה. חקיקה,
ו. קבלנים, ספקים ולקוחות עיקריים,
ז. תהליכים, או תהליכים חדשים או מבוטלים,
ח. סיכון (תפעולי וכספי).

מקורות

מכון התקנים הישראלי, תקן 1495 – אבטחת מערכות מידע ממוחשבות.

מכון התקנים הישראלי, תקן 7799 – ניהול אבטחת מידע.

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

נוהלי אבטחת המידע בעיריית ירושלים, פברואר 2001.

אבטחת תוכנה וחומרה במחשבים אישיים

נוהל מס׳ 30

מטרת הנוהל

להסדיר את השימוש במחשבים האישיים המשמשים את היחידות השונות במשרד, על כל היבטי השימוש/הטיפול האבטחתי בהם, במטרה למזער נזקים למערכות המידע או למידע הקיים בהן.

אחראי לביצוע הנוהל

אחריות ביצוע: המשתמשים הישרים במחשבים בכלל ובמחשבים אישיים בפרט.

אחריות בקרה: ממונה אבטחת מידע, מנהלי היחידות.

גוף הנוהל

א. שמירת קבצים:

1) יש לשמור את הקבצים השונים על גבי הרשת, במחיצות היחידתיות והאישיות שהוקצו לכל משתמש ברשת.
2) הגיבויים ברשת יבוצעו בהתאם למדיניות המשרד הנוגעת לנושא זה ובכפוף לנוהל הרלוונטי.
3) בתחנות אשר בהן אושר לעבוד בתוכנה ישירה מתוך התחנה, ולא מתוך הרשת, יוודא המשתמש לשמור הקבצים הן ברשת והן על גבי הכונן המקומי של המחשב. המשתמש ידאג לגיבוי הקבצים שעל גבי הדיסק.

ב. אבטחת מידע במחשבים אישיים:

1) יש לעדכן כל משתמש בדבר המידע אליו הוא רשאי לגשת, וצורת הגישה המותרת לו.
2) אין לאפשר גישה למחשבים האישיים או לחשוף המידע המאוחסן במחשב, בפני עובדים אשר אין המידע נחוץ להם לצורך עבודתם וכן בפני גורמים שאינם עובדי המשרד, באשר הם.
3) אין לגלות/לחשוף את סיסמת הכניסה למחשב בפני כל גורם שהוא, בשום מקרה או אופן.
4) העובד יעשה שימוש נאות בכל אמצעי/כלי אבטחת המידע שהוטמעו במחשבו על ידי גורמי המשרד. כמו כן, באחריותו ליישם את ההנחיות הנוגעות לבחירה ולשימוש בסיסמא אישית.

ג. ״וירוסים״ במחשבים האישיים:

1) נגע ה״וירוסים״ הולך ומתפשט ועלול לגרום נזק למידע המצוי ברשת המשרד, לתוכנות המותקנות בו ואשר עלולות לשבש את מהלך עבודתו של המשרד, לאובדן שעות עבודה וכדומה.
2) על המשתמש לוודא הימצאות תוכנת אנטי-וירוס פעילה במחשבים האישיים ואין להפסיק את פעולתה..
3) חל איסור מוחלט על הבאת תוכנות זרות לשימוש ביחידות המשרד שלא אושרו וניקנו ע״י מרכז החישוב.
4) במקרים בהם צרכי העבודה דורשים מסירת/קבלת אמצעים מגנטיים בין יחידות המשרד או מגופים חיצוניים, יש לוודא שהם נקיים מ״וירוסים״.
5) יש לבצע מדי מספר ימים סריקה לאיתור ״וירוסים״ בדיסק הקשיח ו/או בדיסקטים שיעשה בהם שימוש באותו יום.
6) נא ראה הרחבה בנושא וירוסים בנוהל נפרד.
7) יש לסרוק אי קיום וירוסים בכל דיסקט ותקליטור לפני התחלת השימוש בו.

ד. תוכנה וחומרה

יש להתקין ולהשתמש בתוכנות אשר נבדקו, אושרו ונרכשו כחוק ע"י המשרד. אין להשתמש בתוכנות ממקור לא מאושר. התקנת חומרה תתבצע רק ע"י טכנאי מורשה ובאישור ממונה אבטחת מידע. התקנת חומרה המאפשרת תקשורת עם גורמי חוץ, מותרת עפ"י אישור בכתב של ממונה אבטחת מידע. יש להתקין תוכנת האנטי – וירוס בכל מחשב. במחשב שבו יש חיבור מאושר לאינטרנט – תוכנת האנטי-וירוס תתעדכן באופן מקוון אוטומטי.

ה. דיווח

על מנהלי היחידות להביא לידיעת הממונה אבטחת מידע, חשדות או אירועים הקשורים בשימוש במחשבים האישיים של עובדי היחידה ואשר עלולים להשליך על יכולת אבטחת המידע במשרד (חשדות או אירועים הידועים או המובאים לידיעתם).

אין להשתמש ברכיבים אוגרי מידע ללא ממונה אבטחת מידע.
בכל צורך הוצאת רכיב אוגר מידע מהארגון, כולל לתיקון או החלפה, יש לקבל אישור על כך מהממונה על אבטחת מידע.

מקורות

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

נוהלי אבטחת המידע בעיריית ירושלים, פברואר 2001.

נוהלי עבודה – אגף לשירותי מידע ומחשוב, משרד הבריאות, פברואר 2000.

נוהלי אבטחת מידע של רשות הדואר, דצמבר 2002.

אבטחת מידע במחשבים ניידים, palm pilot ו-דיסקים נתיקים

נוהל מס׳ 31

1. מחשבים ניידים

מטרת הנוהל

להנחות לגבי דרכי ההגנה על מידע הנאגר או המעובד במחשבים ניידים, במגמה לצמצם את הסיכון שבגניבת הציוד ו/או חשיפת המידע השמור בו ו/או נגישות לרשת המשרד באמצעות המחשב הנייד.

אחראי לביצוע הנוהל

אחריות יישום הנחיות הנוהל חלה על משתמשי המחשבים הניידים.

ממונה אבטחת מידע ומנהל היחידה למערכות מידע ינחו, יטמיעו ויבקרו יישום ההנחיות.

גוף הנוהל

חל איסור לאגור נתונים מסווגים על גבי דיסק קשיח במחשב נייד, אלא אם כן מותקן במחשב אמצעי בקרת גישה המאושר ע״י אגף הביטחון.

נתונים מסווגים הנם אלה המוגדרים כ״מידע רגיש״ בחוק הגנת הפרטיות והתקנות בעניין (״חסוי״ ו״חסוי ביותר״ – ראה נוהל מתאים).

אין לאגור מידע לגבי אנשים, למעט רשימת כתובות וטלפונים לצורך התכתבות או שימוש טלפוני. בכל מקרה רשימות אלה לא תהיינה רשימות מקבוצות של אוכלוסיות שהמידע לגביהן מוגדר כ״מידע רגיש״ בחוק (מוגבלויות למיניהן, שיוך לקבוצה בעלת מכנה משותף וכו׳).

חיבור מחשב נייד לרשת תקשורת של המשרד יתבצע רק לאחר שהממונה על נושא המחשבים הניידים ביחידה למערכות מידע יוודא קיום מתמשך של אמצעי הגנה הולמים במחשב וברשת המשרד.

אגירת מידע מעובד מורשית רק ברמות סטטיסטיות מקובצות ומבלי לכלול הדגרות מפורשות של מכנה משותף למעט קודים אשר ידועים אך ורק למפעיל המחשב, ובפירושם איננו אגור במחשב.

אגירת מידע תותר רק על גבי דיסק נתיק או דיסקט בתנאי שאלה יאוחסנו <u>בנפרד</u> מן המחשב עצמו.

אין להשאיר מחשב נייד ברכב או בחדר ללא השגחה אישית וישירה של בעל המחשב הנייד. אם נגנב מחשב נייד או שיש חשש כי המידע האגור בו נחשף בפני גורם זר, יש לדווח מיידית ליחידה למערכות מידע, למנהל אגף הביטחון ולממונה אבטחת המידע.

מחשב נייד יהיה מוגן (מבחינת הפעלה) בסיסמאות בהתאם להנחיות נוהל ״ניהול ותפעול מערך הסיסמאות״.

מערכת ייעודית תותקן על גבי מחשב נייד רק אם מאגר הנתונים מאוחסן בנפרד (דיסק נתיק או דיסקט), המערכת מוגנת ע״י סיסמאות ולא ניתנת לאחזור (התוכנה לאחר הידור).

2. מחשבי Palm Pilot

מבוא

מחשב כף היד, ה-Palm Pilot, או דומיו, משלב פונקציות של יומן, ספר כתובות, רשימות ומחשבונים במכשיר קטן ונישא, בעל אפשרות סנכרון מידע מול יישומים כמו Lotus Notes ו-Outlook. כמו כן, ניתן לחבר אותו למודם, וליישם צורות תקשורת שונות החל מפקסימיליה ועד לגלישה באינטרנט.

סכנות פוטנציאליות:

1) גודלו הפיסי של מחשב כף היד, היכולת "להתממשק" לכל מחשב אישי וכן יכולתו להעביר קבצים ונתונים באופן דו כיווני מהווים סיכון ממשי ביותר לגניבה ולהעברת מידע לידי גורמים בלתי מורשים, ומחייבים שימוש מאובטח.
2) בין כיבוי והדלקה של מחשב כף היד אין פעולות נעילה המחייבת הקשת סיסמא על מנת לשוב ולהפעיל את המכשיר.

מטרת הנוהל

להגדיר את דרכי ההגנה על מחשבי כף היד, במגמה לצמצם את הסיכון שבגניבת הציוד ו/או חשיפת המידע האגור בהם ו/או נגישות לרשת המשרד באמצעותו.

אחראי לביצוע הנוהל

אחריות יישום הנחיות הנוהל חלה על המשתמשים.
ממונה אבטחת מידע ומנהל היחידה למערכות מידע ינחו, יטמיעו ויבקרו יישום ההנחיות.

גוף הנוהל

יש להתקין תוכנה אשר תדרוש סיסמא בכל פעם שמפעילים את מחשב כף היד, בכדי למנוע גישה בלתי מורשית/מבוקרת למידע. חוקי הסיסמא יהיו זהים לחוקים החלים על מחשבי המשרד.

אין להזין למכשיר מידע מסווג או רגיש מכל סוג שהוא, מכל סיבה ובשום מקרה!

למרות קיומן של מספר תוכנות המבצעות הצפנות על מידע במכשיר, ברמת פתקים, רשומות ואף מילים, **רמת ההגנה של המכשיר והתוכנות אינה מספקת**, ללא קשר לאופן ההצפנה.

כל עובד המקבל את המכשיר יחתום על טופס הצהרה בו מכריז העובד כי הנו מודע לסכנות הטמונות במכשיר, וכי הנו מודע לאיסור להזנת מידע מסווג למכשיר.

אין להשאיר מחשב כף יד ברכב או בחדר ללא השגחה אישית וישירה של בעל המחשב. אם נגנב המחשב או שיש חשש כי המידע האגור בו נחשף בפני גורם זר, יש לדווח מיידית ליחידה למערכות מידע, למנהל אגף הביטחון ולממונה אבטחת המידע.

3. דיסקים נתיקים

חלק זה מתייחס ל**כל אמצעי אחסון נתונים (מידע) נתיקים** באשר הם.

מבוא

דיסק נתיק נחשב לאחד הסוגים של "מדיה מגנטית". דיסק נתיק על צורותיו הנו אמצעי חדש יחסית לאחסון מידע. יתרונו העיקרי הוא שטח זיכרון עצום יחד עם גודל פיזי זעיר. מכך הסכנה הגדולה באובדן/גניבה של הדיסק הנתיק או חשיפת הנתונים שבו. כיום קיימות אפשרויות שונות לגישה למידע המבוקרת סיסמא ו/או הצפנת המידע האגור בו, אך למרות זאת אינם מספקים הגנה מלאה.

סכנה נוספת היא שימוש בדיסקים הנתיקים כאמצעי ציתות מתוחכם (אגירת נתונים שלא ביודעין). יש ליידע עובדי המשרד על כך ולבקשם לגלות ערנות בנושא.

אחראי לביצוע הנוהל

אחריות יישום הנחיות הנוהל חלה על משתמשי הדיסקים הנתיקים.
ממונה אבטחת מידע ומנהל היחידה למערכות מידע ינחו, יטמיעו ויבקרו יישום ההנחיות.

מטרת הנוהל

יש להתנהג בדיסק נתיק כנהוג בכל דיסק קבוע אחר.
אין להזין לדיסק מידע מסווג או רגיש מכל סוג שהוא, מכל סיבה ובשום מקרה!

כל עובד המקבל את המכשיר יחתום על טופס הצהרה, בו מכריז העובד כי הנו מודע לסכנות הטמונות במכשיר, וכי הנו מודע לאיסור להזנת מידע מסווג למכשיר.

אין להשאיר דיסק נתיק ברכב או בחדר ללא השגחה אישית וישירה של בעל הדיסק. אם נגנב הדיסק או שיש חשש כי המידע האגור בו נחשף בפני גורם זר, יש לדווח מיידית ליחידה למערכות מידע, למנהל אגף הביטחון ולממונה אבטחת המידע.

כל הנהלים החלים על שימוש, גיבוי, אחסון והשמדה של דיסקטים או תקליטורים רגילים, תקפים גם לדיסקים נתיקים.

בדומה ל"מדיה מגנטית" כדיסקטים או תקליטורים רגילים, **חל איסור מוחלט להכניס דיסקים נתיקים פרטיים למשרד.**

יש לנהל רישום מסודר של מלאי הדיסקים הנתיקים.

במקרה של **מסירת דיסק נתיק לתיקון/מחיקה/השמדה**, יש לוודא כי החברה המבצעת את התיקון היא "ספק מורשה" וחתומה על הסכם שמירת הסודיות.

מקורות

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת תוכנה ברשתות מקומיות

נוהל מס׳ 32

מטרות הנוהל

להגביל הכניסה למאגרי הנתונים ברשתות תקשורת מקומיות.

אחראי לביצוע הנוהל

המשתמש יהיה אחראי ליישם את הנחיות נוהל זה, כנדרש.
מנהל יחידת המחשב ומנהל הרשת ינהלו תפעולם של הכלים והאמצעים הנדרשים לאבטחה כמוגדר ויבצעו בקרה ואכיפה שוטפת.
ממונה אבטחת מידע יטפל במקרים חריגים ויסייע בביצוע בקרה ואכיפה.

גוף הנוהל

בעקרון ייעשה שימוש באמצעים המובנים ברשת.

על המשתמש להקיש את שם המשתמש ואת סיסמתו האישית ואלו ינתבו אותו ברשת בהתאם להרשאותיו. המשתמש יכול לראות קיום ספריות אחרות וכן את כל הספריות באמצעות פקודת DIR. הסיסמא לכניסה לרשת תוחלף אחת ל-60 ימים לכל היותר. הסיסמא תוחלף ע״י כל משתמש ובאחריותו. העובד יישם את ההנחיות המפורטות בנוהל הנוגע לבחירה ולשימוש בסיסמאות.

בכל הרשתות אשר מופעל בהן יישום ״חסוי ביותר״, יש להפעיל סיסמא סודית בדיוק על פי המפורט בנוהל ״אבטחת תוכנה וחומרה במחשבים אישיים״.

אל דיסק קשיח המותקן במחשב הקשור לרשת מקומית, ושאיננו מחשב השרת, יש להתייחס כאל דיסק במחשב עצמאי ועליו יחולו הוראות הנוהל ״אבטחה בתוכנה״.

תופעל אופציה של רישום LOG של כל הניסיונות הכושלים להיכנס למערכת במפורט בנוהל ״מעקב ופיקוח לוגי״. יירשמו: התחנה, הזמן והמשתמש.

המשתמש לא יוכל לעבוד בו זמנית ביותר מתחנת עבודה אחת ברשת.

מנהל יחידה שבתחום אחריותו מופעלת רשת תקשורת מקומית, ימנה אחראי לרשת. אחראי הרשת יופקד על אבטחת הרשת ויהווה חולית הקשר עם ממונה אבטחת המידע, בכל הקשור לנושא.

לא תותר עבודת משתמשים ברשת בשעות חריגות, בסופי שבוע, מועדי וחגי ישראל. במקרים חריגים תותר הפעילות באישור מוקדם של ממונה אבטחת מידע. בכל מקרה יש לבצע מעקב אחר פעילות חריגה ולבדוק האם הייתה מוצדקת.

מקורות

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

אבטחת התקשורת

נוהל מס׳ 33

מבוא

תקשורת חיצונית הנה תקשורת בין מחשב הנמצא במשרד לבין מחשב, או מסוף, הנמצא פיזית במקום אחר, וקווי התקשורת אליו עוברים ברשות הרבים, מחוץ למבנה המאובטח של המשרד (או, מחוץ לחצר המאובטחת, באם קיימת).

תקשורת חיצונית תוגדר כקשר בין מחשב למסוף, בין מחשב למחשב, או בין מחשב לכל אמצעי קלט/פלט מרוחק.

הסתייעות ב**תקשורת חיצונית** מגדילה במידה רבה את הסיכון לחיסיון ולחיוניות (המהימנות הזמינות והשלמות) של המידע, בשל היותה נגישה לגורמי-חוץ שאין לנו שליטה עליהם. סיכון רב קיים לחיוניות מערכי המידע, בשל חשש לשיתוקם ע״י גורם מרוחק, באמצעות התקשורת.

ההנחה כי מידע המוגדר על ידי גורמים ביטחוניים כ**לא מסווג (״בלמ״ס)**, אין לפרש ממנה בשום אופן, כי למידע זה אין רגישויות אחרות, **אשר הנן לעיתים גבוהות יותר ממידע בטחוני מסווג.** יתכן מאוד כי למידע ולנתונים יש **חיוניות קריטית לניהול** המשרד **ולקיום תקין של משק המדינה**, ויתכנו סייגים מחמירים יותר על אופן העברתו, אחסונו, עיבודו וגם ביעורו. לפיכך, הקביעה כי ברשת תקשורת מסוימת מותר להעביר מידע מסווג בטחוני ברמה מסוימת אינה מתירה שימוש באותם סייגים לגבי מידע ״**חסוי**״.

אבטחת תקשורת חיצונית מיועדת למנוע או לצמצם מאוד את האפשרות כי גורמים מרוחקים (פיזית) מאתר המחשב, יגרמו בשוגג, או במכוון לפגיעה בערכים אלה:

א) חיסיון/סודיות של המידע.
ב) חיוניות המידע, הנתונים, התוכנות ומערכי המידע.

ככלל, לא יותר חיבור ישיר, או עקיף, בין תקשורת מקומית לבין תקשורת חיצונית, אלא אם ניתן לכך אישור מראש ובכתב מ״הממונה״, המאשר כי הותקנו, נבחנו ואושרו כל הכלים הטכנולוגיים וכן המינהליים, כנדרש בנוהל זה.

הגדרות

״**תקשורת חיצונית**״ - תקשורת אשר מכלול האמצעים המשרתים אותה, או חלקים מהם, עוברים - בצורה זו או אחרת, ברשות הרבים ומחוץ ״למבנה המאובטח״, או, ״החצר המאובטחת (אם קיימת) של המשרד.

מטרות הנוהל

קביעת הצעדים המקדימים אשר בהם על המשרד לנקוט, **בטרם** מתבצעת פעילות של רכישת רכיבי תקשורת, או מערכות טכנולוגיות, לשם התחברות לרשת תקשורת חיצונית.
קביעת האמצעים והשיטות לאבטחת המידע ומערכי המידע, אותם יש ליישם במשרד, **במהלך הפעילות השוטפת** של העברת מידע ״**חסוי**״ בתקשורת, או חיבור מערכי-מידע בעלי **חיוניות ברמה בינונית** - אל תקשורת חיצונית.

אחראי לביצוע הנוהל

הממונה על אבטחת ״מידע-רגיש״ (להלן - ״הממונה״) - מהווה במשרד סמכות מקצועית-מינהלית. מכין (בין כלל תפקידיו) את תוכנית אבטחת התקשורת (בתיאום עם מנהל מערכות המידע), מטמיע ומיישם את הנחיות הנוהל, מכין נוהל משרדי, על בסיס המדיניות של משרדו לאבטחת התקשורת ובהתאמה לנוהל מסגרת זה. מבצע ביקורות ובקרות על אופן יישומו. מדווח לממונה הישיר ול״יחידה״ על אירועים חריגים בעלי משמעות אבטחתית.

ה"יחידה הממשלתית לביקורת ואבטחת "מידע-רגיש" במשרד ראש הממשלה (להלן - "היחידה") - יוזמת עריכת ביקורת תקופתית על דרך אבטחת התקשורת והבאת הממצאים לידיעת מנכ"ל המשרד ו"**המועצה לאבטחת מידע רגיש**" (להלן - "**המועצה**").

מנהל מערכות המידע ומנהל התקשורת - אחראים (כל אחד בתחומי תפקידו) - <u>אחריות תפעולית</u> - ליישום נוהל זה.

המבקר הפנימי - אחראי על עריכת ביקורת על דרך יישומו של נוהל זה, במסגרת תכנית העבודה השנתית, תוך התבססות על כלים ממוחשבים לביקורת מערכי המידע ולביקורת האבטחה של מערכי המידע.

המנהל הכללי במשרד - אחראי, אחריות מינהלית כוללת, על יישום הנוהל ועריכת ביקורת על אופן יישומו.

גוף הנוהל

ביצוע תקשורת חיצונית חייב בבחינה ואישור **מראש** ובכתב לביצוע, מאת "הממונה" בכל אחד מהמקרים האלה:

א. אחד (לפחות) מהמחשבים בשני צידי התקשורת החיצונית מסווג כ-"**חסוי**" או כבעל רמת חיוניות בינונית, לפחות, אף אם למידע המועבר בתווך התקשורת אין כלל רגישות של חיסיון.

ב. המידע המועבר בתווך התקשורת החיצונית מסווג כ-"**חסוי**", או "**חסוי-ביותר**".

העסקת יועצים לאבטחת מידע רגיש ומערכי מידע במשרדי הממשלה ומוסדותיה, תיעשה באחריות ה"ממונה" בלבד.

רמת האבטחה המחייבת לאבטחת התקשורת הנה פועל יוצא של רמת הרגישות המירבית התואמת לגבוהה מבין הרגישויות הבאות:

א) מערכי המידע - **רמת החיוניות שלהם, וכן רמת חיסיון המידע** שבהם.
ב) המידע - **רמת החיסיון וכן רמת החיוניות של המידע**.

דוגמא א':
המידע שהמשרד מתכנן להעביר בתקשורת חיצונית נוגע לצנעת הפרט ומסווג כ-"**חסוי**".
רמת החיוניות של מערכי המידע (שנקבעה ע"י הגורמים המוסמכים במשרד) הנה **חיוניות גבוהה** .

רמת האבטחה הנדרשת = כדי לשמור על **רמת חיוניות גבוהה,** תידרש בנוסף ליישום נוהל זה גם הוספת כלים מינהליים וטכנולוגיים לאבטחת מידע ומערכי מידע, מחמירים יותר.

דוגמא ב':
המידע שהמשרד מתכנן להעביר בתקשורת החיצונית הנו - סדר היום של יום עיון אשר נקבע לו סיווג "**בלתי-מסווג**".
סיווג המחשב הנו "**חסוי**" (בשל מידע בסיווג זה האגור בתוכו).

רמת אבטחת המידע הנדרשת = על פי נוהל אבטחת מידע "**חסוי**".

ניתוק הקישוריות בין המשרד לבין תווך תקשורת חיצוני - במקרה של גילוי אירועים או ליקויים שאינם ניתנים לתיקון מיידי ולאיסוף ראיות, או שמסכנים באופן קריטי את המידע הרגיש ואת תפעולם התקין של מערכי המידע, רשאים בעלי התפקיד הרשומים מטה, להורות על **ניתוק מיידי** של מערכי המידע התקשורת, עד להסרת האיום, על פי חוות דעתם של:

א) "הממונה". **ב)** מנהל מערכות המידע. **ג)** מנהל התקשורת. **ד)** המנהל הכללי.

העברה של מידע "**חסוי**" באמצעות מודם ו/או קוו חיוג, בין מחשבים במשרדי הממשלה ומוסדותיה תותר במקרים חריגים וזאת בהתניה כי תיערך קודם לכן בחינה מוקדמת של "**הממונה**" ואישורו

בכתב, כי קיימים ופועלים כהלכה כלי אבטחה טכנולוגיים (הצפנה, סינון וכיוצא בכך) באמצעות כלים "מוקשחים", חתימה דיגיטלית ונוספים - על פי הנחיית "הוראות-שעה") וננקטו גם צעדים מינהליים לאבטחת תוואי תקשורת אלה.

"הממונה" ייעשה שימוש בכלים טכנולוגים לאיתור מודמים "פירטיים" ויהיה ברשותו כל העת מידע עדכני לגבי המודמים (חיצוניים או כרטיסי מודם) שאושרו (בכתב) על ידו.

קיומו של מודם, בתנאים שיפורטו להלן, בחדר שבו קיימת עמדת מחשב, או, "נקודת - קצה" ("חמה"), מבלי שניתן להחזקתו במשרד אישור, מראש ובכתב, מ"**הממונה**", יוגדר בנהלי המשרד כ - **עבירת משמעת חמורה** וזאת בין אם -

1) המודם נרכש על ידי המשרד, או הובא מכל מקור אחר.
2) המודם בנוי על גבי כרטיס בתוך המחשב, או במארז חיצוני.
3) המודם אינו מחובר, או שאינו פועל.

כל היעדים להעברת מידע בתקשורת חיצונית, ממחשב המעבד מידע בסיווג "**חסוי**" - יהיו מאובטחים, לפחות, לרמת "**חסוי**", גם אם סיווג המידע המועבר בתקשורת נמוך מ"**חסוי**". "**הממונה**", אחראי לוודא נושא זה טרם קיום תקשורת חיצונית.

מנהל מערכות המידע במשרד יעביר לידי "**הממונה**" מידע מפורט ומעודכן, אודות פרישת רשת/ות התקשורת הפנימית והחיצונית וידאג לעדכנו באופן שוטף, עפ"י השינויים שיחולו. "הממונה" יבחן מידע זה לאיתור מערכי מידע וקווי תקשורת אשר נעשו ללא הנחייתו האבטחתית ויפעל לתיקון הליקויים.

העברת מידע ונתונים בתקשורת חיצונית, המבוצעת בידי ספק (מיקור חוץ - **OUTSOURCING**, עובדי קבלן וכד') תפוקח אבטחתית **באופן הדוק ותכוף**, באחריות "**הממונה**", בהתאם לנוהל מס' **7** - **קשר עם גורמי חוץ**.

במשרד יימצאו כלים טכנולוגים לניטור וניהול אבטחת התקשורת, בידי שני גורמים, לפחות:

א) "**הממונה**" - הבוחן (על פי תכנית עבודה, או באופן אקראי) את תקינות אבטחת התקשורת.

ב) **נאמן אבטחת התקשורת** - הפועל ליישום נהלי אבטחת המידע ובקרה על פעילותם התקינה

דיווח על אירועים כגון: **א) ניסיונות לחדור אל מערכי המידע**. **ב) חדירה אל מערכי המידע**

קריסה של מערכי המידע - יועבר **<u>מיידית</u>** מהמקור שגילה זאת לראשונה, לגורמים:

1. **עמדת-שירות (HELP DESK)** ובהעדר עמדה זו, אל עובד שישמש "כונן למקרי -חירום" כגון אלה. "הכונן" ידווח לכל בעלי התפקיד הרשומים מטה.

2. ה"**ממונה**" - לידיעה ולהיוועצות, לפי הצורך, עם מומחים בכירים לאבטחת מידע, והנחייה אבטחתית לגורמים **3' ו- 4'.**

3. "**נאמן אבטחת התקשורת**" - לפעולת מיידית (מניעת החדירה ולפעולת מניעה - של אירוע זהה או דומה).

4. **מנהל התקשורת** - לידיעה ופעולה - בדומה לנאמן הביטחון.

5. מנהל "**היחידה**".

אי דיווח לגורמים הנ"ל ייחשב כ**הפרה חמורה של המשמעת**.

העברת סיסמאות כלשהן, בתווך תקשורת חיצוני מותנית בקיום מערכת הצפנה הולמת, על פי אישור מראש ובכתב של "הממונה".

מנהל התקשורת יוודא התקנה ותפעול תקין של מנגנונים הרושמים את תהליכי זרימת המידע

ומאפשרים את ניתוח המידע הזורם, כגון: ניטור פונקציות עקבה בישויות. מנגנונים אלה יפעלו דרך קבע ויזהו פעילויות חריגות ויתריעו עליהן לגורם התפעול וגורם אבטחת המידע.

במקרים מיוחדים ייעשה שימוש במנגנוני מעקב (**TRACE**) לגבי כלל הפעילויות של שירות מסוים, או מעקב אחר משתמש מסוים.

א. העברת מידע "**חסוי**" בתווך תקשורת חיצוני **תהייה מוצפנת**, על פי הנחיית "**הממונה**" ו/או יועץ בכיר מטעמו.

ב. בנתבים (ROUTERS) שבהם קיימת אפשרות להוסמת "**טלאים**" (**PATCHES**) לשיפור אבטחת המידע - חובה על מנהל התקשורת (תוך הכוונה אבטחתית של "**הממונה**") להתקין מנגנוני הצפנה. ההצפנה תיקבע על פי הנחיות "היחידה".

"**הממונה**" יוודא כי יותקנו ויופעלו מנגנונים ואמצעים המאתרים פרצות ברשת ומתריעים על כך. משרד המפעיל רשת **TCP/IP** נדרש להפעיל בקביעות מנגנונים לאיתור פרצות ברשת. ראה: נוהל מס' **30** "אבטחת מידע בשימוש באינטרנט"

הממונה" יוודא כי יותקנו ויופעלו מנגנוני בדיקה המזהים תוכנות מפגע שהוחדרו למערכת, כגון: וירוס, סוס טרויאני, או איומי **JAVA**, ו- **ACTIV-X**.

תנאי חד משמעי לדליית קבצים או תוכנות מגורמי חוץ, באמצעות תקשורת, הנו בדיקת כל החומר שנדלה - במערכת מידע ייעודית/נפרדת, או ברשת נפרדת לחלוטין מהרשת המשרדית, בטרם הפצתה במשרד, ובטרם כל שימוש אחר בקבצים ובתוכנות "שיובאו" למשרד. בין אם בתקשורת ישירה, או באמצעות "מצעי מידע" שהובאו למשרד (בהיתר, או בלעדיו).

אבטחת החיוניות של מערכי המידע

א. מנהל התקשורת, יתקין וישתמש דרך קבע בכלים טכנולוגיים המאפשרים שליטה ובקרה של רשתות התקשורת. מערכות שיאתרו וידווחו, בין היתר, על האירועים האלה: עומסים, תקלות אשר טרם הפכו לקריטיות והשבתת המערכת שלא במועדה.

ב. אבטחת המידע ביישום כלי השליטה והבקרה (אפיון, רכישה, התקנה וכיוצא בכך) תונחה בלעדית על ידי "**הממונה**".

ג. התקנת כלי ניהול ושליטה לשם בקרה או ניהול מרחוק על מערכי מידע, מותנית בבחינה ואישור מראש ובכתב של "**הממונה**", כי הותקנו כלים אבטחתיים הולמים.

היערכות לקראת חיבור מערכי המידע לתקשורת חיצונית (על פי התקן הישראלי מס' 1972 אבטחת מערכות תקשורת, חלק 3) -

נושאים להתייחסות בתהליך תכנון חיבור מערכי המידע לתקשורת חיצונית:

א. מדיניות אבטחת המידע שקבע המשרד (הנגזרת מהקווים-המנחים שקבעה "**המועצה**").

ב. נוהלי אבטחת התקשורת של "**המועצה**".

ג. רמת אבטחת המידע הנדרשת (על פי סקר הערכת סיכונים והצלבת ממצאיו עם ממצאי תהליך מיפוי וסיווג "**המידע-הרגיש**" ומערכי המידע).

ד. רמת האבטחה המירבית, של רכיבי הרשת, בפועל, על פי ממצאי בדיקת אבטחת איכות מגורם טכנולוגי לתקינת אבטחת מידע, בארץ או בחו"ל, אשר יאושר על ידי "**המועצה**".

ה. ארכיטקטורת הרשת.

ו. פריסה פיסית ולוגית של הרשת.

ז. סוגי פרוטוקולי התקשורת

ח. מנגנוני האבטחה ומיקומם.

ט. שימוש בכלי אבטחה לצורך גילוי ומעקב אחר חדירות ופעולות בלתי מורשות ברשת.

י. ניהול ההרשאות להתחברות לתווך תקשורת חיצוני;

י"א. ניטור השימוש בתקשורת לתווך חיצוני;

י"ב. טיפול בחריגים;

י"ג. הגדרת מנגנוני האבטחה לרכיבי רשת התקשורת;

י"ד. הגנת המידע המועבר בתווך התקשורת;

פעילויות מערכת אבטחת המידע בעת התחברות המשרד לתקשורת חיצונית -

א. אימות זהות (AUTHENTICATION) - פעילויות שנועדו לאשר שהמשתמש אשר מתקשר
למערכת הוא אמנם המשתמש האמיתי.

ב. אישרור (CERTIFICATION) - בדיקה ואישור הרשאות הגישה למשתמש.

ג. בקרת גישה (ACCESS CONTROL) - הגנה מפני שימוש לא מורשה במשאבי הרשת.

**ד. מניעת השבתה (מלאה או חלקית) של השירות (DENIAL OF SERVICE PREVENT)
של מערכי המידע.**

ה. שמירת סודיות/חיסיון המידע - הגנה מפני חשיפה לא מורשית של מידע "חסוי"
המועבר ברשת התקשורת.

ו. שמירה על שלמות ואמינות הנתונים (DATA INTEGRITY) - מפני שינוי במזיד של
המידע והנתונים, העלול להתבצע דרך תווך התקשורת החיצונית.

ז. אבטחת זמינות המידע

ח. ניטור, ניתוח ותגובה - מעקב ורישום פעילויות ברשת, ניתוח הפעילויות וגילוי אירועים
חריגים וייצור תגובה מתאימה לטיפול באירוע.

טכנולוגיות המומלצות ליישום אבטחת המידע -

א. חציצה / מידור

1. מיתוג אלקטרו - מכני (בין שתי רשתות שונות) בשילוב עם חלוקת הדיסק הקשיח לשני
אזורי אחסון בסיווג שונה (וגם "אזור מעבר"), כדי לאפשר העברת מידע בין האזור הציבורי
(שאינו רגיש) אל האזור המאובטח בדיסק, ומניעת האפשרות להעביר מידע בכיוון ההפוך.

**שיטה זו נבחנה ואושרה על ידי "המועצה", למטרת מידור בין רשת בלמ"סית לבין רשת בסיווג
(מירבי) "חסוי".**

2. מפסק A-B, המאפשר קישור בין המחשב לבין רשת אחת בלבד, מתוך שתיים, או יותר

(בעלות סיווג שונה), כדי למנוע קישור ישיר בין רשתות בסיווג שונה.

ב. כרטיס זיהוי אלקטרוני (SMART-CARD) - כרטיס המספק קוד משתנה לצורך אימות המשתמש המנסה להתקשר למערכת. יש להרחיב את יישומו לבקרת גישה לבסיסי מידע בעלי חיוניות בינונית, או גבוהה. יהווה אחד מתנאים (זיהוי אמין) לעבודה מהבית.

ג. מנגנונים לאישור זהות (AUTHENTICATION) - והרשאה. הבקשה נשלחת לשרת המאמת את זהות המשתמש. השרת מבצע הרשאה ורישום של הפניות.

ד. חתימה דיגיטלית - מנגנון שבו העובד, יוצר המידע, "חותם" על המידע המועבר. העובד, מקבל המידע, המידע מאמת את זהות ה"חותם" ואת שלמות המידע באמצעות אימות החתימה.

ה. יישומי חתימת קבצים.

ו. הצפנה - טכנולוגיה המבטיחה את סודיות המידע המועבר ברשת.
[הטיפול בנושא הצפנת מידע "חסוי" במשרדי הממשלה ומוסדותיה תהיה על פי נהלי ה"מועצה"].

ז. מנגנוני איתור ואתרעה בנקודות פגיעות - יופעלו מנגנונים הרושמים תהליכי זרימת מידע ומאפשרים ניתוח המידע הזורם, כגון: **מוניטור חיצוני**; **פונקציות עקבה (TRACE)** בישויות.

ח. השארת מנגנון עקבה (**TRACE**) פתוח מהווה סיכון אבטחתי בהיותו מאפשר "שליפת מידע". לכן, העובד המוסמך הפעילה, חייב לסגור אותה, מיד עם תום השימוש.

ט. הפעלת מנגנונים המחפשים פרצות ברשת ומתריעים על כך.

י. העברת מידע בפרוטוקול אמין
השימוש בפרוטוקול אמין עשוי לתרום לאבטחת שלמות המידע ולאמינותו, תוך שימוש במנגנוני אבטחה מתאימים סיכום ביקורת (**CHECKSUM**) שידור חוזר, ספרור יחידות מידע וכדומה.

יא. הגברת היתירות בעזרת הזרמת מידע בדרכים חלופיות
שימוש בדרכים חלופיות כגון: חיוג כדרך חליפית לקו נל"ן או מנגנוני אבטחה מתאימים כגון: סיכום ביקורת (**CHECKSUM**) שידור חוזר, ספרור יחידות מידע וכדומה.

י"ב. ניהול רשת בתווך מקביל לתווך שבו זורם המידע הכללי (OUT OF BAND) הזרמת המידע הנוהלי של הרשת דרך ערוץ שונה מאשר ערוצי המידע הרגילים. על ידי כך לא יוכל המתקיף להשתלט על נתוני הבקרה כאשר הוא משתלט על ערוצי המידע.

י"ג. מיפוי טכנולוגיות אבטחה מול פעילויות.

יד. אבטחה לאימות זהות (AUTHENTICATION)
1. חתימה דיגיטלית;
2. שרת אימות זהות (AUTHENTICATION SERVER).

ט"ו. אבטחה לאישרור (CERTIFICATION)
1. שימוש בחתימה דיגיטלית;
2. נעילת רכיבים המאפשרים שינוי מנגנוני ניתוב;
3. נעילת רכיבים טעוני סיכון בישויות, כגון: רכיבי פרוטוקול או תוכנות - המאפשרות גישה לישות ללא הרשאה;
4. יש נעילת מודולים של תוכנה אשר עברו את תהליך פתיחת - השיח (**LOGIN**).

ט"ז. אבטחת האמינות והשלמות של המידע והנתונים
1. יישומו באמצעות חתימת דיגיטלית
2. יישומו באמצעות חתימת הקבצים

י״ז. אבטחה לזמינות המידע

1. הגנה על מנגנוני הניתוב
2. הזרמת מידע בעל חיוניות גבוהה בדרכים חלופיות
3. הפעלת מערך ניהול הרשת בתווך מקביל לתווך שבו זורם המידע הכללי - **(OUT OF BAND -)**
4. נעילת מנגנונים, בפרוטוקולים או תוכנות המאפשרים ״הצפת״ הרשת.

יש להכין תיעוד מלא לגבי הפריסה הפיזית של התקשורת במשרד, כולל: ארונות תקשורת, ניתובים, מחברים, קופסאות סעף וכו׳. החומר יישמר וינוהל באגף למערכות מידע וענ״א.

ניתוב קווי התקשורת יתבצע בתוך תעלות סגורות, ללא פתחים. קופסאות סעף יהיו תמיד סגורות. גישה וטיפול בניתובים או בארונות תקשורת, רק באישור ובבקרת יחידת המחשב.

אין לאפשר כניסה אוטומטית לתוך המערכת בתקשורת חיוג. שירותים בחיוג יתאפשרו תחת מגבלות של שימוש בשם המשתמש, סיסמאות, חיוג חוזר או כל מנגנון אחר.

אין לאפשר ביצוע תחזוקה מרחוק בתקשורת למחשב המרכזי, ע״י חברה חיצונית. יש לעגן את הנושא בחוזה השירות למחשב, כדי להבטיח תחזוקה במקום.

השירות הרגיל למשתמש המחשב יינתן בשעות הפעילות הרגילות שיוגדרו בהנחיות שיפורסמו ע״י הממונה לאבטחת מידע. מחוץ לשעות אלו – תיחסם התקשורת.

נאמן אבטחת מידע יוכל לפנות בשעות הפעילות למנהל אגף מערות מידע, בבקשה להאריך את זמן התקשורת. בידי אחראי ההפעלה תהיינה הנחיות מדויקות בדבר האפשרות להיענות או לא להיענות לפניה. במידה ותהיה היענות לבקשה, היא תותר רק למבקש וכל שאר המערכת תיחסם.

על כל פעילות חריגה שאושרה ובוצעה, ידווח ע״י האחראי לאבטחת מידע במשרד ולממונה אבטחת מידע במשרד.

מסוף שלא בוצעה ממנו כל פעילות במשך 30 דקות – ינעל ויתבצע logout אוטומטי מהמחשב. הפעלה מחדש תחייב הזדהות חוזרת מלאה.

לאחר חמש דקות של אי פעולה מהמסוף, יתבצע כיבוי מסך, במידת האפשר.

אין לאפשר ביצוע פעילויות system בתקשורת, כולל הפעלת מנגנונים כמו: העתקה, גיבוי וכיוצא באלה.

מקורות

נהלי מסגרת – אבטחת מידע רגיש ומערכות מידע. משרד ראש הממשלה, אגף בכיר לביקורת המדינה וביקורת פנימית, מאי 2000.

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

נוהלי אבטחת המידע בעיריית ירושלים, פברואר 2001.

מכון התקנים הישראלי, תקן מס׳ 1972 - אבטחת מערכות תקשורת, חלק 3 - היערכות ארגונים לקראת התחברות לתווך תקשורת חיצוני.

אבטחת מידע בשימוש באינטרנט

נוהל מס' 34

מבוא

משרדי הממשלה ומוסדותיה נערכים כיום לשימוש מואץ בתקשורת האינטרנט, כתווך יעיל וזול לקישור פנימי בין משרדי הממשלה ומוסדות ציבור אחרים, וכן לתקשורת בין הגופים הנ"ל לבין גורמים עסקיים בארץ ובחו"ל, או עם אזרחים.

קישור זה טומן בחובו, סכנות חמורות לתפקודם התקין של מערכי המידע שבאחריות המשרד ולניהול משק המדינה ,באם הקישור לא נעשה באופן מאד מאובטח.

הסיכונים ש"**המועצה לאבטחת מידע רגיש (להלן - "המועצה")** צופה הם קריטיים, מיידיים ועשויים להביא לידי קריסתם של מערכי המידע ולמוטט עימם (תופעת ה"דומינו") מערכות משקיות נוספות הקשורות עימם.
את ממדיה החמורים של קריסה זו קשה לאמוד מראש והיא מהווה לנו בסיס להנחות אלה:

א. לכל אחד משימושי האינטרנט קיימים סיכונים ייחודיים המחייבים נקיטת אמצעים טכניים ומינהליים מחמירים, **הרבה יותר מאלו שבהם נקטו המשרדים עד כה**.

ב. עצם הרכישה של כלי הגנה טכנולוגיים (כגון: **FIRE-WALL** (להלן- "**FW**" ואח') אינה מהווה "מרשם קסם" לאבטחת מידע. נקיטה בצעד זה חייבת להיעשות ביוזמת "**הממונה על אבטחת המידע**" ("**הממונה**") ובסיוע של יועץ מקצועי בכיר אשר יסייע ל"**ממונה**" באפיון הכלי (טרם רכישתו), בהתקנתו
המקצועית (כולל כיוון הכלי (CONFIGURATION) ובביצוע עדכונים שוטפים ותחזוקה מונעת, שאילולא
כן תתקבל במקום אבטחה - "**אשליה אבטחתית**"!.

ג. בשל השינויים התכופים המתרחשים בשטח תקשורת המידע בכלל, ובשטח האינטרנט וייושמיו, בפרט, ובשל השוני הרב שבין ארכיטקטורה של מערכת מידע אחת למשנה, אין נוהל זה מתאר את הצעדים הנדרשים ליישום ברמת המיקרו (כגון: כיצד יש לתכנן בפירוט את הסינון של "**קיר-אש**").

ד. "**הממונה**" יעגן בנהלים הפנימיים במשרדו את הסייגים וההיתרים לשימוש נאות ברשת האינטרנט. דגש יושם על כללי אתיקה ומשמעת ההולמים את השירות הציבורי. תוך ציון איסור מפורש על ניסיונות חדירה ללא היתר למחשבים של גורמים פרטיים, מסחריים, ממשלתיים ואח', וניסיון או ביצוע פעולות האסורות על פי חוק המחשבים, התשמ"ה - 1985.

ה. "**הממונה**" יביא לידיעת כל המורשים להשתמש באינטרנט במשרד את האיסור המוחלט ליצור קשר, או לנסות לפגוע באתרים של כל גורם פרטי, מסחרי, ממשלתי מחקרי צבאי ואחר, הממוקמים במדינות המוגדרות כעוינות למדינת ישראל או בכל מקום אחר.

ו. בכל ההחלטות והפעילויות הנעשים במשרדים, לשם חיבורם לרשת האינטרנט, יקבלו שיקולי האבטחה על המידע ומערכי המידע **העדפה מערכתית ובלתי מתפשרת, על פני שיקולי נוחות ושיקולים כספיים** ועל מערכות המשוב והבקרה הטכניות ובעיקר המינהליות להגיב, באופן נמרץ ומיידי (**!**) על אירועים חריגים.

ז. "**המועצה לאבטחת מידע רגיש**" הנה הגורם הממשלתי המוסמך לקבוע היתרים או סייגים לאבטחת "מידע רגיש" בממשלה ומוסדותיה. בכל מקרה של סתירה בין הנחיות קיימות של גורמים שונים בממשלה ומוסדותיה או פורומים ממשלתיים בתחום התקשורת - לבין נהלי "**המועצה**", **יועדפו נהלי "המועצה"**.

הגדרות

"**אבטחת מידע לשם חיבור המשרד לאינטרנט**" - כלל הפעילויות הננקטות על ידי משרד המבקש להתחבר לצרכים ראויים שונים לאינטרנט, המיועדות לשמור על חיסיונו של "**מידע רגיש**" ושמירה על חיוניותם של מערכי המידע והמידע עצמו (אף אם אינו רגיש בהיבטי חיסיון).

"תקשורת מאובטחת לאינטרנט" - הנה זו ש"**הממונה על אבטחת** "**מידע רגיש**" (להלן - "**הממונה**") אישר את מימושה. תקשורת שלא אושרה על ידי "**הממונה**" **אסורה לחלוטין.**

"אמצעי לחציצה מאובטחת" - אמצעי אשר נבחן אבטחתית ואושר על ידי "המועצה", המבוסס על חומרה,

והמאפשר מיתוג מאובטח בין רשת תקשורת בסיווג "חסוי" לבין רשת ציבורית בלתי מאובטחת, כגון: אינטרנט, טלפוניה ואח'.

מטרות הנוהל

נוהל מסגרת זה יגדיר את הסייגים, ההיתרים, השיטות והכלים הנדרשים ליישום במערכי תקשורת המידע במשרדי הממשלה ומוסדותיה לשם ביטול או צמצום רב של הסיכונים הייחודיים הנובעים מחיבור מערכי תקשורת המידע [שבאחריותם] לרשת ה"**אינטרנט**".

אחראי לביצוע הנוהל

ע"פ החלטת המועצה לביטחון לאומי והחלטת ממשלה מספר ב/84 מיום 11.12.2002 הגוף האחראי למתן הנחיות בנושא אבטחת מידע לכלל משרדי הממשלה, הינה הרשות הלאומית לאבטחת מידע (בהקמה). הגוף יהיה אחראי גם לגופים אשר אינם מונחים ע"י שב"כ. הנחיות הרשות גוברות על הנחיות פרק זה.

"הממונה" - מהווה סמכות מקצועית-מינהלית בכירה להכנת תוכנית אבטחת התקשורת (בתיאום עם מנהל מערכות המידע), מטמיע ומיישם את הנחיות הנוהל, מכין נוהל משרדי על בסיס מדיניות שקבע משרדו לאבטחת התקשורת, ובהתאמה לנוהל מסגרת זה. "הממונה" מבצע ביקורות ובקרות על אופן יישומו של הנוהל ונהלי המשרד. מדווח לממונה הישיר על אירועים חריגים בעלי משמעות אבטחתית. מעדכן את **מנהל "היחידה"** אודות "אירועים חריגים".

ה"יחידה לביקורת ואבטחת "מידע-רגיש" במשרד ראש הממשלה (להלן **-"היחידה") -** יוזמת עריכת ביקורת תקופתית על דרך אבטחת התקשורת והבאת הממצאים לידיעת מנכ"ל המשרד ו"**המועצה לאבטחת מידע רגיש**" (להלן - "**המועצה**").

מנהל מערכות המידע ומנהל התקשורת - אחראים, כל אחד בתחומי תפקידו**, אחריות תפעולית** ליישום נוהל זה.

המבקר הפנימי - אחראי על עריכת ביקורת פנימית על דרך יישומו של נוהל זה, כחלק אורגני מתכנית העבודה השנתית, תוך התבססות על **כלים ממוחשבים ייעודיים** לביקורת.

המנהל הכללי במשרד - אחראי, אחריות מינהלית כוללת, על יישום הנוהל.

גוף הנוהל

חל **איסור מוחלט** לביצוע תקשורת ישירה בין רשת מסוג "**אינטרנט**" לבין מערכי המידע הפנימיים במשרד, בכל אחד מהמקרים האלה:

א. מערכי המידע מעבדים, מאחסנים, או יוצרים - מידע בסיווג "**חסוי**", אך אין בהם **אמצעי ל"חציצה -מאובטחת"** או ש"**הממונה**" לא בחן ואישר את הקישור לאינטרנט.

ב. המחשב מעבד, מאחסן או יוצר מידע בסיווג "**חסוי-ביותר**".

ג. מערכי המידע, הנתונים, התוכנות, או המידע (אף אם אלה אינם חייבים בחיסיון) – מסווגים כבעלי חיוניות ברמה אמצעית (או גבוהה) לניהולו התקין של המשרד, או, לניהול משק המדינה.

ניתוק הקישוריות בין המשרד לבין תווך תקשורת חיצוני - במקרה של גילוי "**אירועים חריגים**" או ליקויים שאינם ניתנים לתיקון מיידי ולאיסוף ראיות, או שמסכנים באופן קריטי את "המידע

הרגיש״ ואת תפעולם התקין של מערכי המידע, רשאים בעלי התפקיד הרשומים להלן, להורות על **ניתוק פיזי וממיידי** של מערכי המידע מקווי התקשורת, עד להסרת האיום:

א) ״הממונה״. **ב)** מנהל מערכות המידע. **ג)** מנהל התקשורת. **ד)** המנהל הכללי.

אחד מהעקרונות אשר יש ליישם בעת התחברות מאובטחת עם רשת האינטרנט, הנו - ״**הפרדת המערכות**״. משמע - **נתק מוחלט בין רשת האינטרנט לבין מערכי מידע שבמשרד**.

יפורטו להלן מספר שיטות אבטחה העונות על עקרון ״**הפרדת המערכות**״:

א.הקמת עמדת עבודה עצמאית ובלתי-מקושרת STAND ALONE (להלן- ״מחשב - S.A״)
(העמדה מהווה מסוף מקומי של האינטרנט) אשר תופעל על פי כל התנאים שלהלן):

1. מחשב - **S.A** לא יקושר לרשת פנימית במשרד, בכל אחד מהמקרים הבאים:

א) הרשת משמשת למעבר של ״**מידע-רגיש**״ בסיווג ״**חסוי**״ או ״**חסוי-ביותר**״.
ב) הרשת ומערכי המידע המזינים אותה הנם בעלי **חיוניות בינונית, או גבוהה** לניהול המשרד או, לניהול משק המדינה.

2. העמדה תמוקם רק בחדר או במתחם שבו אין ״**נקודות קצה**״ [**PORTS**] ״חמות״ פנויות של הרשתות ״הרגישות״ במשרד.

3. בזיכרון הקבוע של ״מחשב - **S.A** לא יעובד ולא יאוחסן מידע בסיווג ״חסוי״ או ״חסוי-ביותר״.

4. בחדר (או במתחם) שבו קיים ״מחשב - **S.A**״ לא יימצא מצע-מידע נתיק (דיסקט, טייפ, כונן -JAZ, **C.D** וכיוצא בכך) בסיווג ״**חסוי-ביותר**״.

5. ״**הממונה**״ יעגן בנהלים פנימיים של המשרד את האיסורים הנ״ל.

ב. הקמת רשת אינטרנט פנים-ארגונית, שאינה מחוברת למערכי מידע ״רגישים״, פנימיים או חיצוניים, או לרשתות בעלות רמת חיוניות גבוהה. יישום של תקשורת מאובטחת ברשת מסוג זה מותנה בכך שכל מַחְבָּרי הכבילה לסוגיהם יהיו **שונים לגמרי** ממחברי הרשתות הרגישות. זאת כדי למנוע מהעובדים או מאנשי התפעול והתחזוקה, אפשרות לקשר (בשגגה או בזדון) בין רשת האינטרנט הפנימית, לבין רשתות ומערכי מידע המעבדים ״**מידע רגיש**״ (בתוואי ניתוב כבלי הרשת, או בחדרים של ״**משתמשי קצה**״).

ג. מידור/חציצה במקום ובזמן באמצעות כלי אבטחתי (עיבוד שתי רמות סיווג שונות במחשב **pc** אחד)

1. על אף האמור בסעיף **14-א׳** לעיל, על פיו נאסר לעבד או לאחסן ״**מידע רגיש**״ בכונן הקבוע של ״**מחשב - S.A**״, קיימת שיטה מאובטחת, אשר תתואר להלן, הנסמכת על כלי אבטחתי [מבוסס על מיתוג בחומרה], המאחד את שתי השיטות שנמנו לעיל.

2. לשיטה זו מספר יתרונות אשר הנם:

א. ביטול הצורך להתקין מחשב נפרד [״**מחשב - S.A**״] על מנת להיות מקושר לרשת האינטרנט.

ב. ״**משתמש הקצה**״ יכול לעבוד לסירוגין ובאופן מאובטח, ברשת תקשורת בסיווג ״**חסוי**״ או ברשתות ציבוריות כגון: אינטרנט, רשת הטלפונים ואח׳.

ג. בחלופה זו נעשה שימוש בחלוקת הדיסק הקשיח לשלושה אזורים נפרדים, המאפשר הקצאת ״אזור מאובטח״ לאחסון מידע ״**חסוי**״, ״אזור -מעבר״ שינוצל לבצוע תהליכי ביניים כגון: בדיקת וירוסים למיניהם, וכן ״אזור ציבורי״ אליו תחובר רשת ציבורית כגון: אינטרנט, קווי חיוג ואח׳.

ד. מתאפשרת העברה מאובטחת של מידע מ״**האזור-הציבורי**״ (שאינו ״רגיש״) אל ״**האזור המאובטח**״, ולחילופין נמנעת האפשרות להעביר ״**מידע-חסוי**״ בכיוון ההפוך.

3. שיטה זו נבחנה ואושרה אבטחתית על ידי "**המועצה**", לשימוש בכל משרדי הממשלה ומוסדותיה עליהם חלים נהלי "המועצה". יישומה ייעשה באחריות "**הממונה**".

4. שיטה זו לא תיושם למיתוג בין **רשת האינטרנט** לבין מחשבים ורשתות בסיווג "**חסוי -ביותר**", או שהם הוגדרו כ"**חיוניים ברמה גבוהה**" לניהול המשרד או של משק המדינה לדוגמא: שע"ם, בחן, רשב"ג, "אביב", ו"נמר". בחדר שבו יש נקודת קצה של אחת מהרשתות הללו לא תימצא נקודת קצה לרשת האינטרנט, או המאפשרת בעקיפין קישור אליה.

"יבוא" מאובטח של קבצים ותוכנות מהאינטרנט ו/או שילובם במערכי המידע

א. קיימים סיכונים רבים, מיידיים וחמורים ביותר בתהליך ה"**הורדה**"/"**היבוא**" והפתיחה של קבצי מידע ותוכנות (או מיזוגים שלהם) מה"אינטרנט" וטיפול בהם במערכי המידע במשרד. נוהג אשר מקובל היה עד כה על רבים ממשתמשי האינטרנט.

ב. האיומים חלים הן על **חיסיון המידע** (הקיים במערכי המידע) וגם על **החיוניות של המידע ומערכי -המידע**, כמשאבים קריטיים לניהול המשרד ולניהול משק המדינה.

ג. אבטחת מצעי-מידע המכילים מידע (מכל סוג, כגון: טקסטואלי, גרפי ואח'), או קבצים המכילים טקסט, תמונה, קול, תוכנות, מיזוג בין אלה וכל סוג אחר של נתונים אשר "יובאו" מהאינטרנט בעמדת **מחשב - S.A**, תיעשה כדלהלן:

באחריות מנהל מערכות המידע תופעל מערכת ייעודית לאיתור, זיהוי, ו"ניקוי" מצעי -המידע מפגעי תוכנה. תפעול עמדת בדיקה ייעודית זו מותנה בקיום פונקציות טכנולוגיות ומינהליות, כמפורט להלן:

א. מחשב מערכת הבדיקה לא יהיה מקושר לרשתות כלשהן, פנימיות או חיצוניות.

ב. טרם הבדיקה והקביעה כי "**מצע-המידע**" אינו מכיל וירוסים ופגעי אינטרנט למיניהם, יש להדביק על "מצע-המידע" מדבקה בזו הלשון: **מכיל קבצים / תוכנות "מיובאים" - טרם נבחנו וירוסים !!**

ג. "**מצעי-מידע**" שטרם נבחנו - יאוחסנו בנפרד מ"**מצעי-מידע**" "נקיים" שנבחנו.

ד. מפעיל עמדת הבדיקה ינהל יומן (רגיל או ממוחשב), בו יפורטו: מספרי זיהוי של מצעי-המידע, סוגי הוירוסים שנתגלו, סוג הטיפול שניתן לניקוי הוירוס וכיוב', מועד הבדיקה החוזרת שנערכה לוודא כי מצע המידע אכן "**נקי**" מווירוסים, הגורמים שלהם דווח על הווירוסים, פרטי הבודק וחתימתו.

ה. "**מצעי מידע**" לעניין זה משמע - דיסקטים, דיסקים (ניידים או כחלפים), סרטים וכיוב' שהובאו למשרד מכל מקור שהוא.

כל העובדים שהוגדרו על ידי הנהלת המשרד כבעלי זכות גישה לאינטרנט יאשרו בחתימת ידם על גבי טופס התחייבות משרדי-רשמי על התחייבותם למלא אחר ההנחיות הבאות:

א) קיים איסור מוחלט על פתיחת קבצים או תוכנות ממקורות שאינם מוכרים לעובד.

ב) הורדת קבצים ותוכנות תיעשה רק אל דיסקט אשר יועבר ל"עמדת בדיקה ייעודית" לגילוי פגעי אינטרנט, או לאישור "ניקיונם".

ג) הכנסת מצעי-מידע מגנטיים או אופטיים לתחומי המשרד, מותרת רק לאחר שעברו בדיקה מחמירה בעמדת הבדיקה הייחודית שבמשרד, והודבקה עליהם תווית רשמית המאשרת זאת

ד) השימוש ברשת האינטרנט ייעשה על פי כל הנחיות של מינהל ואתיקה שנקבעו בתקשי"ר.

העובד לא ייעשה שימוש ביישומים מסוג JAVA או ACTIV-X האסורים לשימוש מאובטח ברשת האינטרנט !

"**הממונה**" יוודא כי הותקנו והופעלו מנגנוני בדיקה המזהים תוכנות מפגע שהוחדרו למערכת, כגון: וירוס, סוס טרויאני, או איומי **JAVA**, ו- **ACTIV-X**.

אבטחת החיוניות של אתר אינטרנט -

א. לאתר אינטרנט אשר עוצבה עבורו "סביבת אינטרנט מאובטחת" [ללא קישור לרשתות רגישות או למידע "**חסוי**", או "**חסוי-ביותר**"], **עדיין נשקפים סיכונים !**

ב. סיכונים אלה מיוחסים דווקא לחיוניות האתר.

ג. הפעילויות האבטחתיות שעל מנהל אתר האינטרנט, או מנהל מערכות המידע ליישם במשרד, מיועדות לסכל או לצמצם את התרחישים, אשר יתוארו להלן, לפגיעה באתר:

1. סתימת האתר ע"י דואר "זבל" "JUNK-MAIL"

2. **שינוי התכנים** שנקבעו באתר בתכנים סתמיים או שגויים ומטעים במכוון, העלולים להביך את המשרד בעיני הציבור ובעיני גופים עמיתים, בארץ ובעולם.

3. הוצאת האתר או מערכת המידע מכלל שימוש.

4. שתילת וירוסים ומפגעים אחרים בשרת עמדת האינטרנט.

5. התחזות כגורם מוכר אחר לביצוע פעילויות אסורות על פי החוק ונהלי המשרד.

על גבי מסגרת מסך עמדת האינטרנט יש לקבוע שילוט ברור בזו הלשון:

עמדת אינטרנט - אסור לטפל במידע "חסוי-ביותר", או להתחבר למערכי-מידע בעלי חיוניות בינונית או גבוהה !!

העסקת יועץ חיצוני לאבטחת התקשורת עם האינטרנט:

א. העסקת יועץ (בכיר) חיצוני בתחום אבטחת המידע, תיעשה באמצעות "**הממונה**" בלבד ! ה"ממונה" יהיה הגורם **היחיד** אשר יכווין את פעילותו של המומחה הנ"ל.

ב. מימון העסקת "יועץ" כאמור לעיל, יהווה סעיף-משנה בסעיף תקציבי ייחודי, המיועד לכלל פעילויות אבטחת המידע - והנמצא ברשות ה"ממונה".

ג. המלצות היועץ יתועדו על ידי "**הממונה**" והוא רשאי ליישמן.

ד. יועץ לאבטחת מידע לא יספק באותה עת שירותי ייעוץ במשרד, בתחומים אחרים ולבעלי תפקיד אחרים, שאינם קשורים במישרין לאבטחת מידע (כגון: תכנון, אפיון, תכנות ואח' של מערכי מידע (ונתונים), ומערכי תקשורת מידע.

ה. באחריות "הממונה" לוודא כי "היועץ" יתחיל בעבודתו ותהייה לו גישה לנוהלי המשרד ולמסמכים "רגישים" אחרים, **רק** לאחר ביצוע פעולות מינהליות מקדימות שיפורטו להלן:

1. בחירת "**היועץ**" תיעשה תוך בחינה קפדנית של: השכלתו, כישוריו, ניסיונו המוכח בייעוץ ובהטמעת המלצותיו ועבודות שביצע עבור גופים ציבוריים. בתהליך הנ"ל יתייעץ "**הממונה**" עם עמיתים לתפקיד במשרדים אחרים.

2. מרכיב השכר יילקח בחשבון **רק** בתום התהליך, כאשר יוותרו רק יועצים אשר לדעת

"**הממונה**" הוכחו כישוריהם ויכולתם לסייע ל"ממונה" באיכות גבוהה.

3. היועץ קיבל הכשר בטחוני מהממונה הארצי על הביטחון במשרד (קב"ט).

4. היועץ חתם בנוכחות הקב"ט, או עובד מטעמו, על הצהרה לשמירת סודיות.

"**הממונה**" ינחה את הגורמים המקצועיים בתחום מערכי המידע (כגון: מנהל מערכות המידע, מנהל התקשורת ונאמני אבטחת המידע וגורמים טכניים ומינהליים רלוונטיים נוספים) ואת כל "**משתמשי-הקצה**" בארגון לגבי הסייגים וההיתרים לשימוש ברשת האינטרנט.

מומלץ לרכוש וליישם תוכנה אבטחתית אשר מזהה מסמכים "רגישים", בעלי **שדה-סיווג** . תוכנה זו אמורה למנוע העברה בתקשורת של מסמך "**חסוי**" או "**חסוי-ביותר**" אשר הגיע בטעות לסביבת עמדת האינטרנט או למחשב עצמו.

לעניין דיווח על אירועים כגון: **א) ניסיונות לחדור אל מערכי המידע. ב) חדירה אל מערכי המידע, ג) קריסה של מערכי המידע** - ראה: נוהל מס' **29 - אבטחת התקשורת.**

העברת סיסמאות בתווך חיצוני מסוג אינטרנט מותנית בקיום מערכת הצפנה הולמת, על פי קביעת **הממונה".**

לעניין התקנה ותפעול של מנגנונים הרושמים את תהליכי זרימת המידע ומאפשרים את ניתוח המידע הזורם - ראה: נוהל מס' **29 - אבטחת התקשורת.**

כל העברת מידע "**חסוי**", במידה ותאושר על ידי "**הממונה**", תהיה חייבת בהצפנה, על פי תבחינים שיקבעו ע"י "**הממונה**". בנתבים **(ROUTERS)** שבהם קיימת עתה האפשרות להוספת "**טלאים**" **(PATCHES)** להצפנה - חובה על מנהל התקשורת, ביחד עם מנהל מערכות המידע להתקין מנגנוני הצפנה, תוך הכוונה אבטחתית של "**הממונה**".

"**הממונה**" יוודא כי יירכשו, ויופעלו מנגנונים ואמצעים המאתרים פרצות ברשת ומתריעים על כך. משרד המפעיל רשת **TCP/IP** נדרש להפעיל בקביעות מנגנונים לאיתור פרצות ברשת.

הממונה הארצי על הביטחון במשרד (קב"ט) יבדוק [מהימנותית] את ספקי השירותים למיניהם, בתחום תקשורת האינטרנט - כתנאי ובטרם ההתקשרות עימם.

הטמעת נושא אבטחת המידע באינטרנט במסמך מדיניות אבטחת המידע של המשרד

א. אבטחת המידע בתקשורת האינטרנט תוגדר במסמך הנ"ל כ"**חיונית**" באופן קריטי לניהול המשרד. עובדי המשרד נושאים באחריות-אישית לאבטחת המידע המצוי באחריותם. המסמך הנ"ל יובא לידיעת כל העובדים במשרד.

ב. "עובדי המשרד" - עובדים בכל תפקיד ובכל מעמד, במיוחד עובדי היחידה למערכות מידע כולל אלה המועסקים בחוזה.

עבודה מהבית באמצעות האינטרנט:

פעילות זו, אם וכאשר תתבקש, תותר בהתאם לסייגים אלה -

א. מנהל מערכות המידע או מנהל התקשורת יפנו אל "**הממונה**" ויציגו בפניו את מירב הפרטים אודות המיזם. "**הממונה**" יבחן את כל הפרטים המשפיעים על רמת אבטחת המידע ושיטות האבטחה הנגזרות ממנה (רמת חיסיון המידע שיועבר בתווך, רמת חיסיון המידע במחשב המשרד, רמת חיוניות המחשב במשרד וכיוב').

ב. העברת של מידע בין המשרד לבית העובד או אתר דומה אחר, באמצעות רשת האינטרנט **אסורה לחלוטין** במקרים הבאים:

1. המידע המיועד להעברה בתווך האינטרנט מסווג כ- **חסוי-ביותר**".
2. המידע שבמחשב המשרד מסווג כ- "**חסוי-ביותר**".
3. חיוניות המידע שבמחשב המשרד הוגדרה כ**חיוניות גבוהה** (לניהול המשרד או לניהול משק המדינה) - על פי קביעת המשרד - ראה פרק 1.3 **מיפוי וסיווג מידע ומערכי -מידע**.

ג. במקרה ו"**הממונה**" יתיר להעביר מידע בסיווג "**חסוי**" בין המשרד לבין הבית, באמצעות האינטרנט, יידרשו כתנאי לתקשורת זו, בין היתר, רכישה ותפעול של האמצעים האלה:

1. הצפנת המידע (בשיטות שיהלמו את הסיכון למידע בתווך ולמידע במחשב המשרד) ועל פי תבחינים אבטחתיים שתקבע "היחידה".

2. אמצעי הזדהות טכנולוגי מתקדם ואיכותי (כרטיס חכם" משולב בסיסמה).

3. האמצעים הנ"ל ייקבעו בלעדית ע"י "**הממונה**", בהתאם לנהלים ול"הוראות השעה" של "**המועצה**".

פרוייקט תהיל"ה - אבטחת התקשורת באמצעות האינטרנט:

פרוייקט **היערכות ישראל לעידן המידע** ("**תהיל"ה**") מיועד , בין כלל תפקידיו, ליצור תשתיות תקשורת ["**ממשל זמין**"], בין משרדי הממשלה לבין תושבי המדינה.

ככלל, תתאפשר לפונים באמצעות האינטרנט אך ורק "**הצבעה**" על שאלות מובנות וסגורות אשר ייבחרו מתוך "**תפריט סגור**".

בשום מקרה, ללא יוצא מן הכלל, לא תותר לגורמים מחוץ למשרד לבצע **שאילתות פתוחות** מתוך בסיס המידע של המשרד (גם אם הוא בסיס מידע ייעודי לנושא שאילתות ולא בסיס המידע התפעולי של המשרד).

בכל מקרה שבו תידרש הפקת תשובה לשאילתה של פונה (אזרח או תאגיד) לא יתבצע חיבור ישיר בין הפונה (באמצעות האינטרנט ,או קשר אחר) לבין בסיס המידע.

הקישור במיזם זה, בין הפונים לבין משרדי הממשלה יתבסס על "**בידול**" הנעשה ע"י חומרה, או, חומרה הנסמכת על ידי תוכנה.

להלן שיטות הקישור המאובטחות למיזם זה:

1. שיטת ה"**מגש**".
2. שיטת ה"העברה הפיזית" של מצע-מידע בין שתי המערכות, כאשר התשובה לפונה אינה מכילה מידע "**חסוי**" או "**חסוי-ביותר**".

הגנת הפרטיות: במקרה והמידע המבוקש הוא מידע אישי-רגיש אודות הפונה, מידע המוגן בחוק הגנת-הפרטיות, **התשמ"א - 1981**, יש לוודא כי הפונה הוא אכן האיש הרשאי לקבל את המידע "החסוי". יש להשתמש באמצעי זיהוי מתקדמים כגון: "**כרטיס חכם**" (המלווה בסיסמה אישית **P.I.N**), או ע"י זיהוי ביומטרי המאושר על ידי "היחידה".

מידע בסיווג "**חסוי-ביותר**" לא יועבר בשום אמצעי שפורט לעיל, ללא יוצא מן הכלל, באמצעות רשת האינטרנט

אבטחת מערכי התקשורת בפרוייקט תהיל"ה וברשת התקשורת הממשלתית

א. אבטחת מערכי התקשורת הנ"ל תיעשה על פי נהלי המסגרת של "**המועצה**".

ב. האחריות והסמכות להתקין כלים ושיטות לאבטחתם של מערכים אלה ו"המידע הרגיש" המטופל בהם מוטלת על מנהל אגף הביטחון במשרד האוצר.

ג. מחובתו של כל "**ממונה**" במשרדי הממשלה ובמוסדות הקשורים עם מערכי המידע הנ"ל,

ליישם את נהלי "המועצה", **ללא תלות בפעילות הנעשית על ידי משרד האוצר**.

חיסיון המידע אודות כלים ושיטות לאבטחת התקשורת באינטרנט

הנהלים והשיטות המשמשים את המשרד לשמירת "המידע הרגיש" ומערכי המידע מסווגים בסיווג "**חסוי**" (חלקם אף "**חסוי-ביותר**"). לפיכך יש לפעול בקפידה על פי הסייגים הבאים:

א. אין להעביר את נהלי "**המועצה**", בכל דרך שהיא (בע"פ, ברשומות או במצעי - מידע למיניהם) לידי גורמים שאינם עובדי המשרד או גורמים חיצוניים, בטרם ניתן לכך היתר מ"היחידה".

ב. אסור לחלוטין לפרסם את הנהלים לאבטחת "**מידע רגיש**" ברשת האינטרנט **!**

ג. אין לצטט את הנוהל הזה, נהלים אחרים של "**המועצה**", או קטעים מהם, בתוך נהלים ממשלתיים אחרים. בכל מקרה שיתעורר צורך שכזה ניתן ליצור רק הפנייה לנוהלי "**המועצה**".

התכונות הנדרשות ממערך "קיר-אש" (FIRE WALL):

א. הגנה על הרשת ועל שירותים

1. יצירת סינון אבטחתי איכותי - שיאפשר תעבורת מידע או נתונים, רק לאלה אשר הוגדרו על ידי מדיניות אבטחת מידע של המשרד.

2. מצב ברירת המחדל של "**קיר-האש**" יהיה **מניעה של כל הקישורים** מאת ואל הרשת הפנימית! רק קישורים ספציפיים אשר יאושרו על ידי "**הממונה**", יורשו.

3. יש להפעיל במערך "קיר-האש" מנגנוני מניעה וחסימה, כמפורט להלן, אשר יחסמו את הרשת הפנימית בפני מתקפות וחדירות.

הרשימה שלהלן נכונה ליום פרסום הנוהל והיא תתעדכן מעת לעת.

- **Ping of death (fat ping attack)**
- **SYN Flood attack**
- **IP spoofing**
- **Malformed packet attack - (both TCP & UDP)**
- **Forged source address packets**
- **ACK storms**
- **Network probes**
- **Packet fragmentation attacks**
- **Session hijacking**
- **Log overflow attacks**
- **SNMP attacks**
- **Log manipulation**
- **Source routed packets**
- **CMP broadcast flooding**
- **Land attack**
- **DNS cache corruption**
- **ARP attacks**
- **FTP bounce or port call attack**
- **ICMP protocol tunneling**
- **Ghost routing attacks**
- **VPN key generation attacks**
- **Sequence number prediction**
- **Authentication race attacks**
- **Buffer overflows**

ב. במערכת ינוטרלו כל המנגנונים המאפשרים **DYNAMIC ROUTING** דרך "**קיר-האש**".

ג. המערכת תפעיל מנגנוני פיקוח, בחינה, וסינון **בכל** הרמות הבאות:

1. סינון מנות המידע **Packets Filtering**
2. **CIRCUIT** (בדיקת **PORTS**).
3. **PROXIES** - ניתן להגדיר כל סוג **PROXY** כולל - **USER DEFINED PROXY**

ד. המערכת תיצור הגנה על שירותים ויישומים, כגון: **FINGER, TELNET, RLOGIN, HTTP, FTP, PING.**

ה. המערכת תקיים תמיכה בהגנה על שירותי **SMTP:** הסתרת כתובות, הגבלת העברת קבצים כצרופות, הגבלת גודל הדואר.

ו. מערך "קיר-האש" יתמוך בהגנה על שירותים המבוססים על פרוטוקול **TCP/IP** (בעיקר) וכאופציה גם **UDP** ו- **RPC**

ז. המערכת תאפשר תמיכה ו/או ממשקים לתוכנה ייעודית המטפלים בפתרון הגנה בפני וירוסים לצורך בדיקת קיום וירוסים בצרופות לדואר אלקטרוני ובקבצים המועברים לרשת הפנימית.

ח. **המערכת תאפשר** תמיכה ו/או ממשקים לתוכנה ייעודית בפתרון לסינון ומניעת התקפות **Active-X** ו- **Java Applets**.

ט. המערכת תאפשר ניהול "אזור מפורז".

י. **המערכת תאפשר** תמיכה ו/או ממשקים לתוכנה ייעודית המטפלת בסינון כתובות של אתרי אינטרנט (**URL**) במגמה להגביל גישה של משתמשים מתוך המשרד לאתרי אינטרנט לא רצויים.

י"א. מערך "**קיר-האש**" יכיל בתוכו גם **סינון תכנים** (**CONTENT FILTERING**) כדי למנוע את
העמסת הרשת בשוטטות סרק, ולצרכים שאינם מותרים על ידי הנהלת המשרד. מנגנון זה יהיה חלק מ"**קיר-האש**" והוא יאפשר חסימת תכנים לפי קטגוריות שונות כגון: תכנים חסויים או סודיים, אלימות, מין, סמים וכיוצא בכך.

י"ב. שירותי תרגום כתובות.

1. "**קיר-האש**" יאפשר לתרגום כתובות ומספרי **PORTS** באופן שגם הכתובת וגם מספר ה-**PORTS** יוסתרו.
2. "קיר האש" יאפשר לתרגם כתובות בשיטת **M.A.T** דהיינו -**MULTILE ADDRESS TRANSLATION**, כך שניתן יהיה להתקין ולהסתיר מספר שרתים מאותו סוג, כגון: **FTP, WWW** ו- **SMTP**

3. תתאפשר הסתרת שם ה- **Sub domain** או **Host,** באופן ששם האתר או המחשב אשר יוצג כלפי רשתות ציבוריות לא יהא זהה לשם האמיתי של האתר או המחשב.

הגנה על מרכיבי מערך "קיר-האש"

א. נדרשת יצירת חסינות והגנה לוגית רבה על רכיבי "**קיר-האש**" כולל תשתית תפעולית.

ב. "**קיר-האש**" יפעל על **מערכת הפעלה קשיחה** ובלתי ניתנת לגישה כל שהיא, גם לא על ידי נהלי המערכת (מערכת ההפעלה ו"**קיר-האש**" יהיו משולבים לתוכנה אחת).

ג. "**קיר-האש**" יהיה בעל **KERNEL** דואלי - אחד לצורכי תפעול שוטף ואחד לצורכי מינהלה וקביעת תצורה.

ניהול מערך "קיר-האש".

א. ניהול הקונפיגורציה יתאפשר מרחוק מתוך הרשת הפנימית ויבוסס על זיהוי משתמש ואימות הזיהוי באופן שתמנע "התחפשות" או אפשרות להכחשה.

ב. נדרש ממשק גרפי לניהול "**קיר-האש**".

ג. נדרשת אפשרות להגדרת הרשאות מבוססות על חוקים (**Rule Base**).

ד. נדרשת אפשרות לניהול הרשאות לפי קבוצות.

ה. מומלצת אפשרות להגדרה וניהול מדיניות אבטחת מידע אחידה למספר "**קירות-אש**", למקרה שתידרש התקנה של יותר מ-"**קיר-אש**" אחד.

ו. יתאפשר ביזור סמכויות ניהול תוך מתן הרשאות למנהלים לפי רמות ניהול שונות, לדוגמא: אפשרות למידור פעילות בין פונקציה ניהולית אשר תורשה להגדיר משתמשים לבין פונקציה אשר תורשה להגדיר **Rules.**

ז. נדרשת אפשרות להגדרת **ACL`S** שונים ויצירת צירופים (כגון: איסור על העברת **FTP** בימים מסוימים בשבוע, למעט מכתובות **Email** מסוימות, משתמשים וקבוצות, סוג השירות-**WWW, Email, FTP,Telnet** , מספר מקסימלי של sessions מקבילים ורמה נדרשת של הצפנה).

ניהול משתמשים ומנגנוני זיהוי.

א.
1. ממשק למוצר תוכנה ייעודי ו/או מתן אפשרות לניהול משתמשים כולל מנגנון זיהוי ואימות הזיהוי (**Authentication**) למשתמשים המתקשרים מרחוק, באמצעות קווי - חיוג וקווי תקשורת קבועים.

2. לצורכי ביצוע שירותי **Telnet** ו- **FTP** מחוץ למשרד אל תוך המשרד, תתבצע פניה לשירות (**Authentication**) (סיסמאות חד-פעמיות) בתוך "**קיר-האש**".

ב. תתאפשר תמיכה וקביעה של צורות זיהוי ואימות זיהוי משתמשים מגוונות - תמיכה במנגנוני זיהוי שונים: סיסמת מערכת ההפעלה, סיסמה פנימית של "קיר-האש" ומנגנוני זיהוי מקובלים בשוק (לדוגמא: כרטיסים חכמים).

ג. תתאפשר הגבלת גישה של משתמשים לפי שעות עבודה שבועיות / ימים / תאריכים.

ד. יותקן מנגנון ניהול סיסמאות "**קיר-האש**" (סיסמאות מנהלים ומשתמשים) קביעת אורך הסיסמה, דרישה להחלפת סיסמה וכיוצא בכך.

הצפנה

א. מערכת "**קיר-האש**" תאפשר תמיכה ברשת וירטואלית פרטית **V.P.N**. וכן תמיכה ב- **DVPN** (**DYNAMIC VPN**) לצורך תמיכה במחשבים ניידים המתקשרים ל - **8235**.

ב. המערכת תאפשר הצפנת מידע על הרשת הפנימית, תוך שימוש באלגוריתם שייקבע על ידי גורמים ממלכתיים.

ג. נדרשת הצפנת תעבורת המידע על הרשת בין רכיבי "**קיר-האש**". בכל מקרה תיעשה ההצפנה על פי נוהלי "**המועצה**" ואישור מראש ובכתב של מנהל "היחידה".

בקרה

א. מנהל מערכות המידע ייצור נתיב ביקורת **(Audit Trail)** כדי לעקוב אחר ניסיונות פריצה למנגנון האבטחה של "**קיר-האש**" וניסיונות חדירה לרשת.

ב. יש ליזום רמה משופרת של ביקורת אשר תתאפשר כאשר תזוהה פעילות חשודה.

ג. יש לקיים ב"**קיר-האש**" מכניזם לניהול **LOG** אשר יאפשר קריאה והבנת ה - **LOG**

ד. "**קיר-האש**" ינהל **LOG** על התקשורת וניתוק קשר של משתמשים המתקשרים מרחוק.

ה. מערך "**קיר-האש**" [מובנה בתוכו או לצידו] ייתן התרעות ל-**E-mail** בזמן אמת על ניסיונות חדירה.

הפרת נוהל זה משמעה - עבירת משמעת חמורה אשר עלולה להוביל, בין היתר, לביטול היתר הגישה למקורות מידע ומערכי מידע "רגישים" - עם כל הנובע מכך.

"**היחידה**" תערוך בקרות וביקורות אודות אבטחת רשת האינטרנט במשרדי הממשלה ומוסדותיה, כולל עריכת בדיקות מרחוק לבדיקת החוסן של מערכי ההגנה.

קיומה של אבטחת מידע לקויה באינטרנט עשויה להוות עילה לתובענה משמעתית, ללא חובת הוכחה של רשלנות !

בכל מחשבי המשרד תותקן תוכנת האנטי וירוס שתתעדכן מעת לעת.

קיימת העדפה שלא להזדהות בכל פורום ציבורי ע"ג האינטרנט כעובד/ת משרד ממשלתי, למעט במקרים בהם יש הכרך במסגרת התפקיד.

אין לבצע התקנה פרטית של אביזרים או תוכנת גלישה כלשהי ואין לבצע התקשרות על חשבון גורם חוץ, כמו אוניברסיטה, דרך מחשבי המשרד.

אין לבצע התקשרות דרך גופי ביניים (כגון בזק) ללא הרשאה מראש ובכתב מקב"ט ארצי ומראש אגף אבטחת מידע.

משתמשי אינטרנט במשרד ידווחו לראש אגף אבטחת מידע מדי חודש ינואר על <u>המיקום המדויק</u> של הציוד המשמש למטרה זו. משתמש חדש ידווח מיידית עם ההתחברות.

יש להתקין ברשת היחידה (משרד או ארגון) תוכנה לבקרת תוכן כדי למנוע גישה לאתרים בלתי ראויים. מהלך זה מוריד עומס מקווי התקשורת, מגדיל את יעילות השימוש בקו וחוסך בזמן האבוד של העובדים.

פעילותו של מחשב המשמש להתקשרות לאינטרנט <u>תופסק</u> בגמר העבודה עמו.

מקורות

נהלי מסגרת – אבטחת מידע רגיש ומערכות מידע. משרד ראש הממשלה, אגף בכיר לביקורת המדינה וביקורת פנימית, מאי 2000.

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

תוכנות פוגעניות במחשב אישי וברשת מקומית

נוהל מס׳ 35

מטרות הנוהל

ניטרול הסיכון של פגיעות ״וירוסים״ ותוכנות מזיקות אחרות. להגן על כלילות (integrity) של התוכנה והמידע.

אחראי לביצוע הנוהל

אחריות הביצוע מוטלת על מנהל יחידת המחשב, על מנהל הרשת ועל משתמשי המחשבים האישיים, כל אחד בתחומו כפי שיפורט בהמשך.

אחריות הבקרה מוטלת על ממונה אבטחת מידע ועל מנהל יחידת מערכות המידע.

הגדרות

תוכנה מפגיעת: תוכנה שנכתבה במגמה לפגוע במאגרי מידע או בתפעול מערכות. המוכרת מביניהן היא וירוס מחשב.

וירוס מחשב: תוכנית מחשב היודעת, ללא התערבות מכוונת, לשכפל את עצמה למאגרי/קבצי מידע ובהמשך לפגוע בהם בדרכים שונות: מחיקת מידע, האטת פעילות, מילוי זיכרון, שינוי מידע וכדומה.

פצצה לוגית: תוכנית או קוד שבנוי בתוכנית כלשהי, שאינה עושה דבר עד שמתקיים תנאי ל״התפוצצות״. בזמן התרחשות התנאי (תאריך מסוים, מספר הפעלות וכדומה), ה״פצצה״ מופעלת והתוצאה אינה צפויה ואינה רצויה. מאמץ השחזור יכול לנוע מ״לא נוח״ עד לבלתי אפשרי.

סוס טרויאני: תוכנה שאמורה לבצע פעולה כלשהי אולם, היא מכילה חלק לא מפורסם שהנו הרסני. וירוסים ופצצות לוגיות מתחבאים בתוך סוסים טרויאניים. הסוס הטרויאני יכול לעבוד בצורה יפה זמן רב עד שמנגנון ההפעלה של הוירוס או הפצצה הלוגית מתחיל לפעול.

תולעת: תוכנית שסורקת את המערכת או הרשת ומחפשת מקום פנוי לפעול בו. תולעת נוטה לקשור את כל המשאבים במערכת או ברשת במטרה לשתקה.

אנטי-וירוס למחשבים אישיים – תוכנת מחשב היודעת לאתר וירוסים במחשבים אישיים, הן בזיכרון והן בקבצים שבדיסק הקשיח, מתריעה עליהם ומחסנת נגדם. התוכנה מורכבת משני חלקים:
TSR שמזהה את הוירוס, ומונע את פעילותו
תוכנת ניקוי, סריקת קבצים.

גוף הנוהל

דרושים אמצעי זהירות כדי למנוע ולגלות כניסה של תוכנה זדונית. תוכנה ומתקנים לעיבוד מידע רגישים לקיומן של תוכנות זדוניות, כגון וירוסים, תולעי רשת, סוסים טרואינים ופצצות לוגיות. המשתמשים ייודעו באשר לסכנה הגלומה בתוכנות לא מורשות או זדוניות, והמנהלים ינהיגו בקרות מיוחדות, כדי לגלותן או כדי למנוע כניסתן. במיוחד חיוני לנקוט אמצעי זהירות לגילוי ומניעה של ווירוסי המחשב במחשבים אישיים.
יש לערוך סקרים רגילים על תכולת התוכנות והנתונים שבמערכות התומכות בתהליכים קריטיים של המשרד. כל נוכחות של קובץ לא מאושר או תיקונים לא מורשים תיחקר רשמית.
יש לבדוק כל קובץ נספח שנשלח בדואר אלקטרוני וכל הורדה מהרשת (download) לגילוי תוכנות זדוניות לפני השימוש. בדיקה זאת יכולה להיערך במקומות שונים, כגון בשרתי הדואר האלקטרוני, במחשבי ההוצאה לאור השולחנית או בכניסה לרשת של המשרד.

יש להכין תוכנית התאוששות מהתקפות וירוסים, לרבות כל הגיבויים הדרושים לנתונים ולתוכנות וכל סידורי ההתאוששות.
מומלץ לערוך נהלים לאימות כל המידע המתייחס לתוכנה זדונית, ולהבטחה שהודעות האזהרה מדויקות ומכילות מידע הולם. מנהלים יבטיחו שימוש במקורות ראויים כגון עיתונים בעלי שם, אתרים אמינים באינטרנט או ספקים אמינים של תוכנות אנטי-וירוס, כדי להבחין בין מעשי קונדס לבין וירוסים אמיתיים. העובדים ייודעו באשר לבעיית מעשי הקונדס ובאשר לאופן הטיפול בהם.
בקרות אלה חשובות במיוחד עבור שרתי קבצים ודואר של רשתות התומכים במספר גדול של תחנות עבודה.

א. פעילויות משתמשי המחשב:

1) כדי למנוע המצאות וירוסים במחשבים, חל **איסור מוחלט** להכניס לכוונני הדיסקטים תוכנה לא מורשית, תוכנה פרטית ותוכנה שלא ידוע מקורה.
2) כמו כן, חל **איסור מוחלט** להתקין בדיסק השרת ו/או במחשב האישי תוכנה שנקלטה באמצעי תקשורת חיצוני מתוך מחשב אחר או מתוך מאגר תוכנה חיצוני.
3) כל קובץ ממקור חיצוני, לרבות קבצים ודיסקים, יש לבדוק בנפרד בתחנת "stand alone" לנושא זה, בה לא קיים מידע רגיש או בעמדת אינטרנט.
4) כל מקרה חריג ידווח מיידית לממונה אבטחת מידע.

ב. פעילות מנהל חדר המחשב/מנהל הרשת

1) גילוי, ניקוי והתראה על המצאות וירוסים במחשבי המשרד.
2) דיווח לממונה על אבטחת המידע על גילוי וירוסים.
3) התקנה של תוכנת אנטי-וירוס בגרסה העדכנית ביותר.
4) בכל רשת תקשורת מקומית, תותקן תוכנת אנטי וירוס במחשב השרת. הכוונה לתוכנה שוכנת זיכרון, מגרסא שנועדה לרשת תקשורת מקומית.
5) התעדכנות שוטפת באשר לקיומן של גרסאות עדכניות יותר של תוכנת אנטי-וירוס וטיפול בהתקנתן, במעורבותו של מנהל היחידה למערכות מידע.
6) ניהול יומן עדכון גרסאות שבאמצעותו ניתן יהיה לעקוב אחר העדכון, תאריכי ההתקנות והמחשבים בהם הותקנו הגרסאות.
7) הדרכה ועזרה לעובדים בגילוי וירוסים והפעלת תוכנת אנטי-וירוס במחשביהם.
8) בדיקה יומית של ה-LOG הנוגעת לפעילות תוכנת האנטי-וירוס.

ג. פעילות ממונה אבטחת מידע

1) בקרה ומעקב אחר פעילות מנהל חדר המחשב/מנהל הרשת והמשתמשים במשרד, בהיבטי הנחיות אבטחת המידע.
2) ביצוע בדיקות פתע וביקורות לוידוא המצאות תוכנת אנטי-וירוס עדכניות וכן וידוא תפעול עפ"י נהלי העבודה עם תוכנת אנטי-וירוס.
3) תיעוד האירועים והפעולות שננקטו.

ד. תהליך טיפול בוירוסים ברשת ובמחשבי "stand alone"

האירוע	אופן הטיפול	אחריות הביצוע
פעולות מנע יזומות בתדירות של אחת ליום (בהדלקת מחשב או בפעילות יזומה).	ביצוע סריקה יזומה, לאיתור וירוסים חבויים שהסתננו למערכות, באמצעות תוכנת הסריקה, גילוי וניקוי של האנטי-וירוס.	מנהל הרשת
	ניסיון לאתר את מקור הופעת הוירוס ברשת ומתן פתרונות למניעת הידבקות חוזרת ממקור זה או ממקורות אחרים.	מנהל הרשת
גילוי וירוס ברשת/תחנת Stand alone	הפעלה מיידית של תוכנת אנטי-וירוס לסריקה, גילוי וניקוי הוירוסים בזיכרון ובקבצי השרתים ברשת. התקנת כלי ניקוי מתאים לווירוס.	מנהל הרשת
	סריקה מיידית של כל תחנות העבודה ברשת.	מנהל הרשת בסיוע גורמי התקשורת
	הפסקת עבודת הרשת עד לוידוא שהוירוס נוקה. דיווח מיידי לממונה אבטחת המידע ומנהל היחידה למערכות מידע.	מנהל הרשת
תוכנת האנטי-וירוס מזהה את הוירוס, אך לא מצליחה לנטרל אותו	הפסקה מיידית של העבודה ברשת	מנהל הרשת בסיוע אנשי התוכנה של החברה הספקית
	נקיטת פעולה מיידית לניקוי הוירוס והחזרת הרשת לתפקוד תקין.	מנהל הרשת בסיוע אנשי התוכנה של החברה הספקית
נזקים עקב פעילות הוירוס	שחזור מיידי של הקבצים והנתונים שנפגעו מגיבוי הרשת	מנהל הרשת

ה. הטיפול באנטי-וירוס

1) תהליך הפצת עדכוני גרסת האנטי-וירוס:

א. מנהל חדר המחשב יודיע מדי פעם על הפצת גרסה עדכנית של תוכנת אנטי-וירוס.

ב. ההתקנה תתואם בכתב, תוך פירוט פרטי החברה (שם הרפרנט, כתובת החברה, טלפון).

ג. תהליך התקנת הגרסה יהיה מבוקר ויתבצע ע"י מנהל הרשת.

2) תהליך איתור תוכנת אנטי-וירוס

אחת לשנתיים יבוצע תהליך הבחינה המקצועית, לבחירת תוכנת אנטי-וירוס, על פי הפירוט הבא:

1. מנהלי הרשת יוציאו פניה לכל חברות התוכנה המספקות תוכנות אנטי-וירוס לקבלת עותק וספרות מתאימה של תוכנה זו.
2. מנהלי הרשת יבדקו וישוו את התוכנות בין היתר מהבחינות הבאות:

א) מספר הוירוסים שהתוכנה יודעת לטפל בהם.

ב) התאמה למחשבי המשרד

ג) התאמה לתוכנות הפועלות במשרד

ד) נוחות ההתקנה

ה) רמת הידידותיות בהפעלתה ובהודעותיה למפעיל המחשב

ו) יכולת החברה המספקת לעדכן את גרסאות התוכנה באופן מהיר

ז) יכולת החברה המספקת לספק סיוע טכני מהיר ומיידי במקרה של תקלות ונזקים שתוכנת האנטי-וירוס לא הצליחה לטפל בהם

ח) מחיר התוכנה וחוזה השירות עם החברה המספקת

3. מנהל הרשת, במעורבות ובסיוע הממונה על הרכש, יאתר את התוכנה האופטימלית ויבצע רכישתה כנדרש.

3) פעילות התקנה של תוכנת אנטי-וירוס:

מנהל הרשת יבצע בדיקה של שרתי הרשתות וכל מחשב אישי קיים במשרד כלהלן:

א. סריקת כל הקבצים הקיימים על הדיסק הקשיח של כל מחשב/שרת וסילוק וירוסים קיימים ותוכנות קודמות המטפלות בוירוסים.

ב. התקנת תוכנת האנטי-וירוס שנבחרה ע"י המשרד בכל שרת רשת ו/או מחשב אישי.

ג. רישום פרטי המחשב שנבדק ביומן מעקב ייעודי, שם האחראי על המחשב האישי, תאריך הבדיקה ומספר הוירוסים שסולקו.

אירועים המצביעים על קיומו של וירוס

1. הודעות בלתי צפויות או בלתי מובנות, או שלא לעניין התוכנה המתבצעת
2. "תקיעת" מחשב
3. זמן ביצוע תוכנית ארוך מהרגיל או נראה כ"לולאה"
4. system boot (המחשב מבצע reset מעצמו) בלתי צפוי
5. האטה כללית בפעולות המחשב
6. היעלמותם של קבצים או מחיצות שלמות
7. הוספה בלתי מוסברת של קבצים נסתרים או לא מוסתרים שאינם מוכרים
8. קבלת דואר מסיבי מאותם משתמשים

מקורות

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

נוהלי אבטחת המידע בעיריית ירושלים, פברואר 2001.

התקנה ואבטחה של תוכנות השתלטות מרחוק

נוהל מס׳ 36

מטרות הנוהל

אפיון הפתרון לאבטחת המידע בתהליכים של גישה מרחוק, ופרוט של אמצעי אבטחה אשר נועדו לאפשר את יישומו של נוהל זה. הגדרת אמצעי האבטחה הנוגעים לתוכנות השתלטות מרחוק.

הגדרות

מודם – רכיב תקשורת המאפשר תקשורת בין מחשב לציוד היקפי מרחוק (מסוף, מדפסת או מחשב אחר) דרך רשת קווי טלפון.

אחראי לביצוע הנוהל

אחריות ניהולית לנוהל זה חלה על מנהל אגף לשירותי מידע ומחשוב.

מנהל סיוע טכני ותקשורת רוחבית יוודא ביצוע תקין של הנחיות נוהל זה ויבצע בקרה שוטפת בנושא.

ממונה אבטחת מידע יסייע בקיום בקרה, ינחה ויטמיע ההנחיות.

משתמשי המחשב אשר בעמדותיהם מותקנת תוכנת התקשרות מרחוק או אשר להם צורך התקשרות זו, יפעלו על פי הנחיות ונהל זה.

גוף הנוהל

במסגרת יישום מדיניות אבטחת המידע, קיימת חשיבות רבה ליישום האבטחה בתהליכים של גישה מרחוק , בהיותה ״שער כניסה״ למידע המצוי במערך המחשוב המשרדי.

אבטחת מודמים

ככלל, לא יקושרו מודמים לחיוג למחשבים המחוברים לרשת המשרד. כל קישוריות תבוצע באמצעות מחשב אשר אינו מחובר לרשת המשרד ובכפוף להנחיות אבטחת מידע. במידה והועלה צורך בקישוריות חריגה, יינקטו הפעולות המפורטות להלן.

כל בקשה להתקנת מודם תוגש עפ״י הנוהל הקיים במשרד ועפ״י הטופס הסטנדרטי לאישור של מנהל אבטחת המידע וחתימה על טופס הצהרת סודיות משני הצדדים.

בבקשה יפרט המבקש את הפרטים הבאים:

- השימוש הדרוש למודם
- סיווג הנתונים שיעברו באמצעות הקישור
- מספר הטלפון לו דרושה ההתקשרות
- האם המודם ישמש כ-host או כמקשר ליעד מרוחק
- היישום בתחנת העבודה אשר מולה דרושה ההתקשרות. האם מדובר ביישום מקומי או ביישום ברשת
- גורם בצד המתחבר האחראי לתפעול/אבטחת מערכות המידע

אם אישור ההתקנה על ידי האגף, יבצע מנהל ענף תשתיות פעילות הכנה הנוגעת להתקנה. במקביל, יבקר מנהל אבטחת מידע את הגורם שמולו מתחבר המשרד לצורך בדיקה ואימות הפרטים שצוינו בבקשה, וכן על מנת לעמוד על סדרי האבטחה הננקטים באתר המרוחק. (אחראי אבטחת המידע יעביר דרישה מסודרת כחלק מתנאי להתקנת המודם).

ככלל, יותקנו מודמים בעלי סידורי ואמצעי אבטחה משני טיפוסים:

- מודם בעל אמצעי בקרת גישה איכותיים
- מודם בעל אמצעי בקרת גישה built in (סידורי callback)

המודמים שיותקנו, ישמשו לשיחות יוצאות בלבד. מודמים אשר ישמשו כ-hosts יאופיינו על פי צרכי הפרוייקט והמטרות לשמן נועדו כאשר במקביל יאופיינו עבורם אמצעי אבטחה ייעודיים.

בקו טלפון שבו יותקן מודם המוגדר להתקשרות כלפי חוץ יוגדרו במרכזיה הגדרות המונעות מן הקו לקבל/לענות לשיחות נכנסות.

בכל בקשה חריגה להתקנת מודם המקושר לרשת המשרד או למחשב בו קיים מידע חסוי, יותקן מודם בעל אמצעי אבטחה איכותיים.

למודמים בעלי אמצעי אבטחה built in, יותקנו במחשבים עצמאיים שרגישות המידע בהם היא עד פנימי (מידע שאינו רגיש).
במודם מסוג callback תוגדר רשימת הטלפונים המופיעה בטופס הבקשה.

מודם איכותי שיותקן יהיה בעל רכיבי אבטחה מסוג: smart cards, מערכת אבטחה ייעודית. אחת לרבעון או אחת לחצי שנה תבוצע ביקורת לגבי נחיצות הקישורים החיצוניים וכן בדיקת אמצעי האבטחה המקושרים לכל קו וקו.

חשוב לציין כי נוהל זה לאחר אישורו יופץ בכל המשרד. לאחר קבלת הנוהל יתבקשו היחידות להסיר את כל המודמים שאינם עומדים בקריטריונים האבטחתיים שנקבעו וכן כחלק מתכנית העבודה השנתית יבוצע בכל המשרד בדיקה ע"י חייגן טלפון מלחמתי.

תוכנת השתלטות מרחוק

התקנת תוכנת השתלטות מרחוק מורשית לביצוע רק בידיעתו ובאישורו מראש של הממונה על אבטחת מידע ותתבצע עפ"י המפורט בנוהל זה.

התקנת תוכנת השתלטות תבוצע רק ע"י צוות היחידה למערכות מידע.

התקשרות מרחוק של עובדי קבלן או עובדי חברת חוץ בסיוע מודם חיוג ו/או בסיוע תוכנת השתלטות למחשב אשר נאגר בו מידע פנימי של המשרד או מחשב מחובר פיזית לרשת במשרד לצורך עבודות תחזוקה או כל צורך אחר תתבצע **אך ורק** בפיקוח מלא של עובד המשרד. העובד יאשר התקשרות (יפעיל אותה), ישגיח במהלכה ויוודא ניתוק מוחלט של הגורם החיצוני בתום ההתקשרות.

מקרים חריגים יטופלו לגופם ולגביהם יינתן אישור מראש ובכתב של ממונה אבטחת מידע.

כל משתמש ישא באחריות אישית לגבי עמדת עבודתו, ינהג בכפוף להנחיות נוהל זה בכל הנוגע להתקשרות מרחוק וידווח לממונה אבטחת מידע על תוכנות התקשרות אשר הותקנו שלא בהתאם לאישורים הנדרשים.

לצורך השתלטות על המחשב המארח **<u>חייבים</u>** להפעיל את אפשרויות האבטחה הקיימות בתוכנת השתלטות מרחוק:

1. שם משתמש
2. סיסמא בת 6 תווים לפחות, עפ"י ההנחיות שיוגדרו
3. הפעלת אפשרות ניתוק לאחר חוסר פעילות של פרק זמן שיקבע ע"י הממונה אבטחת מידע
4. הפעלת יומן LOG של פעילות המתבצעת באמצעות תוכנת ההשתלטות.

במידת הצורך ניתן להשתמש גם באפשרויות "call back" בהפעלת תכונות ההצפנה.

אין להשאיר ציוד מחשבים דולק/פועל לאחר שעות העבודה אלא ע"פ אישור ממונה אבטחת המידע.

על המשתמשים להודיע לצוות תשתיות או לממונה אבטחת המידע על תופעות חריגות או בלתי מובנות אשר התרחשו תוך כדי ובסמוך לפעילות מורשית של התקנת תוכנת השתלטות מרחוק.

מקורות

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

נוהלי אבטחת המידע בעיריית ירושלים, פברואר 2001.

נוהלי עבודה – אגף לשירותי מידע ומחשוב, משרד הבריאות, פברואר 2000.

הפעלה ושימוש במודמים

נוהל מס׳ 37

מטרות הנוהל

להגדיר סייגים והרשאות בתחום זה.

אחראי לביצוע הנוהל

באחריות המשתמשים לוודא יישומן של הנחיות נוהל זה.

ממונה אבטחת מידע ומנהל יחידת המחשב יבצעו בקרה ואכיפה בקרב המשתמשים.

גוף הנוהל

חל איסור על הפעלת מודמים חיצוניים או כרטיסי מודם (או מודם/פקס) במחשבי המשרד, אלא באישור ממונה אבטחת מידע.

באחריות כל משתמש אשר ברשותו ציוד כנ״ל (רכוש המשרד או מימון ע״י כל גוף אחר) לדווח מיידית לממונה אבטחת מידע, על מנת לקבל אישור/מענה מקצועי לגבי השימוש.

ההיתר הקיים להפעלת ציוד לצורך התקשרות לאינטרנט או רשת אחרת מאותו סוג מתיר גם שימוש בציוד האמור וכל זאת בתנאי שבציוד המשמש להתקשרות איננו מחובר לרשת המשרד ועומד בפני עצמו.

במקרה של צורך טכני (לצורכי עבודה לבד), ואך רק במקרה זה,יש לקבל אישור מראש ובכתב מממונה אבטחת מידע להתקנת ציוד מסוג זה או לקבל חלופה אחרת לאותה מטרה.

עם סיום הצורך הטכני בפתרון הנ״ל, יוסר ציוד התקשורת ויסולק מן המקום.

לא תופעל תוכנת התקשרות/השתלטות מרחוק בסיוע מודם/חיוג ללא אישור מראש ובכתב מהממונה על אבטחת המידע.

לאחר אישור כאמור, תבוצע ההתקשרות רק כאשר בקצה המחובר למשרד נמצאים עובדי המשרד. ההתקשרות תהיה בזמנים לא קבועים ולמשך זמן קצר ככל האפשר. ההתקשרות תופעל רק כאשר הצד הרחוק יפעיל את תוכנת ההשתלטות באמצעות סיסמא שתיוחד לו ולשם כך יש להפעיל את תוכנות האבטחה של תוכנת ההתקשרות/השתלטות מרחוק (כגון PCANYWHERE), ראה פירוט בנוהל מס׳ **32** – ״התקנה ואבטחה של תוכנות השתלטות מרחוק״.

אין לחבר לציוד מחשב כלשהו, ציוד תקשורת מכל סוג, גם לצורך ניסוי, ללא תאום עם ממונה אבטחת מידע.

במידת האפשר תבוצע ההתקשרות דרך מרכזיה ולא בקו ישיר.

מקורות

קובץ נוהלי אבטחת מידע במערכות ממוחשבות של משרד האוצר, ינואר 2002.

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

שימוש בפקס להעברת "מידע רגיש" או מסווג

נוהל מס' 38

מבוא

בשל טעויות אנוש או בעיות טכניות מתבצע לעיתים חיוג שגוי, למרות שעל גבי צגים (במכשירים בהם יש צג) מופיע לכאורה מספר נכון. כך מועבר מידע מסווג לגורם לא ידוע.

מטרות הנוהל

למנוע העברה בשוגג של מידע מסווג לנמען לא ידוע.

אחראי לביצוע הנוהל

באחריות המשתמשים לוודא יישומן של הנחיות נוהל זה.
באחריות ממונה אבטחת מידע להדריך, להטמיע ולאכוף הנחיות נוהל זה בקרב עובדי המשרד וגורמי החוץ העוסקים במידע.
באחריות המנהלים הישירים לבקר יישום ההנחיות על ידי עובדיהם.

גוף הנוהל

חל איסור להעביר מידע המוגדר כ "מידע רגיש" על פי חוק הגנת הפרטיות בשיגור בפקס. ("חסוי" או "חסוי ביותר" לפי נוהל מס' **2** – "מיפוי ויסווג של מידע רגיש ומערכי מידע").

במקרים מיוחדים, אפשר להעביר באישור הממונה, מידע בעל רגישות חוקית או הכפוף לכללי אתיקה מקצועית ומעוגן בנהלי המשרד, רק בשיטה הבאה:

א. תבוצע התקשרות טלפונית עם הנמען, אשר ימתין <u>ליד</u> מכשיר הפקס. המקבל, על מנת לוודא שיגור ליעד הנכון.
ב. ישוגר בפקס דף מוביל או יותר (לפי הצורך) עד אשר הנמען מאשר כי הוא מקבל פקס את הדפים המובילים.
ג. רק לאחר מכן ניתן לשלוח מידע רגיש או מסווג בסיווג נמוך כהמשך <u>לאותו שיגור</u>.

למעט מקרים חריגים ובאישור ממונה בלבד, יש למחוק כל פרט מזהה במידע המועבר בפקס.

מידע רגיש רצוי כי ישלח משלוחה במרכזיה ואל שלוחה במרכזיה (אפשרי גם חיוג ישיר פנימה לשלוחה). זאת בניסיון להימנע ככל האפשר מהאזנה ישירה לקו מוגדר או ישיר.

מקורות

אבטחת מידע – קובץ נהלים של משרד העבודה והרווחה, אפריל 1996.

מילון מונחים

אבטחה לוגית הפעלת מנגנוני תוכנה ייעודיים לצורך אבטחה. מימוש יכולת אבטחה הקיימת בתוכנה.

אבטחת מידע כלל הפעולות והאמצעים הננקטים והמיושמים במשרדי הממשלה, שמטרתם:
* להבטיח כי המידע והמערכות היוצרות אותו ומטפלות בו יוגנו מפני פגיעה, חשיפה ו/או שימוש לרעה שלא כדין.
* להבטיח כי ישמרו השלמות, הזמינות, המהימנות, הסודיות והשרידות של המידע.

אינטרנט רשת מידע ותקשורת ציבורית בין לאומית אליה ניתן לגשת באמצעות התקני תקשורת מתאימים ישירות ממחשב אישי בודד או ממחשב ברשת.

"אל פסק" (UPS) מכשיר המחובר בין המחשב לבין מקור הזרם ומאפשר למחשב לפעול גם בעת הפסקת חשמל. כמו כן, מקטין המכשיר את הסיכון של הזדקרות מתח. באנגלית ובקיצור מכונה המכשיר UPS.

אלפא- נומריים אלפא-ביתיים וספרתיים. הכוונה לתווים במחשב שיכולים להיות שילוב בין תווים אלפא-ביתיים (אותיות), לבין תווי ספרות.

אמצעי קלט/פלט טפסים, דוחות, מצעים מגנטיים/אופטיים המכילים מידע.

אתר מקום גיאוגרפי בו מופעלים מחשבים.

בטיחות פעילות ואמצעי הגנה כנגד סיכוני אש, מים וחשמל.

גורמי חוץ ספקי חומרה ותוכנה, גורמי ייעוץ, ספקי ציוד ואמצעים, ספקי שירותים (כגון: חשמלאים, עובדי ניקיון, שליחים וכד'), גורמי מחקר (מאקדמיה ואחרים).

גיבוי יצירת מאגרי נתונים ותוכנות חליפיים, שיוכלו לסייע להקים מחדש את המאגרים במחשב, במקרה של נזק למאגרים המקוריים. הגיבוי משקף את מצב הנתונים והתוכנות במועד יצירתו. כגון: יצירת העתק של מידע שבמחשב, על דיסקטים או קלטות.

דור גיבוי מהלך גיבוי שנוצר לצורך שחזור נתונים או תוכנות. לדוגמא: כאשר אנו אומרים "גיבוי שבועי בשלושה דורות", הכוונה לגיבוי שעושים בכל שבוע ושומרים תמיד את הגיבויים של שלושה שבועות אחרונים.

דיסק קשיח הדיסק הקבוע בתוך המחשב, בו מאוחסנים הנתונים והתוכנות.

הרשאה מתן אפשרות גישה במחשב אל תוכנה או אל מאגר נתונים. ההרשאה ניתנת באופן שמגדיר
מי רשאי לגישה, מאיזו עמדת עבודה ומה מותר לו לעשות במערכת (אם בכלל), לקרוא חומר, לעדכן נתונים וכו'.

וירוס סדרת פקודות מזיקה שנכתבה בזדון ע"י גורם אנושי. הוירוסים עלולים לשבש ולפגוע בתוכנות או במאגרי הנתונים. הווירוס מגיע למחשב ממקור חיצוני ויכול לחדור למערכת בעיקר במקרה של שימוש בקלטת או בדיסקט בלתי בדוקים.

חומרה מכלול הציוד במערכת הממוחשבת: מחשב, מדפסת, דיסק קשיח, מכשיר "אל פסק" וכד'.

יחידה מסגרת ארגונית, כגון: אגף, שירות, מחוז, מחלקה, תחום, מעון.

מאגר מידע ממוחשב אוסף נתונים בתחום מסוים, המאוחסנים במחשב. ניתן לעבד נתונים אלה

באופן קבוע באמצעות תוכנה.

מודם מתקן המאפשר תקשורת בין מחשב למחשב או בין מחשב למסוף הנמצאים במרחקים גדולים. המודם מחבר בין המחשב/מסוף לבין קו התקשורת, בכל מקרה של תקשורת בין שני אתרים, ישנו מודם בכל אחד משני קצותיו של קו התקשורת.

מחשב נייד מחשב הניתן לנשיאה ולעבודה עצמאית ללא חיבור קבוע לרשת חשמל.

מחשב שרת המחשב המרכז את רשת התקשורת המקומית. במחשב השרת נמצאים מאגרי הנתונים והתוכנות העיקריים. יתר המחשבים הקשורים לרשת עושים כולם שימוש בחומר המאוחסן במחשב השרת.

מידע נתונים שעניינם צנעת הפרט, נתונים תפעוליים של המשרד, נתונים סטטיסטיים וכד׳. הבאים לידי ביטוי באופנים הבאים: מסמכי מקרו, תדפיס – כולל תדפיס מחשב, אמצעי אחסון מחשבי – מגנטי או אחר, או נתונים שנמסרו בעל פה.

מנהל מאגר מנהל הממונה על מאגר מידע.

מצעים מגנטיים אמצעים עליהם ניתן לאחסן נתונים ותוכנות באופן מגנטי.

מצעים מגנטיים נתיקים אמצעים מגנטיים השומרים את הנתונים באמצעות מצע שניתן להפרידו פיזית מן הציוד. לדוגמא: קלטת, דיסקט, תקליטור וכדומה.

״נובל״, NT סוג מערכות תוכנה לניהול רשת תקשורת מקומית.

סיווג מידע אפשריות שלוש רמות של סיווג (בהיבט של צנעת הפרט או חשיבות הנתונים): ״בלתי מסווג״, ״חסוי״, ״חסוי ביותר״.

סיסמא רצף של אותיות וספרות המהווה תנאי להתחבר אל המערכת הממוחשבת ולקבל ממנה הרשאה לבצע פעולות מסוימות. הסיסמא הנה סודית על מנת למנוע שימוש בלתי מורשה.

ענ״א ראשי תיבות: עיבוד נתונים אוטומטי. הכוונה לפעילות באמצעות המחשב.

רשת תקשורת מקומית תשתית המורכבת מחומרה ותוכנה המחברת מספר מחשבים אישיים. במרכז הרשת – מחשב שרת. הרשת פועלת באמצעות תוכנה מיוחדת (כגון ״נובל״) ובעזרת חיבור פיזי בין כל המחשבים ברשת.

תו סימן אחד – אות או סיפרה, או סימן מיוחד (כגון: א, ב, ג, 8, 3, A, @, # וכו׳).

תוכנה תוכנית מחשב הכוללת הוראות בשפה ״מובנת״ למחשב ומאפשרת לבצע פעולות עיבוד נתונים. לדוגמא: מעבד תמלילים WORD, EXCEL וכו׳.

תקשורת חיוג תקשורת של מערכת ממוחשבת באמצעות קו חיוג טלפוני רגיל.

לוג (LOG) ״יומן״ המנוהל אוטומטית ע״י המחשב ובו נרשמות הפעולות הנעשות במחשב. כגון: שימוש במחשב, סיום השימוש במחשב, רישום שינויים בנתונים, ניסיונות לבצע פעולה חריגה או בלתי מורשית.

סיסטם (SYSTEM) מערכת הפעלה = תוכנה בסיסית הנחוצה לתפעול המחשב ואשר בלעדיה לא ניתן להפעילו. כגון: דוס- DOS וחלונות WINDOWS.