מדינת ישראל
משרד האוצר - אגף שוק ההון, ביטוח וחסכון

כ"ד בתשרי התשס"ז
16 באוקטובר 2006

חוזר גופים מוסדיים 6-9-2006
סיווג: כללי

הוראה לניהול סיכוני אבטחת המידע של הגופים המוסדיים

בתוקף סמכותי לפי סעיף 2 (ב) לחוק הפיקוח על שירותים פיננסיים (ביטוח), התשמ"א- 1981, ולאחר התייעצות עם הועדה המייעצת, אני מורה כדלקמן:

1. מבוא

התפתחות המערך הטכנולוגי התומך בפעילות העסקית בתחום הביטוח והגמל, יוצר הזדמנויות עסקיות חדשות ומצד שני טומן בחובו סיכונים למידע האגור בו. לכן, על הנהלת הארגון (וגורמים אחרים הפועלים בתחום כגון סוכני ביטוח) להגן על המידע אודות לקוחותיה.

לצורך כך, על הארגונים להקצות משאבים (כספיים, אנושיים וטכנולוגיים) ליישם בקרות ומנגנוני אבטחת מידע. הוראה זו מתווה את העקרונות לצמצום הסיכונים הנובעים משימוש במערכות מידע.

הוראה זו מתבססת על עקרונות אבטחת מידע מקובלים והסתייעה ברגולציות שהותוו ע"י הגופים הבאים:

1. ארגון התקינה הבריטי: BS7799;
2. המפקח על הבנקים (ישראל): ניהול בנקאי תקין, ניהול טכנולוגיות המידע, הוראה 357;
3. ועדת באזל לפיקוח בנקאי: Risk Management Principles for Electronic Banking;
4. HIPAA Security Standard: Department of Health and Human Services, United States.

מבנה ההוראה כולל שלושה תחומים עיקריים:

1. דרישות לנושא ניהול אבטחת המידע בארגון;
2. דרישות כלליות ליישום בקרות אבטחת מידע;
3. אופן טיפול בנושאים הדורשים תשומת לב מיוחדת.

על הארגון להגדיר עקרונות שימוש מאובטח במערכות מידע של הארגון. עקרונות אלה יגדירו את אופן השימוש בשרתים, מחשבים נייחים, מחשבים נישאים, ציוד תקשורת וכל ציוד מחשובי אחר המשמש את הארגון לצורכי עיבוד או שמירת מידע.

בקרות ומנגנוני אבטחת מידע יטפלו בגילוי, מניעה, תיעוד והתרעה של חשיפה ואירועי אבטחת מידע. אבטחת המידע תטפל בנושאי זמינות ושרידות (Availability), אמינות שלמות ודיוק (Integrity) וסודיות (Confidentiality).

על עקרונות אלו להתייחס לפחות לנושאים כגון שימוש ברשת האינטרנט, שימוש בדואר אלקטרוני, שמירה וטיפול במידע, הרשאות גישה לוגיות ופיזיות, שמירה ושימוש בסיסמאות, נעילת המחשב בפני גישה כאשר אינו בשימוש וכדומה.

יישום ההוראה הינו תהליך מורכב הדורש תכנון קפדני בהתאם לאופי הארגון. הוראה זו אינה מבחינה בשונות שבין הגופים המוסדיים (להלן – "הארגונים"). היקף הפעילות הנדרשת ביישום ההוראה ייגזר בהתאם לפעילות העסקית של הארגון ולמידת מוכנותו לדרישות ההוראה. לשם יישום ההוראה, הארגון ישקול את יישום ההוראה באופן הבא:

1. הקמה והטמעה של נושאי ניהול אבטחת המידע בארגון;
2. בניית תוכנית עבודה ליישום ההוראה;
3. הגדרת מדיניות אבטחת מידע, סיווג נכסים וביצוע הערכת סיכונים;
4. תכנון אופן יישום בקרות אבטחת המידע, כולל כתיבת נהלים;

רח' קפלן 1, ירושלים 91036 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

5. יישום בקרות ומנגנוני אבטחת מידע, אמינותם, מנגנוני דיווח ואופן הטיפול באירועים אלו.

כבר כיום קיימת התייחסות לנושאי אבטחת מידע בחוקים שונים כגון חוק הגנת הפרטיות התשמ"א- 1981 (להלן – "חוק הגנת הפרטיות"). על אף זאת, חוקים אלה אינם נותנים מענה לאופי הפעילות בארגונים. מערכות המידע השונות בארגונים מכילות מידע רגיש מסוגים שונים הנגיש למגוון גורמים, הן בתוך הארגון והן מחוצה לו. על כן, הוראה זו מרכזת את נושאי אבטחת המידע ותהווה אבן בסיס להגנה על מידע זה.

רח' קפלן 1, ירושלים 91036 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

מדינת ישראל
משרד האוצר - אגף שוק ההון, ביטוח וחסכון

תוכן עניינים

1. מבוא 1

2. דרישות ניהול אבטחת מידע 4

2.1 ניהול אבטחת מידע 4
2.2 מדיניות אבטחת מידע 5
2.3 סיווג נכסים והערכת סיכוני אבטחת מידע 5
2.4 סקרי סיכוני אבטחת מידע ומבחני חדירה מבוקרים 6
2.5 נהלים 6

3. בקרות אבטחת מידע 6

3.1 אבטחת מידע בניהול משאבי אנוש 6
3.2 אבטחה פיזית וסביבתית 7
3.3 ניהול תקשורת ותפעול 8
3.4 בקרת גישה לוגית 10
3.5 ניהול סיסמאות 12
3.6 בקרות ומנגנוני קריפטוגרפיה (CRYPTOGRAPHY) 12
3.7 פיתוח ותחזוקה של מערכות 13
3.8 ניהול המשכיות עסקית (BUSINESS CONTINUITY MANAGEMENT) 13
3.9 מיקור חוץ (OUTSOURCING) 14
3.10 נתיב בקרה (AUDIT TRAIL) 15

4. נושאים מיוחדים לטיפול 16

4.1 סוכנים וסוכנויות ביטוח 16
4.2 קישור עובדים לאינטרנט 16
4.3 דואר אלקטרוני 17
4.4 מסחר ושירותים מקוונים 17

5. החלת ההוראה 17

5.1 תחולה 17
5.2 תחילה 18
5.3 ביטול תקפות 18
5.4 הוראות מעבר 18

6. נספח מונחים 18

רח' קפלן 1, ירושלים 91036 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

2. דרישות ניהול אבטחת מידע[1]

2.1 ניהול אבטחת מידע

מטרה: להבטיח שאבטחת מידע מוטמעת כראוי בטכנולוגית המידע של הארגון.

2.1.1 מחויבות דירקטוריון

א) דירקטוריון הארגון יגדיר ויאשר את מדיניות אבטחת המידע בארגון.

ב) דירקטוריון הארגון ידון לפחות אחת לשנה, ועם כל שינוי משמעותי בהיערכות אבטחת מידע, ויאשר את תוכניות ההנהלה לאבטחת מידע.

ג) ועדת הביקורת של הדירקטוריון תוודא שמבקר הפנים עורך ביקורות בנושאי אבטחת המידע עם אנשי מקצוע בעלי כישורים מתאימים, בפרקי זמן סבירים ולפי העניין. ועדת הביקורת תאשר את נושאי ביקורת הפנים, וכן תדון ותטפל בממצאי מבקר הפנים.

2.1.2 מחויבות ההנהלה

א) הנהלת הארגון תקים ותטמיע תהליך ניהול אבטחת מידע בארגון.

ב) ההנהלה תוודא שמטרות, יעדים ותוכניות אבטחת מידע מוגדרות וממומשות.

ג) ההנהלה תספק משאבים מספקים לפיתוח, הטמעה, תפעול ובקרה של אבטחת מידע בארגון.

ד) ההנהלה תגדיר תפקידים ותחומי אחריות באבטחת מידע.

2.1.3 ניהול אבטחת המידע בארגון

א) הנהלת הארגון תמנה את אחד מחברי ההנהלה בעל כישורים מתאימים, בכפיפות למנכ"ל אשר יהיה ממונה על נושאי אבטחת המידע בארגון (להלן – "הממונה"). אין בהוראה זו כדי לפגוע בחובת מינוי ממונה לפי סעיף 17ב לחוק הגנת הפרטיות.

ב) הממונה יהיה אחראי על פיקוח ובקרה על הפעילות המתבצעת בתחומי אבטחת מידע וכן על בקרה על תכנית עבודה בנושא אבטחת המידע בהתאם למדיניות אבטחת המידע של הארגון.

ג) הנהלת הארגון תמנה מנהל אבטחת מידע שיהיה כפוף לממונה בנושאי אבטחת המידע בארגון ותעמיד לרשותו את המשאבים הדרושים לניהול אבטחת מידע.

ד) מנהל אבטחת המידע:

1. לא יעסוק בתחומים ביצועיים ותפעוליים של מערכות המידע אשר עלולים לגרום לניגוד עניינים עם נושאי אבטחת מידע.
2. יהיה אחראי על יישום מדיניות אבטחת המידע.
3. יהיה אחראי על בקרת אבטחת המידע בארגון.
4. יהיה אחראי על החדרה והטמעה של פתרונות אבטחת מידע בכל הרמות (תשתית ויישומים, נהלי אבטחת מידע) בארגון.
5. ינחה מקצועית את הארגון בהובלת נושאי אבטחת מידע.

ה) מנהל אבטחת המידע יהיה בעל כישורים וניסיון בתחום אבטחת מידע.

---

[1] א. השימוש באמצעים מקובלים יחול על כל סעיפי ההוראה (כמפורט בסעיף 3.3.2 ג') בכל מקום שלהנחת הארגון יש להשתמש בהם או שהשימוש בהם עדיף על השימוש באמצעים שצוינו בהוראה זו; ב. ההוראה חלה על כל סוגי התקשורת: תשתית תקשורת ציבורית, תקשורת פנימית, תקשורת טלפוניה ותקשורת אחרת ככל שתהיה (ולא רק על מסחר ושירותים מקוונים- סעיף 4.4), הכל לפי רמות הסיכון ולפי הענין.

רח' קפלן 1, ירושלים 91036 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

2.2. מדיניות אבטחת מידע

מטרה: להתוות ולהגדיר מדיניות אבטחת מידע שתנחה את הארגון בהנחלת הנחיות אבטחת מידע בארגון.

א) כאמור בסעיף 2.1.1 א', דירקטוריון הארגון יגדיר ויאשר את מדיניות אבטחת המידע בארגון.

ב) המדיניות תתועד במסמך אשר יופץ בכל הארגון וישמש כבסיס לפיתוח בקרות אבטחת מידע ולכתיבת נהלי אבטחת המידע.

2.3. סיווג נכסים והערכת סיכוני אבטחת מידע

מטרה: לשמור על אבטחת מידע נאותה של נכסי הארגון.

2.3.1. סיווג נכסי מידע

א) הארגון ייצור ויתחזק רשימת מלאי של כל נכסי המידע העיקריים של כל מערכת. רשימה זו תנוהל במאגר ממוחשב באופן שוטף.

ב) הארגון יסווג נכסים אלה לפי רמת רגישותם ויגדיר להם את בקרות אבטחת המידע הנדרשות. תהליך הסיווג ייקח בחשבון את הדרישות העסקיות לשיתוף וגישה למידע, ואת ההשלכות העסקיות הנובעות מכל דרישה.

ג) רמות הסיווג יצביעו באופן ברור על רגישות נכסי המידע. כותרות רמות הסיווג יהיו ברורות וחד משמעיות.

ד) נכסי מידע המכילים מידע שיש בזליגתו כדי לפגוע פגיעה מהותית במבוטחים/עמיתים, ובין היתר, מידע על אישיותו של אדם, מצב בריאותו ומצבו הכלכלי, ככל שיש בו כדי לפגוע פגיעה מהותית במבוטחים/עמיתים, יסווגו בכל מקרה כבעלי סיווג גבוה. לסיווג גבוה זה יש השלכות המוגדרות באופן ייחודי בהוראה זו.

2.3.2. הערכת סיכוני אבטחת מידע

א) הארגון יקיים תהליך של הערכת סיכוני אבטחת מידע במערכות המידע והממשקים בארגון.

ב) הערכת הסיכונים תגדיר את רמת הרגישות של המערכות ותתייחס למכלול סיכוני אבטחת המידע הפוטנציאלים הנובעים ממערכות המידע ומההתנהלות העסקית השוטפת של הארגון. סיווג רמת הרגישות של כל מערכת תיקבע לפי המידע בעל הרגישות הגבוהה ביותר בו היא מטפלת.

ג) תהליך זה יתבסס על סיווג הנכסים, אופי העבודה במערכים והאגפים השונים בארגון והאופי העסקי של הארגון.

ד) הארגון יעדכן את הערכת הסיכונים עם שינויים משמעותיים בתהליכים העסקיים, במערכות המידע או באיומי אבטחת מידע.

ה) תוצר הערכת הסיכונים ינחה את הנהלת הארגון בהפניית משאבים נאותים להטמעת אמצעי אבטחת מידע ולמיקוד בסקרי סיכוני אבטחת המידע במערכות השונות בארגון.

ו) תוצר הערכת הסיכונים, המתבסס בין היתר על סיווג נכסי המידע, יספק מדרג רגישות של מערכות שונות בארגון.

ז) המערכות הבאות יסווגו כמערכות בעלות סיכון גבוה:

1. מערכות המכילות מידע שסווגו בסיווג גבוה, לפי סעיף 2.3.1;
2. מערכות המכילות מידע אחר ככל שקבע הארגון.

בנוסף יוגדרו הממשקים הבאים כסיכון גבוה:

3. קישור סוכנים וסוכנויות ביטוח ונותני שירותים אחרים מחוץ לארגון לרשת הארגון;

רח' קפלן 1, ירושלים 91036 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

4. תקשורת דרך רשת ציבורית אל תוך רשת המידע בארגון המכיל מידע רגיש.

2.4. סקרי סיכוני אבטחת מידע ומבחני חדירה מבוקרים

מטרה: להבטיח עמידת מערכות המידע בדרישות מדיניות אבטחת המידע של הארגון ושל מתודולוגיות אבטחת מידע מקובלות בעולם.

א) מנהל אבטחת המידע ייזום סקרי אבטחת מידע של מערך טכנולוגיית המידע של הארגון.

1. מערכות בעלות סיכון גבוה ייסקרו לפחות אחת ל – 18 חודש.
2. לגבי מערכות אחרות ההנהלה תקבע את תדירות הסקרים בהתאם לרגישות המערך.

ב) הסקרים יבחנו את נושאי הניהול ואת יעילות אמצעי ההגנה (כולל אמצעים פיזיים ולוגיים) שיושמו בארגון ואת רמת הגדרות אבטחת המידע במערכות המידע הן ברמת התשתית (ציוד ותווך תקשורת, מערכות הפעלה, בסיסי נתונים) והן ברמת האפליקציה (ברמת קוד מקור או חבילות תוכנה).

ג) הארגון יערוך סקרי אבטחת מידע לפני הטמעת שינויים משמעותיים במערכות שהוגדרו ע"י הארגון כבעלות סיכון גבוה לפי הערכת הסיכונים, בהתאם לסעיף 2.3.2, כאשר חלו שינויים משמעותיים במערכות אלו או לפני הכנסת מערכות אלו לשימוש תפעולי (Production).

ד) מנהל אבטחת המידע ייזום מבחני חדירה (Penetration Tests) הן ברמת התשתית והן ברמת היישום (אפליקציה), המדמים ניסיונות פריצה ע"י פורצים מתוך ומחוץ לארגון, הן כמשתמש קיים והן כפורץ ללא חשבון קיים, למערך הטכנולוגי. תדירות מבחני החדירה תיקח בחשבון את רגישות המערך בהתאם לסעיף 2.3.2. מערכות מידע הפתוחות לתווך תקשורת ציבורי, יעברו מבחני חדירה לכל הפחות אחת ל – 18 חודש.

ה) סקרי אבטחת המידע ומבחני החדירה התקופתיים ייערכו ע"י גורם מקצועי, עצמאי, בלתי תלוי וחיצוני לארגון.

ו) הנהלת הארגון תקיים דיונים על תוצאות סקרי אבטחת המידע ומבחני החדירה ותפעל למימוש המלצותיהם תוך פרק זמן סביר.

2.5. נהלים

א) לכל תהליך המטפל בניהול, הכנסה, תפעול, תחזוקה, והוצאה של מידע בארגון, כולל מערכות המכילות זיכרון נייד כדוגמת מחשבים ניידים וסייען דיגיטלי (Personal Digital Assistant), ייכתב נוהל אבטחת מידע מפורט. לכל הפחות, ייכתבו נהלים לכל הנושאים המפורטים בהוראה זו.

ב) נהלים אלה ייגזרו ממדיניות אבטחת המידע ומצרכי אבטחת המידע בארגון.

ג) ההנהלה תאשר את הנהלים עם כתיבתם או את השינויים המהותיים בהם ותפעל להטמעתם.

ד) הנהלים יעברו תהליך בדיקה ועדכון בהתאם לצורך, עם שינוי משמעותי בסביבה הטכנולוגי או לאחר אירוע אבטחת מידע, ולכל הפחות אחת ל – 24 חודש.

3. בקרות אבטחת מידע

3.1. אבטחת מידע בניהול משאבי אנוש

מטרה: להקטין סיכונים הנובעים מטעות אנוש, גניבה, הונאה או שימוש לרעה במערכות.

רח' קפלן 1, ירושלים 91036 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

3.1.1. אבטחת מידע בתהליכי גיוס עובדים

א) עובדים המגויסים לארגון יעברו בדיקות רקע, אשר מטרתן לאמת את הנתונים שנמסרו על-ידי המועמד/ת. במסגרת זו, תיבדק אמינות הנתונים.

ב) עבור משרות רגישות הנוגעות במידע, כפי שיוגדרו על-ידי מנהל אבטחת המידע, יבוצעו בדיקות רקע ואמינות נוספות.

ג) חוזה הנחתם עם עובדים חדשים יכלול התייחסות לאחריות העובד בכל הנוגע להיבטי אבטחת מידע, וילווה בהצהרת סודיות.

ד) חוזה של הארגון עם חברות כוח אדם/השמה או עם חברות המספקות שירותי מיקור חוץ (Outsourcing), יכלול התייחסות בכל הנוגע לבדיקות המבוצעות בתהליכי גיוס העובדים.

3.1.2. אבטחת מידע בעת העסקת עובדים והגברת המודעות שלהם

א) מנהל אבטחת המידע יגדיר מהן הפעולות שיש לבצע כדי לשמור על נכסי המידע של הארגון, פעולות אלו יכללו גם אמצעים שינקטו לגבי התקשרות של העובדים מחוץ למקום העבודה.

ב) לגבי עובדים להם יש נגישות למידע רגיש או מידע בעל סיכון גבוה, יוגדרו על-ידי מנהל אבטחת המידע, פעולות נוספות המיועדות למנוע את זליגת המידע.

ג) מנהל אבטחת המידע יגדיר תוכנית הדרכה להעלאת רמת מודעות העובדים לאבטחת המידע בארגון.

ד) לעובדים יינתנו הדרכות אבטחת מידע בהתאם למידת הידע הנחוץ לכל בעל תפקיד.

3.1.3. אבטחת מידע בסיום העסקת עובדים

א) לעובדים (כולל עובדים חיצוניים לארגון) המסיימים את העסקתם בארגון, בין אם ביוזמתם או ביוזמת המעסיק, ייחסמו הרשאות הגישה למידע (בין אם למערכות מידע ובין אם לאמצעים פיזיים).

ב) הארגון יוודא כי בסיום ההעסקה לא יישארו נכסי מידע של הארגון בידי העובד.

ג) מנהל אבטחת המידע יגדיר את אופן הטיפול בעובדים בהיבטי אבטחת מידע לתקופת הזמן שבין הודעת העזיבה לסיום העסקה. יש להגדיר דרישות לפחות בנושאי בקרת גישה, עבודה על מערכות ומסמכים, עבודה על תוכנת דואר אלקטרוני.

3.2. אבטחה פיזית וסביבתית

מטרה: למנוע גישה לא מורשית, נזק והפרעה בחצרי העסק ואל המידע העסקי של העסק.

3.2.1. אזורים מאובטחים

א) הארגון יחלק את סביבת העבודה למעגלי אבטחה/אזורים מאובטחים לפי רמות רגישות. להלן דוגמא לאופן חלוקת אזורים לפי רמת רגישות: גבוהה (כגון חדרי שרתים), עסקית (אזור עבודה לעובדי משרד אחורי – Back Office), ציבורית (הקהל הרחב רשאי להסתובב באזור זה).

ב) הארגון יקבע את רגישות אזורי עבודה ואופי ההגנה עליהם, על סמך המידע הנשמר בכל אזור וסוגי הקהל (עובדים, סוכנים, נותני שירותים, עמיתים/מבוטחים וכדומה) בהתאם לסעיף 2.3.2.

ג) הארגון יישם מספר מעגלים של בקרות גישה פיזית. אם אין ביכולת הארגון ליישם בקרת גישה פיזית, עליו ליישם לכל הפחות בקרות ניטור בכל אחד מאתריו. רגישות המידע ומערכות המידע ייבחנו לכל אזור ויוגדרו מורשי גישה לכל אזור.

ד) בהתאם להערכת הסיכונים יוגדרו בקרות פיזיות לאבטחת המידע.

ה) על בקרת הגישה באזורים המוגדרים ברגישות גבוהה לכלול לפחות שער כניסה אחד הנפתח ע"י אמצעי זיהוי חזק, לפי סעיף 3.4.2 סעיף קטן ו'. דוגמא לאזור ברגישות גבוהה: חדר השרתים.

רח' קפלן 1, ירושלים 91036 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

ו) ארגונים המעניקים שירותי קבלת קהל במשרדיהם, ישקלו הפרדה בין האזור בו ניתנים שירותים אלו, לבין אזורי העבודה השוטפים בארגון. בכל מקרה, לא יתאפשר לגורם, שאינו מורשה, להסתובב במשרדי הארגון ללא פיקוח.

ז) האזורים הציבוריים המכילים מידע המסווג כרגיש (כגון תכתובות או פוליסות של לקוחות, מדיה המכילה מידע הנשלח לסוכנים וכדומה) יוגנו וימודרו בפני גישה של אנשים שאינם בעלי הרשאה למידע. אזורים אלה כוללים בין השאר משרדים, תאי הדואר של הסוכנים, ארכיונים, אזורי טעינה ופריקה של ציוד.

3.2.2. אבטחת ציוד וניירת

א) הוצאת ציוד המכיל מידע רגיש מאחד ממעגלי האזורים המאובטחים תיעשה בהתאם להערכת הסיכונים.

ב) הארגון יוודא שציוד המכיל מידע רגיש ומיועד להשמדה או תחזוקה או נמסר אל גורם מחוץ לארגון אינו מכיל מידע על לקוחות.

ג) מדיית זיכרון שהכילה מידע בסיווג גבוה, לפי סעיף 2.3.1, תוצא אל מחוץ לארגון לצורכי תחזוקה רק לאחר שנקטו אמצעים מספקים למחיקת המידע באופן המונע אפשרות שחזור המידע באמצעים טכנולוגים גם לאחר מחיקה המידע.

ד) בהתאם להערכת הסיכונים, סעיף 2.3.2, תונהג מדיניות המגדירה את אופן הטיפול במצעים פיזיים, כולל במסמכים הנשלחים לסריקה מחוץ לארגון, בעת שימוש שוטף ובעת סיום יום העבודה או עזיבת סביבת העבודה.

ה) הארגון יוודא גריסה או השמדה של מצעים רגישים אשר אין בהם שימוש.

ו) יש להגדיר אופן טיפול מאובטח בניירת המכילה מידע בעל סיווג גבוה, כולל בהעברה להשמדה.

ז) ניירת המגיעה לסריקה תאובטח באופן נאות, כולל בתהליך הגניזה וההשמדה.

3.3. ניהול תקשורת ותפעול

3.3.1. נוהלי תפעול ואחריות תפעול

מטרה: להבטיח פעולה רציפה ובטוחה של מערכות מידע.

כדי להבטיח פעולה רציפה ומאובטחת של מערכות המידע בארגון יש ליישם תהליכים מבוקרים של תפעול מערכות המידע ולתעדם בנוהל המתייחס בין היתר לנושאים הבאים: תהליכים, חלוקת אחריות, בקרות, טפסים.

3.3.2. הגנה מפני ניסיונות פגיעה

מטרה: להגן על שלמות ואמינות המידע ומערכות המידע ולמנוע פגיעה במשתמשים.

א) על מנת להגן על רשת הארגון ומשתמשיו, יתקין הארגון אמצעים מקובלים ונאותים המצמצמים את החשיפה לניסיונות פגיעה (כולל איתור, זיהוי ומניעת ניסיונות אלה). אמצעים אלו יגנו מפני שימוש לא תקין במידע, במערכות המידע ובבסיסי הנתונים. דוגמא לאמצעים המצמצמים את החשיפה לניסיונות פגיעה הינה קיומן של מערכות לאיתור ניסיונות חדירה מהאינטרנט ומתוך הארגון (IDS/IPS), מערכות לסינון תכנים (Content Filtering) וכדומה.

ב) הארגון רשאי להשתמש באמצעים מקובלים ונתונים אחרים, ובלבד שמהות אבטחת המידע הנדרשת בסעיף זה לא תפגע.

ג) על הארגון להתאים את האמצעים המקובלים והנאותים בהתאם להתפתחויות הטכנולוגיות שישררו באותה עת, ולאיומים ולחשיפות הרלוונטיים לאותה תקופה.

רח' קפלן 1, ירושלים 91036 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

3.3.3. גיבוי מידע

מטרה: לקיים את שלמות וזמינות המידע, שירותי עיבוד המידע ושירותי התקשורת.

א) הנהלת הארגון תגדיר דרישות גיבוי למערכות המידע השונות בהתאם לרמת הרגישות שנקבעה בהערכת הסיכונים, בהתאם לסעיף 2.3.2.

ב) מנהל אבטחת המידע יהיה אחראי על בקרת איכות הגיבויים.

ג) אמצעי הגיבוי ישמרו במקום מרוחק, מאובטח ומוגן בפני פגיעה באמצעים ובתוכנם.

3.3.4. זמינות נתונים

מטרה: להבטיח זמינות של מידע חיוני.

א) הארגון יישם כלים להבטחת זמינות הנתונים של מידע שהוגדר כחיוני בתהליך הערכת הסיכונים.

ב) לצורך כך ישקול הארגון שימוש בכפילות ויתירות של מערכות, במערכות לחלוקת עומסים, בכלים לייצוב מתח חשמלי וכדומה.

3.3.5. ניהול רשת

מטרה: להבטיח את הגנת המידע ברשתות ואת הגנת התשתית התומכת.

א) קישור גורמים חיצוניים מ/אל רשת הארגון יתבצע באופן ריכוזי, דרך מספר נקודות כניסה מאובטחות. לא תאושר כל התחברות "עצמאית", שאינה דרך נקודות כניסה מאובטחות אלה.

ב) ייושם מידור בין החלקים השונים ברשת באמצעות חלוקה לוגית או פיזית של הרשת והגבלת אפשרות הקישור בין הרשתות השונות. רמת המידור תיקבע בהתאם לרמת הרגישות של המערכות, בהתאם לסעיף 2.3.2.

ג) תיושם בקרה וסינון של תקשורת יוצאת ונכנסת על פי הגדרות הארגון.

ד) תיושם בקרה על הפעילויות המתבצעות במערכות לאיתור אירועים חריגים. בנוסף לבקרה בדיעבד, תיושם בקרה בזמן אמת.

3.3.6. טיפול במצעים (Media) ואבטחתם

מטרה: למנוע נזק לנכסים, והפרעות לפעילות העסקית.

א) הארגון ישקול איסור שימוש במצעי זיכרון נתיקים (כגון דיסקים, דיסקטים, זיכרון Flash) ובכל מקרה יוגדר שימוש מותר ואסור תוך התחשבות בצרכי אבטחת מידע.

ב) אופן הטיפול והאבטחה של מצעי זיכרון נתיקים ייגזרו בהתאם לשימוש בהם ובמידע האגור בהם, בהתאם לסעיף 2.3.1.

ג) יקבע תהליך מסודר של השמדת מצעים האוגרים מידע רגיש של הארגון.

3.3.7. תהליך העברת מידע רגיש אל מחוץ לארגון

מטרה: להגדיר את רמת האבטחה המינימלית הנדרשת להעברת מידע על פי סיווגו.

א) בהתייחס לרמות סיווג המידע שהוגדר בארגון בהתאם לסעיף 2.3.1, יגדיר הארגון את דרישות אבטחת המידע ההכרחיות ליישום בתהליך העברת המידע אל מחוץ לארגון (למשל לבנקים, לקוחות).

ב) בתהליך העברת מידע בתווך תקשורת ציבורי:

1. מידע שאינו ציבורי יוגן באמצעים מקובלים לשמירת סודיות, אמינות ושלמות הנתונים.
2. מידע שסווג כבעל סיווג גבוה, בהתאם לסעיף 2.3.1, יוגן במנגנוני הצפנה סטנדרטיים.

ג) בתהליך העברת מידע על גבי מדיה או על גבי עותק קשיח כלשהו:

רח' קפלן 1, ירושלים 91036 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

1. העברת מידע שאינו ציבורי תיעשה באופן המבטיח את חשאיות ואמינות המידע.
2. העברת מידע שסווג כבעל רגישות גבוהה, בהתאם לסעיף 2.3.1, תיעשה ע"י גורם אמון ומאושר של הארגון.

3.3.8. הפרדת סביבות

מטרה: למנוע פגיעה במידע בסביבת הייצור התפעולית (Production)

א) סביבת הייצור תופרד מסביבות אחרות כגון פיתוח ובדיקות.

ב) הגישה לרשת הייצור תאופשר ע"י הרשאות מיוחדות בהתאם למדיניות ההרשאות בארגון.

ג) כל גזירת מידע מסביבת ייצור לסביבה אחרת תתבצע באישור מנהל אבטחת המידע, תוך וידוא כי הסביבה אליה נגזר המידע מאובטחת בהתאם לרגישות המידע המועבר.

ד) העברת מערכות ומידע מסביבות פיתוח לייצור תיערך בצורה מבוקרת, בהתאם לנהלים, בכדי למנוע פגיעה בנתונים בסביבת הייצור.

3.3.9. תגובה לאירועי אבטחת מידע

מטרה: להגדיר אופן טיפול באירועי אבטחת מידע בארגון

א) הארגון יגדיר מה הם אירועי אבטחת מידע וישקול על איזה מהם יש להגיב.

ב) הארגון יגדיר מנגנון דיווח על אירועי אבטחת מידע שיהיה נגיש לעובדים.

ג) הארגון יגדיר את אופן התגובה לכל אירוע כזה, למי מדווחים ומהו זמן התגובה הסביר לדיווח.

3.3.10. הגנה על אמצעי מחשוב ניידים

מטרה: למנוע פגיעה באבטחת המידע באמצעי מחשוב ניידים כגון מחשבים ניידים, סייענים דיגיטאליים, טלפונים.

א) הארגון יגדיר מה הם השימושים המותרים בשימוש באמצעי מחשוב ניידים.

ב) הארגון יגדיר את אופן אבטחת אמצעים אלה, בהתאם לסעיף 2.3.1.

ג) במידה ואמצעים אלה מחוברים לרשת הארגון, יש לאבטח את הרשת ואת האמצעים בפני פגיעה הדדית ברמת אבטחת מידע.

3.3.11. גניבת זהות

מטרה: למנוע גניבה של זהות או מידע אישי ע"י התחזות לגורם רשמי המבקש מידע זה

א) הארגון ימפה את ערוצי התקשורת (למשל אתר אינטרנט, דוא"ל, מכתבים) בהם הוא פונה אל הלקוח או צד שלישי ודרכן הלקוח יכול לפנות אליו.

ב) הארגון ישקול יישום מנגנוני אבטחת מידע שיבטיחו את זהות ערוצי תקשורת אלה כשייכים לארגון.

ג) תוגדר פעילות לאיתור ניסיונות התחזות דרך ערוצי תקשורת אלה.

ד) הארגון יידע את לקוחותיו בדבר הסיכונים הכרוכים בשימוש בערוצי תקשורת.

3.4. בקרת גישה לוגית

3.4.1. אכיפת בקרות גישה

מטרה: לאכוף מדיניות בקרות גישה למערכות מידע.

א) ייושמו מנגנונים ממוכנים לניהול בקרות גישה במערכות מידע וביישומים (אפליקציות).

רח' קפלן 1, ירושלים 91036 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

ב) בקרות גישה יורכבו מאמצעי זיהוי ובקרת הנתיב בין תחנת הקצה לשירות/שרת.

ג) מדיניות בקרת גישה תיקח בחשבון מידור מתאים של הרשאות בין הארגון לחברות בנות וחברות אחרות השייכות לארגון ושאינן בהכרח גוף מוסדי.

3.4.2. אמצעי זיהוי

מטרה: לזהות באופן חד ערכי כל מורשה גישה למערכות מידע.

א) ייקבעו אמצעי זיהוי למערכות ושירותים לצורך זיהוי חד ערכי (Unique User ID) של המשתמש.

ב) אמצעי הזיהוי יהיו אישיים ולא יותר שיתוף של אמצעי הזיהוי.

ג) אמצעי הזיהוי יוחלו הן על עובדי הארגון והן על משתמשים אחרים (לקוחות, ספקים וכדומה) המתחברים למערכות הארגון.

ד) לכל הפחות, אמצעי הזיהוי יורכבו משילוב של שם משתמש (User Name) וסיסמא.

ה) נתוני הזיהוי יישמרו חסויים (הן בתווך התקשורת והן במערכות השונות).

ו) למערכות המוגדרות כבעלות סיכון גבוה, בהתאם לסעיף 2.3.2, הארגון ישקול שימוש באמצעי זיהוי חזק כמוגדר בפרק 6 (נספח מונחים). יש להשתמש בטכנולוגיה המונעת אפשרות העתקה או שחזור הפריטים.

ז) ייקבע פרק זמן של אי פעילות (Session Time Out) במערכת שלאחריו יופעל מנגנון ניתוק תקשורת שיחייב זיהוי מחדש של המשתמש. במידה ומנגנון הניתוק מטיל מגבלה על פעילות בעלת אופי רציף, יש להתריע לפני ניתוק התקשורת.

3.4.3. ניהול הרשאות

מטרה: לוודא שהרשאות גישה למערכות מידע מאושרות, מוקצות ומתוחזקות כראוי.

א) יוגדר תהליך רישום וביטול רישום להרשאות גישה למערכות מידע ולשירותים.

ב) מתן הרשאות גישה למערכות ושירותים יוגבל ויפוקח בהתאם לרגישות המערכות, בהתאם לסעיף 2.3.2, חובה לנהל טבלת הרשאות לעובדים בהתאם לתפקידם ולמידע הנדרש להם לצורך ביצוע תפקידם.

ג) הרשאות הגישה לכל העובדים והמערכות ייבחנו לפי שיקול דעת ההנהלה. לכל הפחות, הפעילות תתבצע אחת לשישה חודשים במערכות בעלות סיווג גבוה.

ד) ניהול ההרשאות ייעשה ע"י מנגנון ממוכן לניהול הרשאות.

3.4.4. בקרת גישה מהאינטרנט/מרחוק

מטרה: לאכוף מדיניות בקרת גישה חזקה בגישה לארגון דרך האינטרנט/תשתית תקשורת ציבורית.

א) בגישה מרחוק לרשת הארגון, על גבי תשתית תקשורת ציבורית, נתוני ההזדהות למערכת יוגנו בפני ציתות (הצפנה מקצה לקצה).

ב) בגישה למערכות לצורך ביצוע פעולות מהותיות ייעשה שימוש באמצעי זיהוי חזק, בהתאם לסעיף 3.4.2, סעיף קטן ו'. אין חובה ליישם סעיף קטן זה על לקוחות שכל עניינם לוודא את מצב חשבונם או את פרטיהם האישיים ובתנאי שמידע זה אינו בעל סיווג גבוה, בהתאם לסעיף 2.3.1.

ג) בקישור עובדים או נותני שירות (כגון סוכנים ושמאים) לרשת הארגון, תווך התקשורת יאובטח בפני ציתות וזליגת מידע. במקרה של חיבור עובדים תאובטחנה גם תחנות הקצה.

ד) הרישום ללקוחות לשירות גישה מהאינטרנט למערכות המכילות מידע בעל סיווג גבוה יבוצע לאחר זיהוי פיזי של מבקש השירות. לחלופין, ניתן לאפשר גישה לשירות ללא זיהוי פיזי באופן אחר המאפשר זיהוי ודאי של מבקש השירות.

רח' קפלן 1, ירושלים 91036 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

ה) בכל מקרה, הגישה לשירות גישה מהאינטרנט לא תאופשר ללא אישור מפורש של הלקוח.

3.5. ניהול סיסמאות

מטרה: לאכוף שימוש בסיסמאות חזקות שתמנענה גישה של משתמשים לא מורשים אל מערכות מידע.

א) הארגון יגדיר מדיניות סיסמאות ויחילה בהתאם לרגישות המערכת, בהתאם לסעיף 2.3.2.

ב) הסיסמא תהיה ידועה אך ורק למשתמש.

ג) הסיסמא הראשונית תוגדר ע"י המשתמש או תימסר לידיו באופן חסוי. בכל מקרה, הסיסמא לא תימסר דרך רשת האינטרנט או דרך התשתית לה נדרשת הסיסמא להזדהות.

ד) במידה וסיסמא נמסרת למשתמש, יש לאמת ראשית את זהות המשתמש. המשתמש יחויב לשנות את הסיסמא בהתחברות הראשונה למערכת. תוקף הסיסמא הראשונית יהיה עד 30 יום ויקבע לפי סוגי הקהל עובדים, סוכנים, נותני שירותים, עמיתים/מבוטחים.

ה) סיסמאות לא ישמרו באופן גלוי (Clear Text) או באופן הניתן לשחזור ברשומות, בזיכרון או במאגרי מידע.

ו) סיסמא תבוטל מיידית בכל מקרה של חשש לפגיעה בחשאיותה. לא יתאפשר לשחזר את הסיסמא.

ז) אי שימוש בחשבון למשך תקופה של חצי שנה יביא לביטול הסיסמא הנדרשת בתהליך ההזדהות לאותו חשבון.

ח) מורכבות הסיסמא, תוקפה ותחולתה לפי סוגי הקהל – עובדים, סוכנים, נותני שירותים, עמיתים/מבוטחים וכדומה – ייקבעו בהתאם לתקנים מקובלים (כגון ת"י 1495). לדוגמא: הסיסמא תורכב משילוב של אותיות וספרות, לא יאופשר שימוש בתווים זהים רצופים, תוקפה יפוג לאחר 60 יום, המערכת תינעל לגישה לאחר 4 ניסיונות גישה כושלים וכדומה.

3.6. בקרות ומנגנוני קריפטוגרפיה (Cryptography)

מטרה: להגן על החיסיון, המהימנות או השלמות של המידע.

3.6.1. מדיניות שימוש בבקרות קריפטוגרפיה (Cryptography)

א) הארגון יפתח ויישם מדיניות שימוש במנגנוני קריפטוגרפיה (Cryptography) להגנה על מידע רגיש.

ב) הארגון יגדיר את סוגי המידע השונים הדורשים שימוש במנגנוני קריפטוגרפיה בהתאם לתהליך סיווג המידע שהארגון ביצע, לפי סעיף 2.3.1.

3.6.2. הצפנה (Encryption)

א) הארגון ישקול יישום מנגנוני הצפנה להגנה על חיסיון מידע בעל סיווג גבוה האגור באמצעי אחסון (קובץ, בסיס נתונים וכדומה), בהתאם לסעיף 2.3.1.

ב) הארגון יישם הצפנה להגנה על חיסיון מידע בעל סיווג גבוה בתווך התקשורת אל מחוץ לארגון, בהתאם לסעיף 2.3.1.

ג) בכל מקרה, יוצפנו כל סיסמאות הגישה לכל המערכות (קצה לקצה).

3.6.3. חתימה דיגיטלית (Digital Signature)

א) הארגון ישקול יישום חתימה דיגיטלית להגנה על מהימנות ושלמות של מידע בעל סיווג גבוה, בהתאם לסעיף 2.3.1.

רח' קפלן 1, ירושלים 91036 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

ב) החתימה תיושם באופן שיאפשר לגופים מחוץ לארגון לזהות את בעלי החתימה הדיגיטלית באופן המקובל בסטנדרטים בין-לאומיים.

ג) בכל מקרה של ביצוע פעולות מהותיות ושינוי פרטים מהותי, כגון, שינוי פרטי מוטב, על גבי מערכות הארגון, בין הארגון ללקוחות הארגון וחברות צד שלישי, על גבי האינטרנט/תשתית תקשורת ציבורית, תיושם חתימה דיגיטלית באופן המבטיח את אימות זהות המשתמש.

3.6.4. מנגנוני מניעת הכחשה (Non-Repudiation)

א) מנגנוני מניעת הכחשה ייושמו בכדי ליישב מחלוקות לגבי התרחשות או אי-התרחשות של אירועים או פעולות, כפי שיוגדר במדיניות אבטחת המידע של הארגון.

ב) בכל מקרה של ביצוע פעולות מהותיות הכולל מידע בעל סיווג גבוה של לקוחות דרך האינטרנט וחברות צד שלישי, יבוצע שימוש בשירות זה באופן המבטיח את אימות זהות המבצע.

3.7. פיתוח ותחזוקה של מערכות

מטרה: להבטיח הטמעת בקרות אבטחת מידע בתהליך פיתוח מערכות מידע.

בתהליך קליטה של מערכות מידע חדשות או בעת שדרוג מהותי של מערכות מידע קיימות, יילקחו בחשבון שיקולי אבטחת מידע.

א) דרישות אבטחת מידע יוגדרו לתהליך פיתוח של מערכות חדשות או שדרוג של מערכות קיימות.

ב) ייושמו מנגנונים קריפטוגרפיים על מנת להבטיח חשאיות (Confidentiality) ואמינות (Integrity) של נתונים בעלי סיווג גבוה, בהתאם לסעיף 2.3.1.

ג) אבטחת מידע תוטמע ברמת היישום (האפליקציה) כולל וידוא קלטים, וידוא פלטים, אימות שדרים, אישור אמיתות נתונים וכדומה.

ד) כאשר פיתוח מערכת נעשה ע"י גורם חיצוני, יש להבטיח בהתקשרות הגנה על נושאים כגון:

1. קניין רוחני כגון בעלות על קוד מקור עם תום הפיתוח.
2. לשקול שמירת קוד מקור אצל נאמן במידה והחברה המפתחת תחדל מלהתקיים.
3. קוד המקור עבר בדיקה נגד פרצות אבטחת מידע וקוד זדוני ונמצא נקי.

מחזור קליטת מערכת חדשה או שינוי מהותי במערכת קיימת יכלול בין היתר את השלבים הבאים:

1. **אפיון המערכת:** אפיון פרמטרים של אבטחת מידע המופיעים בהוראה זו בעת תכנון המערכת, כגון סיסמאות, הרשאות, הצפנות, נפח וטיפול בזיכרון וכדומה.
2. **בניית המערכת:** מימוש דרישות אבטחת המידע המופיעות באפיון המערכת.
3. **בדיקת המערכת:** בדיקות במהלך הפיתוח ובדיקות קבלה בהיבטי אבטחת מידע.
4. **קליטת המערכת:** קבלה והתקנה מאובטחת ומאושרת של המערכת ע"י הגורמים המוסמכים לכך בארגון, תוך שילוב אנשי אבטחת המידע בעת ההתקנה.
5. **שינויים במערכת:** על הארגון לקחת בחשבון שיקולי אבטחת מידע בעת כל שינוי הנעשה במערכת ולהעביר שינוי זה למנהל אבטחת המידע.

3.8. ניהול המשכיות עסקית (Business Continuity Management)

מטרה: להקים תוכנית עסקית לטיפול במצבי שבר וחירום למניעת הפרעות לפעילויות העסקיות הקריטיות מהשפעת מקרי כשל או אסון.

א) הנהלת הארגון תפתח תוכנית המשך פעילות עסקית של הארגון במצבי משבר BCP (Business Continuity Planning) שתובא לאישור הדירקטוריון.

רח' קפלן 1, ירושלים 91036 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

ב) בקביעת המדיניות תבחין ההנהלה בין הצעדים המיידים אותם ניתן לבצע ובין הצעדים ארוכי הטווח.

ג) ה – BCP יתייחס לפחות להיבטים הבאים:

1. קביעת התהליכים העסקיים הקריטיים שיש להפעילם במצבי משבר וחירום, תוך זמן סביר, בהתייחס למכלול היחידות הארגוניות של הארגון ובהתאם לסיווג נכסי המידע, סעיף 2.3.1.
2. הקמת אתר חירום לצורך הפעלת מערך טכנולוגית המידע ופרק הזמן המרבי להפעלתו מרגע התרחשות האסון או ההכרזה על מצב חירום.
3. תוכנית התאוששות ממשבר – Disaster Recovery Plan (DRP).

ד) הנהלת הארגון תדון ותקבע את ההסדרים הקונקרטיים לביצוע המדיניות שנקבעה על ידי הדירקטוריון, לרבות:

1. מינוי צוות ניהולי של בעלי תפקידים רלוונטיים בראשות נושא משרה בכיר, שיהיה אמון על הכנת תוכניות היערכות להתמודדות עם מצבי משבר וחירום. צוות ניהולי זה יפעל לפקח על תהליכי יישום, הטמעה והדרכה בארגון ובגופים הקשורים לו (להלן צוות חירום ניהולי). צוות החירום הניהולי יקבע נהלי עבודה לשעת חירום, לרבות נהלים להמשך טיפול בתביעות.
2. מינוי "הנהלת גיבוי" אשר תחליף במידת הצורך, את ההנהלה הקיימת בעת משבר. מינוי "הנהלת גיבוי" יאושר בידי הדירקטוריון.
3. מינוי צוותי חירום במערכים השונים.
4. הקמת תשתיות טכנולוגיות ופיזיות לתמיכה בהמשכיות העסקית של הארגון ובניית תוכניות פעולה ליחידות הקריטיות.
5. הקמת אתר חירום לגיבוי מערך טכנולוגית המידע - גיבוי לנתונים, חומרה, תוכנה וידע. אתר החירום ימוקם במרחק סביר מהאתר הראשי, כך שתקטן ככל שניתן, ההסתברות לפגיעה בשני האתרים בעת ובעונה אחת.
6. בחינת היערכותם של ספקי השירותים העיקריים לארגונים, ובפרט ספקי מחשוב ומערכות מידע, ובחינת היערכות מוסדות פיננסיים באמצעותם מבוצעים תשלומים לעמיתים/מבוטחים.
7. הדרכה והכשרת העובדים, לרבות חברי ההנהלה וצוותי החירום, באשר למדיניות הארגון ובאשר לנוהלי העבודה בשעת משבר או חירום.
8. תרגול והפעלת סימולציות בנוגע למצבי חירום שונים.
9. קיום מעקב אחר ביצוע בפועל של תוכנית ההערכות ודיווח לדירקטוריון.

3.9. מיקור חוץ (Outsourcing)

מטרה: לקיים את רמת אבטחת המידע של הארגון, כפי שמוגדר במדיניות אבטחת המידע, כאשר האחריות לעיבוד, אחסון ותחזוקת המידע הועברה לארגון אחר.

א) ארגון רשאי לבצע פעילויות של ניהול, עיבוד, אחסון או פיתוח של המידע שברשותו על ידי גורמי צד ג' שאינם עובדי הארגון. בנוסף, הארגון רשאי להשתמש בשירותי מיקור חוץ של שירותי טלפוניה ומוקד שירות לקוחות (כולל IVR). עם זאת, אין בהוראת סעיף זה בכדי לגרוע מאחריותו של הארגון לכל פעולה המבוצעת מטעמו על ידי גורמים חיצוניים.

ב) על הנהלת הארגון לנסח מדיניות למיקור חוץ, המנחה האם וכיצד לבצע הוצאה של הפעילויות השונות לגורם חיצוני. בעת ניסוח המדיניות יילקחו בחשבון הסיכונים השונים אליהם עלול להיחשף הארגון בעת הוצאת הפעילות השונות לגורמי חיצוניים, בהתייחס לסעיף 2.3.1. באחריות דירקטוריון הארגון לדון ולאשר את מדיניות מיקור החוץ.

ג) הנהלת הארגון תקיים תכנית לניהול סיכוני מיקור חוץ. תכנית זו תיושם בעת התקשרות עם גורם מיקור חוץ חדש. כמו כן תיושם באופן שוטף לבקרה ומעקב אחר גורמי מיקור החוץ הקיימים.

רח' קפלן 1, ירושלים 91036 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

ד) על הנהלת הארגון ליישם כלי בקרה שיוודאו כי פעילות מיקור החוץ לא תפגע בשירות אותו מקבלים לקוחות הארגון. כמו כן, לא תפגע ביכולת הממונה על שוק ההון, ביטוח וחסכון והמפקח על הביטוח (להלן – "הממונה") לפקח על פעילות הארגון.

ה) על הנהלת הארגון להגדיר קריטריונים מקדמיים שיוודאו את יכולת ספק מיקור החוץ לעמוד בהתחייבויותיו הן בהיבט המקצועי והן בהיבט חוסנו הכלכלי של הספק.

ו) בעת הספקה של שירותי מיקור חוץ מהותיים, על הנהלת הארגון בשיתוף ספק שירותי מיקור החוץ להגדיר תוכנית להמשך הספקת שירותי מיקור החוץ בעת אסון (הן אסון בחצרי הארגון והן אסון בחצרי ספק שירותי מיקור החוץ).

ז) על הנהלת הארגון לוודא כי ספק שירותי מיקור החוץ שומר על עקרונות אבטחת מידע נאותים על מנת להגן על נכסי המידע של הארגון ושל לקוחות הארגון מפני דליפה, שינוי או מחיקה. על מנת לוודא כי מחויבות זו נשמרת יבצע הארגון ביקורות שוטפות וביקורות פתע על פעילות הספק.

ח) בעת אספקה של שירותי תחזוקה מרחוק (של מידע, תוכנה או ציוד תקשורת) על ידי גורמי מיקור חוץ, יישם הארגון את הבקרות הבאות:

1. פתיחה של הרשאות גישה למערכות מרחוק אך ורק בתיאום מראש.
2. מעקב בעזרת כלי ניטור אחר הפעולות שהתבצעו.
3. הגבלת ספק מיקור החוץ לגישה למידע לפי הצורך בלבד.
4. ספק מיקור החוץ יקבל אישור פוזיטיבי להתחברות, לפני תחילת עבודתו, וזאת לפי הוראות סעיף 3.4.4.
5. צמצום חשיפת ספק מיקור החוץ עד למינימום ההכרחי, ובמידת היכולת חסימה מלאה, למידע אודות לקוחות במערכות תפעוליות (Production).

ט) הסכם התקשרות עם ספק שירותי מיקור חוץ יתבצע בכתב. במיקור חוץ למערכת מרכזית יתייחס ההסכם הכתוב לפחות לנושאים הבאים:

1. הגדרת תחומי אחריות של כל אחד מהצדדים להסכם לרבות קבלני משנה.
2. הסכם רמת שירות (Service Level Agreement).
3. חובת הסודיות, אבטחת מידע ומצבי חירום.
4. הסדרים להפסקת ההסכם וליישוב מחלוקות.
5. הסכמת הספק נותן השירותים לביצוע ביקורות בחצרו מטעם הארגון.

3.10. נתיב בקרה (Audit Trail)

מטרה: לגלות פעילויות לא מורשות ולזהות את מקורן.

א) במערכות קיימות - הארגון יקיים נתיב בקרה לניטור ומעקב אחר ביצוע פעולות ושאילתות במערכות המוגדרות בסיכון גבוה, הן מתוך הארגון והן מחוצה לו.

ב) במערכות חדשות מה – 01/01/2007 - יש להחיל מנגנון נתיב בקרה על כל המערכות.

ג) תכולת נתיב הבקרה תיקבע בהתאם לרמת רגישות המערכת כפי שנקבעה בסעיף 2.3.2., על ה - Log להכיל את הנתונים הרלוונטיים, כך שיתאפשר לגלות ניסיונות גישה ופעולות לא מורשות ולזהות את מקורן. נתיב הבקרה יכלול מידע לפחות על ניסיונות של מורשים ולא מורשים, מוצלחים ולא מוצלחים, מהות הפעולה, מקור הגישה וזמן הגישה.
לגבי מערכות שאינן בעלות סיכון גבוה, תכולת נתיב הבקרה, תקבע לפי שיקול הארגון.

ד) פרק הזמן לשמירת קבצי התיעוד ייקבע בהתאם לרגישות המערכת כפי שנקבעה בסעיף 2.3.2.

ה) כל ניסיון גישה כושל וחריג למערכת ינוטר ויתועד במנגנון אירועים.

ו) הארגון יידע את עובדיו ולקוחותיו בדבר ביצוע רישום פעילויותיהם בקובץ לוג.

רח' קפלן 1, ירושלים 91036 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

ז) על שעון מנגנון הניטור להיות מסונכרן עם מקור שעון מדויק לצורך דיוק התיעוד.

ח) קבצי ה – Log יאובטחו בפני מחיקה, שינוי או קריאה בלתי מורשים.

4. נושאים מיוחדים לטיפול

4.1. סוכנים וסוכנויות ביטוח

מטרה: למנוע אפשרות של גישה לא מורשית לרשת הארגון דרך מחשבי סוכנויות הביטוח (כולל עמדות סוכנים מחוץ לסוכנויות ביטוח).

רקע:

מחשבי סוכנים וסוכנויות ביטוח אינם מאובטחים באופן המאפשר לוודא כי רק גורמים מורשים נגישים למידע רגיש במערכות המידע של הארגון. בקטגוריה זו נכללת כל עמדה המכילה קישוריות לרשת הארגון, כולל עמדות בבנקים או 'קיוסקים' (למשל עמדה מקושרת בסוכנות נסיעות, דואר וכדומה). לפיכך:

א) לסוכנים לא תותר גישה ישירה למערכות מידע ברשת הפנימית (קישור ישיר ל – LAN) של הארגון, אלא דרך מערכת שער (Gateway) מאובטחת, הממוקמת באזור מפורז מחוץ לרשת הפנימית, שתיזום את ההתקשרות לרשת הפנימית בשם הסוכן.

ב) אם קיים צורך בחיבור הסוכנים למערכת מידע פנימית, הארגון יגדיר אופן גישה מאובטח בהתייחס לסעיף 2.3.2. במקרה כזה, בקרת הגישה תכלול אמצעי זיהוי חזקים, הצפנת התווך מקצה לקצה, הקפדה על מדיניות הרשאות נוקשה ויישום בקרות למניעה ואיתור של חריגות.

ג) כל העובדים בסוכנות ביטוח יזוהו באופן חד ערכי מול מערכות המידע של ארגונים (בהתאם לסעיף 3.4.2).

ד) הארגון יגדיר לכל סוכן או עובד בסוכנות הרשאות גישה למערכות השונות. הרשאות אלה יותאמו בהתאם לסטאטוס ההתקשרות הנוכחי עימו, לדוגמא, סוכן שהפסיק את פעילותו השוטפת מול הארגון, אך עדיין מקבל עמלות בגין פוליסות ישנות, הרשאות הגישה שלו יצומצמו.

ה) קישור הסוכנים יבוצע על תווך מוצפן בין שני הקצוות.

ו) שימוש בדואר אלקטרוני ייעשה בהתאם לסעיף 4.3.

ז) לא יותר שימוש בתוכנות השתלטות על מחשבי הסוכנים באופן המסכן מידע רגיש של ארגונים .

ח) לארגון לא תהיה גישה למערכות המידע וציוד התקשורת של סוכנים באופן שיאפשר לו לגשת לרשת של ארגון אחר ולמידע האגור בסוכנות.

ט) ארגונים יעגנו בהתקשרויות, כי סוכני הביטוח יפעלו לאבטחת המחשבים שלהם, על מנת למנוע פגיעה במערכות המידע של הארגון, וכן ינקטו אמצעים לצמצום הפגיעה משימוש באינטרנט ובקרות גישה.

י) הארגון ידרוש מהסוכנים הצהרה בדבר היותם מודעים לאחריותם על סיכוני אבטחת המידע , ועל אחריותם לצמצום סיכונים אלו.

יא) תאי הדואר (מסמכי נייר) לסוכנים הממוקמים בארגון יאובטחו באופן המונע גישה לתוכנן לגורמים לא מורשים.

4.2. קישור עובדים לאינטרנט

מטרה: למנוע חשיפת מידע רגיש אל מחוץ לארגון ולצמצם יכולת פריצה של גורמים לא מורשים אל רשת הארגון.

א) הנהלת הארגון תגדיר את השימושים המותרים לעובדים לקישור לאינטרנט.

רח' קפלן 1, ירושלים 91036 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

ב) לעובדים המקושרים למערכות פנימיות ברשת הארגון המכילות מידע בעל סיווג גבוה, לפי סעיף 2.3.1, וצריכים להיות מקושרים לאינטרנט, הקישור לאינטרנט יתאפשר באחד מן האופנים הבאים:

1. רשת ייעודית מנותקת לוגית או פיזית מסביבת העבודה הראשית – תתאפשר הורדת קבצים ברשת יעודית, תוך נקיטת אמצעי בקרה נאותים בלבד. הארגון יגדיר במסגרת מדיניות אבטחת המידע את סוגי הקבצים המורשים להורדה באופן קישור זה.

2. ממחשב שאינו מחובר לרשת (Stand Alone) – במקרה זה תתאפשר הורדת קבצים באופן מאובטח.

ג) הקישור לאינטרנט יאובטח בפני גישה בלתי מורשית מהאינטרנט, תוכנות זדוניות ושימוש בלתי תקין.

4.3. דואר אלקטרוני

מטרה: למנוע דליפת מידע מסווג אל מחוץ לארגון.

א) בכל מקרה של העברת מידע בעל סיווג גבוה בדואר אלקטרוני, יידרשו אמצעי הצפנה, שמירה על מהימנות נתונים, חתימה דיגיטלית וזיהוי אישי חד ערכי. לצורך כך, יש לעשות שימוש באמצעים מקובלים.

ב) הודעות דואר אלה יישמרו באופן מאובטח לצרכי תיעוד לתקופת זמן כפי שייקבע במדיניות אבטחת המידע.

4.4. מסחר ושירותים מקוונים

מטרה: למנוע חשיפת מידע הקשור בצנעת פרט לגורמים לא מורשים ולצמצם יכולת פריצה של גורמים לא מורשים אל רשת הארגון.

א) מידע בעל סיווג גבוה, לפי סעיף 2.3.1, המועבר במערכת למסחר ושירותים דרך תשתית תקשורת ציבורית (לדוגמא, דרך אתר הארגון באינטרנט) ודרך תקשורת טלפוניה יאובטח באופן המצמצם את הסיכון לחשיפתו.

1. בכל מקרה כזה, יידרשו אמצעי הצפנה, שמירה על מהימנות נתונים, זיהוי אישי חד ערכי ואמצעי מניעת התכחשות. יש לעשות שימוש באמצעים מקובלים.
2. התקשורת (Session) תהיה מאובטחת לכל אורך חייה. במידת הצורך, במהלך התקשורת (Session) תידרש הזדהות חוזרת גם לאחר הזדהות ראשונית.

ב) הארגון יישם מנגנוני אבטחה בכל הרמות (לרבות רמת אפליקציה) במערכת.

ג) לא תותר גישה ישירה מבחוץ (אתר הארגון) למערכות מידע ברשת הפנימית (קישור ישיר ל – LAN) של הארגון, אלא דרך מערכת שער (Gateway) מאובטחת, הממוקמת באזור מפורז מחוץ לרשת הפנימית Demilitarized Zone (DMZ), שתיזום את ההתקשרות לרשת הפנימית.

ד) בסיסי נתונים המכילים מידע רגיש, לפי סעיף 2.3.1, לא יהיו נגישים למשתמשים מהאינטרנט ולא ימוקמו ברשת המפורזת DMZ. הגישה לבסיסי הנתונים תתאפשר אך ורק דרך מחשבי הארגון המשמשים כמתווכים באופן מאובטח.

ה) יוגדרו הרשאות כך שכל משתמש יוכל לבצע אך ורק את הפעולות שהוגדרו לו כמותרות.

5. החלת ההוראה

5.1. תחולה

ההוראה תחול על כל הגופים המוסדיים בישראל, כהגדרתם בחוק שירותים פיננסיים (ביטוח), התשמ"א -1981 .

רח' קפלן 1, ירושלים 91036 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

5.2. תחילה

א) תחילת ההוראה מיום פרסומה;

ב) על הגופים עליהם חלה ההוראה, לפי סעיף 5.1, לעמוד בדרישות הוראה זו בתאריך 30/06/2007.

5.3. ביטול תוקף

הוראות חוזר ביטוח 2003/12 בטלות.

5.4. הוראות מעבר

על אף האמור בסעיף 5.2 (ב), עמידה בדרישת ההוראה של הסעיפים המפורטים להלן תהיה בתאריך 01/01/2009.

א) סעיף 3.2.1 סעיף קטן ג' בקרות גישה באזורים מאובטחים.

ב) סעיף 3.3.5 ניהול רשת, סעיף קטן ד': בקרות בזמן אמת עבור מערכות שהוטמעו לפני 01/01/2006.

ג) סעיף 3.3.8 הפרדת סביבות.

ד) סעיף 3.4.2 אמצעי זיהוי, סעיף קטן ו'.

ה) סעיף 3.6.3 חתימה דיגיטלית (Digital Signature), סעיף קטן ג'.

ו) סעיף 3.6.4 מנגנוני מניעת הכחשה (Non-Repudiation), סעיף קטן ב'.

ז) סעיף 3.10. סעיף קטן א' נתיב בקרה (Audit Trail): עבור מערכות בעלות סיכון גבוה.

ח) סעיף 4.1 סוכנים וסוכנויות ביטוח, סעיפים קטנים א', ח', ט': רק לגבי התקשרויות ישנות (התקשרות שחודשה יראו אותה כהתקשרות חדשה).

ט) סעיף 4.2 קישור עובדים לאינטרנט, סעיף קטן ב'.

י) סעיף 4.3 דואר אלקטרוני, סעיף קטן א': יישום חתימה דיגיטלית.

ידין ענתבי
הממונה על שוק ההון, ביטוח וחסכון

נספח מונחים

פרק זה מפרש מונחים שונים בהם נעשה שימוש לאורך ההוראה. מונחים אלה מפורשים בהקשר של אבטחת מידע.

- ✓ **איום – Threat**: אפשרות פוטנציאלית לפגיעה בשלמות, זמינות או חשאיות המידע.
- ✓ **אמצעי זיהוי**: אמצעי המספק פרטים לגבי זהותו של אדם או מערכת בעת ניסיון כניסה ואישור ביצוע פעולות מטעמם למערכת מידע.
- ✓ **אמצעי זיהוי חזקים**: אמצעי זיהוי המתבסס על לפחות שניים מהפריטים הבאים:
  - Something You Are – תכונה פיזיולוגית ייחודית של המשתמש
  - Something You Have – פריט הנמצא ברשות המשתמש;
  - Something You Know – פריט מידע הידוע למשתמש;
- ✓ **גניבת זהות**: ניסיון לגניבת זהות או מידע אישי (פיננסי, רפואי או אחר) ע"י התחזות לגורם רשמי (למשל חברת ביטוח) המבקש מידע זה (למשל דרך דוא"ל, אתר אינטרנט, מענה טלפוני, מכתבים), אחת האפשרויות לגניבת זהות היא על ידי **Phishing**.
- ✓ **הערכת סיכונים**: תהליך של הערכת רמת הסיכון של המערכות השונות בארגון. התהליך ממפה את האיומים השונים הנובעים מהפעילות במערכות השונות. תוצר הערכת הסיכונים הנו מסמך המדרג את

רח' קפלן 1, ירושלים 91036 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

רמת הרגישות של המערכות השונות בארגון. מסקנות מסמך זה משמשות לגזירת פעילויות אבטחת המידע השונות.

- ✓ **הצפנה**: יישום של קריפטוגרפיה הממירה מידע גלוי (Clear Text) למידע מקודד (Cipher Text) באופן שיוכל להיות מפוענח ומובן אך ורק לגורמים מורשים.
- ✓ **זיהוי חד ערכי**: ערך ייחודי המזהה את מי שמתיימר להיות בעל אמצעי הזיהוי.
- ✓ **חומת אש – Firewall**: רכיב (תוכנה על שרת או רכיב חומרה) המבקר את התעבורה הנכנסת והיוצאת מרשת תקשורת על פי מדיניות אבטחה מוגדרת.
- ✓ **חשיפה – Vulnerability**: חולשה במערכת העלולה להוביל להתממשות איום.
- ✓ **חתימה דיגיטלית (Digital Signature)**: פריט מידע ייחודי הנוצר כפונקציה קריפטוגרפית של פריט מידע אחר, כך שהוא מזהה את התוכן בצורה מדויקת ומאפשר לזהות שינוי בו.
- ✓ **לוג – Log**: קובץ התיעוד של נתיב בקרה.
- ✓ **מדיניות אבטחת מידע**: מסמך המציג את תפיסת ההנהלה בנושא אבטחת המידע בארגון, מביע את מחויבותה לנושא ומגדיר את המבנה הארגוני וחלוקת הסמכויות בתחום. במסמך זה נקבעים עקרונות מנחים ליישום ולבקרה של אבטחת מידע, תוך יצירת תשתית ממנה ייגזרו נהלי עבודה בתחומים השונים.
- ✓ **מידע רגיש**: מידע שהארגון סיווג כבעל סיווג הדורש אמצעי אבטחת מידע נאותים. בכל מקרה מידע בעל סיווג גבוה, יוגדר כמידע רגיש, תכולת מידע זה נתונה לפרשנותו של הארגון, אלא אם צוין אחרת במפורש בהוראה זו.
- ✓ **מערכות איתור חדירה – Intrusion Detection System (IDS) או Intrusion Prevention System (IPS)**: רכיב (תוכנה על שרת או רכיב חומרה) האוסף ומנתח תעבורה העוברת ברשת. הרכיב מזהה ומתריע בפני ניסיונות תקיפה הבאות מחוץ לרשת הארגון או מתוכה.
- ✓ **מערכות מידע**: כלל הציוד הממוכן התומך בעיבוד מידע של הארגון הכולל בין השאר: שרתים, מחשבים נייחים וניידים, ציוד תקשורת, ציוד אבטחת מידע.
- ✓ **נתיב בקרה**: תיעוד פעולות המתבצעות במערכות מידע. קובץ התיעוד מקשר את הפעולה לנתונים נוספים כגון: שם מבצע הפעולה, המועד, הפעולה עצמה ועוד.
- ✓ **סינון תוכן – Content Filtering**: רכיב המונע מתכנים המוגדרים כאסורים על ידי הארגון להיות נגישים עבור עובדי הארגון.
- ✓ **סקר סיכונים**: סקר המאתר איומים/חשיפות הקשורות באבטחת מידע במערכות שונות והמעריך את רמת הסיכון שלהם לארגון.
- ✓ **קצה לקצה**: לאורך כל ההוראה, קצה הנו התחנה/שרת (למשל של משתמש) היוזם את השירות או תחנה/שרת (למשל מערכת מידע) המספקת את השירות. קצה לקצה מתייחס (לרוב בהקשר של הצפנה) לתווך התקשורת מקצה אחד, כולל הרשת הפנימית בארגון, ועד לתחנה/שרת הסופי בו יתבצע פענוח המידע.
- ✓ **קריפטוגרפיה**: שימוש בכלים מדעיים ואלגוריתמים לצורך הגנה על מידע. המטרות העיקריות של קריפטוגרפיה הינן שמירה על חשאיות ואמינות המידע, מתן פתרון למניעת הכחשה של פעולות ומתן מנגנון לאימות זהות משתמשים.
- ✓ **שימוש באמצעים מקובלים**: שימוש בטכנולוגיה לאבטחת מידע, שאומצו על ידי מומחי אבטחת המידע. אמצעים אלו יותאמו בהתאם להתפתחויות בנושא ולסיכונים הרלוונטיים באותה עת.
- ✓ **רשת פנימית - Local Area Network (LAN)**: קבוצת מחשבים המקושרים זה לזה בעזרת ציוד תקשורת ונגישים למשאבים (משתמשים ומחשבים אחרים) בתוך הארגון. במובן של הוראה זו, רשת פנימית הנה רשת המופרדת מרשתות ציבוריות ע"י אמצעים שונים כגון Firewall.
- ✓ **תווך תקשורת ציבורי**: תשתיות תקשורת המשרתות/משתפות מספר רב של צרכנים ואינן שייכות לאחד מהם. תשתיות אינטרנט מוגדרות כתווך תקשורת ציבורי.

רח' קפלן 1, ירושלים 91036 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il