כ״ח בתשרי התשע״ו
11 באוקטובר 2015

חוזר גופים מוסדיים 2014-117
סיווג: כללי <טיוטה>

ניהול סיכוני אבטחת מידע בגופים מוסדיים - טיוטה

בתוקף סמכותי לפי סעיף 2(ב) ו-42 לחוק הפיקוח על שירותים פיננסיים (ביטוח), התשמ״א-1981, סעיף 39(ב)(1) ו-40 לחוק הפיקוח על שירותים פיננסיים (קופות גמל), התשס״ה-2005 ותקנה 8(א)(20) לתקנות הפיקוח על שירותים פיננסיים (דירקטוריון וועדותיו), התשס״ז-2007 ולאחר התייעצות עם הוועדה המייעצת, להלן הוראותיי:

1. כללי

ניהול סיכוני אבטחת מידע הינו נדבך מהותי בניהול טכנולוגיות המידע לאור מרכזיות מערכות המידע בתהליכים העסקיים של הגופים המוסדיים ולאור הגידול בסיכונים להם חשופים גופים מוסדיים בתחום זה לרבות סיכוני סייבר.

על אף הגברת המודעות לסיכוני סייבר בעת האחרונה, חוזר זה מתייחס לסיכונים אלו כחלק בלתי נפרד מסיכוני אבטחת מידע.

מטרת חוזר זה להבטיח את שמירת זכויות העמיתים והמבוטחים על ידי שמירה על סודיות, שלמות וזמינות נכסי המידע, מערכות המידע והתהליכים העסקיים של הגוף המוסדי. החוזר מגדיר ומגביר את אחריות דירקטוריון והנהלת הגוף המוסדי לניהול תהליכי אבטחת מידע וסיכוני סייבר מתמשכים, להנחיה ופיקוח על יישום אבטחת המידע, ולמעורבות רציפה של גורמי אבטחת המידע במכלול פעילויות הגוף המוסדי.

החוזר מגדיר עקרונות לניהול סיכוני אבטחת מידע בגוף מוסדי ואת החובה של גופים מוסדיים לנהל את מכלול סיכוני הסייבר ואבטחת המידע, בהתבסס על עקרונות הגנת המידע. על הגופים המוסדיים לנהל את אבטחת המידע וסיכוני הסייבר באופן עדכני ושוטף, ועל בסיס עקרונות ממשל תאגידי נאותים הכוללים התייחסות לשיטות, לתהליכים ולבקרות.

לאור מרכזיות הגופים המוסדיים בשוק ההון הישראלי, ולאור הסיכון הגבוה בתחום אבטחת המידע, מצופה מגוף מוסדי לנהל סיכונים אלו ולאמץ סטנדרטים גבוהים בתחום זה.

רח׳ קפלן 1, ירושלים 9103002 ת.ד. 3100 טל׳ 02-5317111 פקס׳ 02-5695342
www.mof.gov.il

תוכן עניינים

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

2 . הגדרות

"**איום – Threat**" – אפשרות פוטנציאלית לפגיעה בשלמות, זמינות או חשאיות המידע.

"**אירוע אבטחת מידע**" – כל מקרה בו קיים חשד לפגיעה בסודיות, אמינות או זמינות במערכות הגוף המוסדי, מידע הגוף או כל אמצעי אחר אשר שייך לגוף המוסדי.

"**אמצעי זיהוי**" – אמצעי המספק פרטים לגבי זהותו של אדם או מערכת בעת ניסיון כניסה ואישור ביצוע פעולות מטעמם למערכת מידע.

"**גישה מרחוק – Remote Access**" – התחברות גורם (חיצוני או פנימי) מחוץ לרשת הארגון אל הרשת הפנימית של הארגון לצורך שימוש במשאבי הארגון.

"**גניבת זהות**" – גניבת מידע רגיש או ביצוע פעילות בלתי מורשה על ידי התחזות לגורם רשמי (למשל חברת ביטוח) המבקש מידע זה (למשל דרך דוא"ל, אתר אינטרנט, מענה טלפוני, מכתבים).

"**הזדהות חזקה – Strong Authentication**" – מבוססת על שימוש באמצעי זיהוי המתבסס על לפחות שניים מתוך הפריטים הבאים:

א. Something You Are – תכונה פיזיולוגית ייחודית של המשתמש.

ב. Something You Have – פריט הנמצא ברשות המשתמש.

ג. Something You Know – פריט מידע הידוע למשתמש.

"**הערכת סיכונים**" – תהליך של הערכת רמת הסיכון של כלל המידע, מערכות המידע והתהליכים העסקיים בגוף. התהליך ממפה את האיומים השונים הנובעים מהפעילות והתהליכים במערכות השונות ומתייחס בין היתר לעניינים אלו:

א. סביבת המערכת;

ב. ניתוח מידע שנאסף בנוגע לתקלות שאירעו במערכות הליבה ולהשפעתן;

ג. משתמשי המערכת הפנימיים והחיצוניים לגוף המוסדי;

ד. פעילות המערכת והשלכותיה על הפעילות העסקית בגוף המוסדי;

ה. רגישות המידע;

ו. מיקור חוץ;

ז. מידת התלות של הגוף המוסדי במערכת.

תוצר הערכת הסיכונים הנו מסמך המדרג את רמת הסיכון של המערכות והתהליכים השונים בארגון. מסקנות מסמך זה משמשות לגזירת פעילויות אבטחת המידע השונות.

"**הצפנה**" – המרת מידע גלוי (Clear Text) למידע מוצפן (Cipher Text) באופן שיוכל להיות מפוענח ומובן אך ורק לגורמים מורשים. "**טוקניזציה**" – תהליך המרת נתונים רגישים בערכים חלופיים שאינם רגישים ("טוקנים") אשר אין סכנה בחשיפתם. לרוב, תהליך זה מבוצע על ידי מערכת המחליפה את הערך המקורי בערך חלופי, ומאפשרת את שחזור הערך המקורי בעת הצורך, ובאופן מוגבל.

"**זיהוי חד ערכי**" – ערך ייחודי המזהה את מי שמתיימר להיות בעל אמצעי הזיהוי.

"**חשיפות אבטחת מידע – Vulnerability Scan**" – חולשה במערכת העלולה להוביל להתממשות איום.

"**יעד התאוששות** (RTO - Recovery Time Objective)" – יעד אותו קבע גוף מוסדי להחזרת פעילות עסקית ספציפית ומערכות התומכות בה לרמת שירות מוגדרת בפרק זמן מוגדר;

"**יעד שירות**" – רמת שירות לעמיתים או למבוטחים במצב חירום שעליה החליט דירקטוריון גוף מוסדי;

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

"**לוג - Log**" – קובץ התיעוד של נתיב בקרה, מכיל פרטים בנוגע לפעולות הממוחשבות המבוצעות בארגון."**מידע רגיש**" – כהגדרתו בחוק הגנת הפרטיות, תשמ"א-1981, וכל מידע אשר סווג על ידי הגוף כבעל סיווג הדורש אמצעי אבטחת מידע נאותים.

"**מיסוך נתונים**" – טכנולוגיה המבצעת הסתרה של נתונים או חלק מהם אשר הוגדרו סודיים, כך שבעת הצגת נתון, הוא מוחלף ברצף תווים אחר. שימוש בטכנולוגית מיסוך מאפשר לעבד נתונים כך שהצפייה בהם תהיה מוגבלת לגורמים מועטים בלבד.

"**מערכות ליבה**" – המערכות שהוגדרו על ידי גוף מוסדי כמערכות מרכזיות של הארגון ואושרו ככאלה על ידי הדירקטוריון, לרבות כל מערכת אשר יש לה השפעה ישירה על זכויות עמיתים ומבוטחים וכל מערכת שהמידע המנוהל בה עשוי להשפיע באופן מהותי על עסקי הגוף המוסדי ויציבותו, בין היתר, לרבות המערכות שלהלן וכל אחת מאלה:

א. מערכות ביטוח חיים;

ב. מערכות ביטוח כללי;

ג. מערכות ביטוח בריאות;

ד. מערכות תפעול זכויות עמיתים ומבוטחים;

ה. מערכות ההשקעות והפיננסים;

ו. מערכות מקבילות ו/או מערכות התומכות מהותית בפעילות המערכות המפורטות לעיל כגון: מערכת הכספים, מערכת אקטוארית, מערכת תביעות, מערכת ביטוח משנה וכד'.

"**מערכות מידע**" – כלל המערכות התומכות בפעילות העסקית בגוף מוסדי, לרבות ציוד ממוכן, תשתיות וטכנולוגיות התומכות בתפעולן, בין השאר: שרתים, מחשבים נייחים וניידים, ציוד תקשורת, ציוד אבטחת מידע.

"**נוזקה – Malware**" – תוכנה שמטרתה לחדור אל מערכות המחשוב לצורך שיבוש הפעילות התקינה או לצורך השגת מידע.

"**נכסי מידע**" – נכס מידע הוא מאגר נתונים, התקן, או רכיב של סביבה התומך בפעילויות הקשורות במידע (לרבות תשתיות). נכסי מידע כוללים, בדרך כלל, חומרה, תוכנה ומידע.

"**נתיב בקרה**" – תיעוד פעולות המתבצעות במערכות מידע. התיעוד מקשר את הפעולה לנתונים נוספים כגון: שם מבצע הפעולה, המועד, הפעולה עצמה ועוד לצורך זיהוי האלמנטים שהשתנו.

"**סיכון שורשי**" – סיכון מובנה. מאפיין את פעילות הגוף ללא תלות באמצעי אבטחת המידע המיושמים בגוף.

"**סיכון שיורי**" – סיכון שנותר לאחר יישום בקרות ואמצעי אבטחת מידע בגוף.

"**סקר סיכונים**" – תהליך שמטרתו זיהוי האיומים, הערכת הסיכון הנובע מהם (תוך התחשבות בסבירות התממשותם והנזק הפוטנציאלי כתוצאה מכך) וזיהוי הבקרות הנדרשות לצמצום סיכונים אלה.

"**קוד עוין**" – קוד המושתל על ידי משתמש זדוני ועשוי לגרום לביצוע פעולות לא רצויות, פגיעה במערכות הארגון וזליגת מידע רגיש לגורמים לא מורשים.

"**הצפנה מקצה לקצה**" – הצפנת תווך התקשורת/הנתונים מהתחנה/השרת (למשל: תחנת עבודה של משתמש) היוזמת את השירות אל התחנה/השרת (למשל: מערכת מידע) המספקת את השירות.

"**רשת פנימית – Local Area Network (LAN)**" – קבוצת מחשבים המקושרים זה לזה בעזרת ציוד תקשורת ונגישים למשאבים בתוך הארגון. במובן של הוראה זו, רשת פנימית הנה רשת המופרדת מרשתות ציבוריות.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

"**תווך תקשורת ציבורי – Public Network**" – תשתיות תקשורת המשרתות/משתפות מספר רב של צרכנים ואינן שייכות לאחד מהם. תשתיות אינטרנט מוגדרות כתווך תקשורת ציבורי.

"**תעודת הצפנה – SSL Certificate**" – תעודה הניתנת על ידי "רשות אמון" המאשרת את אמינות החיבור ומאמתת את מהימנות מקור החיבור.

"**DNS**" – שרות הממיר כתובות IP לכתובות מילוליות(URL) ובכך מקל את השימוש ברשת האינטרנט.

3 . ממשל תאגידי

א. תפקידים ותחומי אחריות

1) דירקטוריון

א) דירקטוריון גוף מוסדי יאשר מדיניות כאמור בסעיף 3ב1.) בתחום אבטחת המידע לכל הפחות אחת לשנה.

ב) הדירקטוריון ידון, לכל הפחות אחת לשנה, בתכנית אבטחת מידע מעודכנת והערכת סיכונים לרבות סייבר, הכוללת תכנית להפחתת סיכונים ופירוט השינויים במסגרת ניהול תחום אבטחת המידע.

ג) הדירקטוריון יאשר את כתב מינוי ועדת ההיגוי בתחום אבטחת המידע שבמסגרתו יוגדרו תפקידיה וסמכויותיה של הוועדה כאמור בסעיף 3 להלן.

ד) הדירקטוריון יאשר שימוש בשירותי מחשוב ענן, בהתאם לאמור בסעיף 5ז3.)א).

2) הנהלה

א) הנהלת גוף מוסדי תבטיח את ניהולו התקין של תחום אבטחת המידע בהתאם ליעדים, למדיניות ולצורכי הגוף המוסדי.

ב) הנהלת גוף מוסדי תקיים מסגרת נהלים כאמור בסעיף 3ב2.) ותאשר תכנית עבודה שנתית בתחום אבטחת המידע כאמור בסעיף 3ב3.).

ג) הנהלת גוף מוסדי תקיים מבנה ארגוני הולם בתחום אבטחת המידע ותגדיר את אחריות הגורמים העוסקים בתחום ואת הממשקים ביניהם, תוך שמירה על עקרונות של הפרדת תפקידים וסמכויות.

ד) הנהלת גוף מוסדי תקיים מנגנוני בקרה ופיקוח נאותים בתחום אבטחת המידע.

ה) הנהלת גוף מוסדי תקבע הוראות דיווח להנהלה ולגורמים אחרים בתחום אירועי אבטחת מידע.

ו) הנהלת גוף מוסדי תדון בסקר הערכת סיכונים ובתכנית להפחתתם, בהתאם לאמור בסעיף 4ב.,
וכן בהפחתת תדירות ביצוע סקר למערכת, בהתאם לאמור בסעיף 5ג1.)ד)(6).

ז) הנהלת גוף מוסדי תבחן אימוץ תקן ת"י ISO 27001 של מכון התקנים הישראלי.

3) ועדת היגוי בתחום אבטחת המידע

א) גוף מוסדי ימנה ועדת היגוי ובראשה יעמוד המנהל הכללי של הגוף המוסדי ובין חבריה יכללו מנהל מערכות המידע, מנהל הסיכונים ומנהל אבטחת המידע.

ב) הוועדה תסייע להנהלת גוף מוסדי לקבל החלטות ולבצע את תפקידיו בכל הקשור לניהול התקין של תחום אבטחת המידע מתוך ראיה אינטגרטיבית של התחום ברמה כלל ארגונית.

ג) הוועדה תבצע מעקב אחר יישום תכנית העבודה בתחום אבטחת מידע.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

ד) הוועדה תדווח להנהלת הגוף המוסדי אחת לרבעון על סטטוס ביצוע תכנית העבודה ולדירקטוריון הגוף המוסדי, לכל הפחות אחת לשנה, על פעילותה, מסקנותיה והמלצותיה בנושאים שהוסמכה לעסוק בהם.

ה) הועדה תתכנס לכל הפחות אחת לרבעון ותערוך פרוטוקולים של ישיבותיה.

ו) ועדת ההיגוי תדון בתוצאות הערכת סיכונים ובתכנית להפחתתם בהתאם לאמור בסעיף 4ב., בסיכונים אפשריים בהפעלת שימוש במערכות מבוססות ענן בהתאם לאמור בסעיף 5ז3.)א) ותתחקר, תפיק לקחים ותעביר המלצות להנהלה לגבי כל אירוע אבטחת מידע משמעותי בהתאם לסעיף 5ד1.)ט).

4) מנהל אבטחת מידע

א) מנהל אבטחת מידע יהיה בעל מומחיות וניסיון מוכחים בתפקיד ניהולי בתחום אבטחת מידע.

ב) מנהל אבטחת מידע לא ימלא כל תפקיד שעלול לפגוע ביכולתו לבצע כראוי את תפקידו כמנהל אבטחת מידע או להגבילה, ויהיה כפוף לאחד מחברי ההנהלה החברים בוועדת ההיגוי.

ג) חבר ההנהלה הממונה על מנהל אבטחת המידע יהיה אחראי על הפעילות המתבצעת בתחומי אבטחת המידע וכן על בקרת תכנית העבודה בנושא אבטחת מידע, בהתאם למדיניות אבטחת מידע של הגוף המוסדי.

ד) מנהל אבטחת מידע יישם את מדיניות אבטחת המידע בגוף המוסדי, ינחה את הגוף מוסדי בנושאי אבטחת מידע ויבצע פיקוח ובקרה בהתאם להוראות חוזר זה.

ה) למנהל אבטחת מידע יהיו המשאבים והמקורות הדרושים לביצוע תפקידו.

ב. מסגרת אבטחת מידע (FRAMEWORK)

1) מדיניות

גוף מוסדי יגדיר מדיניות אבטחת מידע הקובעת עקרונות מנחים של ההנהלה ליישום ובקרת אבטחת המידע בגוף. עקרונות אלו יתייחסו, בין היתר, למסגרת ארגונית (תחומי אחריות, ערוצי דיווח, פיקוח ובקרה), ליישום אבטחת המידע בהיבטי משאבי אנוש (מהימנות עובדים, הדרכה ובקרה), ליישום אבטחת מידע פיסית ולוגית בתהליכים, במערכות ובתשתיות הגוף ולכל הנושאים שיש להם השפעה רוחבית על יחידות גוף מוסדי.

2) נהלים

א) גוף מוסדי יקבע נהלים המגדירים את תהליכי אבטחת המידע בגוף תוך תיאום בין דרישות אבטחת המידע לבין תהליכי ניהול מידע ומערכות מידע.

ב) הנהלים ייגזרו ממדיניות אבטחת המידע שנקבעה על ידי הדירקטוריון, מההנחיות החיצוניות (כגון אסדרה או מחויבויות חוזיות), ומשיקולי ניהול סיכוני אבטחת המידע וסייבר של הגוף המוסדי.

ג) גוף מוסדי יגדיר נוהל לדרישות אבטחת מידע ביחס לסיכוני מיקור חוץ כאמור בסעיף 5ז1.)א).

ד) הנהלים יעברו תהליך בדיקה ועדכון בהתאם לצורך, עם שינוי משמעותי בסביבה הטכנולוגית או שינוי במתאר הסיכונים של הגוף המוסדי, ולכל הפחות אחת ל – 24 חודשים.

3) תכנית עבודה

תכנית עבודה תתייחס לאופי המידע, לתהליכים, לתשתיות ולמערכות הגוף המוסדי ותכלול, לכל הפחות, תכנית לניהול סיכוני אבטחת מידע וסייבר כאמור בסעיף 4, לרבות תכנית להפחתתם, תכנית להעלאת רמת מודעות העובדים כאמור בסעיף 5ה3.), תכנית לביצוע סקרים כאמור בסעיף 5ג1.)ד) ותכנית היערכות לאירועי אבטחת מידע וסייבר כאמור בסעיפים 5ד3.)ב) - 5ד3.)ד).

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

4. ניהול הסיכון

גוף מוסדי יגדיר תכנית לניהול סיכוני אבטחת מידע וסייבר, שתעסוק בסיכונים לתהליכים ולמידע ותתבצע בהתאם לסעיפים שלהלן:

א. הערכת סיכונים ועדכניותה

1) גוף מוסדי יעריך את סיכוני אבטחת המידע והסייבר במערכות המידע והממשקים אצלו, כדי לספק תמונת מצב עדכנית של מכלול הסיכונים שהוא מתמודד עמם.
2) הערכת הסיכונים תכלול, לכל הפחות, את השלבים הבאים:
   א) זיהוי תהליכים ונכסי מידע, החשופים לסיכוני אבטחת מידע וסייבר.
   ב) מיפוי סיכונים לתהליכים ולנכסי מידע כאמור.
   ג) הערכת רמת סיכונים שורשיים, תוך הערכת תוחלת הנזק שעלולה להיגרם כתוצאה מהתממשותם (לגוף וללקוחותיו) והסבירות להתממשותם.
   ד) מיפוי והערכת הבקרות למזעור סיכונים אלה, לרבות בחינה של מידת השפעת הבקרות עליהם.
   ה) הערכת סיכון שיורי (בהתאם להשפעת הבקרות שיושמו).
3) לצורך זיהוי והערכת הסיכונים, גוף מוסדי ישתמש, בין היתר, בממצאי ביקורות וסקרים, אירועי אבטחת מידע שהתרחשו בעבר וניתוח תרחישים לזיהוי אירועים פוטנציאליים של התממשות הסיכון.
4) הערכת הסיכונים תתייחס גם לסביבות פיתוח ובדיקות, העשויות להכיל מידע רגיש או לגלם חשיפות אבטחת מידע למערכות גוף מוסדי כולו.
5) הערכת הסיכונים תתייחס גם לסיכוני אבטחת מידע הנובעים מהסכמי מיקור חוץ.
6) הערכת הסיכונים תעבור תהליך בדיקה ועדכון בהתאם לצורך, עם שינוי משמעותי בתהליכים עסקיים, בסביבה הטכנולוגית או במתאר הסיכונים, ולכל הפחות אחת ל-24 חודשים.

ב. דיווח וניטור סיכונים

1) הערכת סיכונים תהווה בסיס לתכנית להפחתתם, תשולב בתכנית העבודה ותנחה את הנהלת גוף מוסדי בהקצאת משאבים להטמעת אמצעי אבטחת מידע.
2) תוצאות הערכת סיכונים ותכנית להפחתתם ידונו בוועדת היגוי, יאושרו בהנהלה ויוצגו לדירקטוריון. הצגה זו תכלול, לכל הפחות, פירוט סיכונים שיוריים, תכנית הפחתת סיכונים, ופירוט הסיכונים שהנהלת גוף מוסדי החליטה שלא להפחית לרמה מזערית.

ג. הגדרת נכסי מידע, זיהויים וסיווגם

1) גוף מוסדי ינהל רשימה עדכנית של כלל נכסי המידע הקיימים בו ויסווג אותם לפי רמת רגישותם והסיכון הכרוך בהם . הרשימה תעודכן לכל הפחות אחת לשנתיים.
2) גוף מוסדי יישם בקרות מתאימות לצמצום סיכונים של חשיפת מידע לגורמים בלתי מורשים, בהתאם לרמת רגישות המידע ולרמת הסיכון בחשיפתו. על הבקרות להתייחס, לפחות, למקרים הבאים:
   א) מידע הנשמר בציוד קצה.
   ב) מידע הנמצא בתהליך העברה בין אתרים או בין ארגונים.
   ג) מידע הנשמר באופן קבוע בשרתים, מסדי נתונים ובגיבויים.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

ד) חשיפת מידע כתוצאה מהעברה בלתי מבוקרת בתווך תקשורת ציבורי, לאתרי אינטרנט (כגון אתרי אחסון מידע) בלתי מאובטחים, למדיה חברתית שאינה מאובטחת או באמצעות דואר אלקטרוני בלתי מבוקר.

ה) חשיפת מידע כתוצאה מתהליך השמדת מידע בלתי מבוקר.

ו) חשיפת מידע כתוצאה משימוש במחשוב קצה שאינו בשליטה מלאה של גוף מוסדי (כגון מחשוב נייד פרטי של עובדים).

5 . אבטחת מידע של גוף מוסדי

א. אבטחת מערכות, תקשורת ותפעול

1) יישום אמצעי אבטחת מידע טכנולוגיים

א) גוף מוסדי ישתמש באמצעי אבטחת מידע טכנולוגיים, שמטרתם ליצור שכבות הגנה על מערכותיו ועל תהליכיו העסקיים, כדי למנוע את התממשות הסיכונים, לזהות את התממשות הסיכונים באופן מהיר, לעצור התפשטות התקפות על מערכות גוף מוסדי ולאפשר שחזור של המערכות וצמצום הנזק שנגרם כתוצאה מהתממשות סיכונים.

ב) גוף מוסדי יבצע הערכה שנתית של התאמת אמצעי האבטחה למכלול סיכוני אבטחת המידע שלו. הערכה זו תתחשב בהתפתחויות מתאר האיומים, באופי ההתקפות הנוכחי ובטכנולוגיות הקיימות במטרה להתמודד עם איומים אלה.

2) אבטחת רשת וגישה מרחוק

א) גוף מוסדי ישתמש באמצעי אבטחת מידע המתאימים לסיכוני גישה מרחוק לרשת הגוף, כגון אמצעי סינון תקשורת ותוכן, אמצעי ניטור אבטחת מידע ותהליכי בקרה.

ב) אמצעי אבטחת מידע יותאמו לסיכונים ייחודיים לשירותי רשת שונים, כגון דואר אלקטרוני, DNS, שירותי העברת קבצים, שירותי Web ועוד.

ג) גוף מוסדי יישם מידור בין החלקים השונים ברשת באמצעות חלוקה לוגית או פיסית של הרשת והגבלת אפשרות הקישור בין הרשתות השונות. רמת המידור תיקבע בהתאם לרגישות הנתונים המנוהלים במערכות.

ד) גוף מוסדי יגדיר אמצעי אבטחה מיוחדים כגון שימוש בהזדהות חזקה, הצפנה מקצה לקצה וניטור מוגבר בגישה מרחוק לרשת הגוף, על גבי תשתית תקשורת ציבורית או מנקודות קצה שאינן מאובטחות דיין.

ה) גוף מוסדי יישם מנגנונים שינטרו ויצמצמו את הסיכונים הנובעים מחיבור התקן זר או התקן בלתי-מאובטח לרשת הגוף.

3) קישוריות גוף מוסדי לרשת האינטרנט

א) גוף מוסדי יצמצם את רמת הגישה של העובדים לרשת האינטרנט למינימום הנדרש.

ב) קישור מערכות גוף מוסדי לרשת האינטרנט יבוצע תוך יישום אמצעי הפרדה מתאימים, שמטרתם למנוע הפעלה של קוד עוין, הכנסה בלתי מבוקרת של קבצים לרשת גוף מוסדי או יצירה של ערוצים חשאיים אל מחוץ לארגון.

ג) גוף מוסדי יבצע הפרדה מוחלטת של רשתות אלחוטיות מרשת הייצור שלו, לחילופין יישם מנגנונים מספקים לאבטחת רשתות אלחוטיות, לרבות הצפנה, הזדהות חזקה, מניעת התקפות על הרשת ומניעה של התחברות גורמים או ציודים בלתי מורשים לרשת האלחוטית.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

4) הוצאת נתונים אל מחוץ לארגון

א) גוף מוסדי יקבע את האופן שבו תאושר הוצאת נתונים אל מחוץ לארגון, בהתאם לרמת רגישותם.

ב) גוף מוסדי יגדיר את אופן אבטחת מידע ההכרחי ליישום בתהליך העברתו אל מחוץ למערכותיו (כגון: הצפנת נתונים, וידוא הגעת נתונים ליעדם וכדומה) בהתאם לרמת רגישות מידע.

5) הצפנה

א) גוף מוסדי יישם הצפנה להגנה על חיסיון מידע רגיש בתווך התקשורת אל מחוץ למערכותיו.

ב) גוף מוסדי יישם טכניקות הצפנה מוכרות שהוכחו כיעילות, ויתקף את האפקטיביות של אלה באופן תקופתי.

ג) גוף מוסדי יגדיר נהלים מתאימים ליצירה, עדכון, חידוש, התקנה וביטול של מפתחות הצפנה.

6) אבטחת מערכות ועדכונן

א) גוף מוסדי ישמור רשימה עדכנית של תשתיות ומערכות מידע, ויגדיר תהליכים לשמירת עדכניות רישום זה.

ב) גוף מוסדי יגדיר תהליכי עדכון מבוקרים למערכות ולתשתיות, תוך התייחסות למקוריות קבצי העדכון, בדיקת עדכונים בטרם יישומם, ושמירה על יציבות מערכות בתהליך העדכון.

ג) גוף מוסדי יתייחס לסיכונים הנובעים מחוסר עדכניות או היעדר תמיכה במערכות.

ד) גוף מוסדי יישם עדכוני אבטחת מידע שוטפים למערכות באופן תקופתי.

ה) גוף מוסדי יעקוב באופן תדיר אחר פרסום עדכוני אבטחת מידע למערכותיו, ויישם עדכונים קריטיים בהקדם האפשרי, בהתייחס לרמת החשיפה של מערכותיו לסיכוני אבטחת מידע הקשורים לעדכונים אלה.

7) אבטחת מערכות קצה

א) גוף מוסדי יישם אמצעי הגנה על מערכות קצה, תוך התחשבות בסיכוני הפעלת קוד עוין וסיכוני חדירה למערכות, תוך ניצול התקנים המחוברים למערכות קצה.

ב) גוף מוסדי יישם הצפנת נתונים רגישים במערכות קצה ניידות, במטרה למזער את הסיכון של חשיפת נתונים רגישים (כגון: מחשבים ניידים, טאבלטים, התקני אחסון ניידים וטלפונים ניידים).

ג) גוף מוסדי ישתמש במערכות בקרה, שמטרתן צמצום סיכון של זליגת נתונים רגישים ממערכות קצה או הגבלת היכולת לשמור מידע רגיש על מערכות קצה.

8) מניעת קוד עוין

א) גוף מוסדי יטמיע אמצעי אבטחה, למניעת חדירה והתפשטות קוד עוין במערכותיו, שיכללו מספר שכבות אבטחה כגון: סינון תקשורת וקבצים נכנסים, סריקת מערכות קבצים, הגנה בזמן אמת על שרתים או תחנות קצה, ומערכות ניטור ומניעה ייעודיות.

ב) גוף מוסדי יעדכן בתדירות גבוהה את אמצעי האבטחה האמורים לעיל, ויגדיר תהליכים לווידוא עדכניות אמצעי האבטחה כאמור (כגון: קבלת התרעות על כשל בעדכון קבצי חתימות).

ג) בעת חיבור אמצעי מדיה למערכות מידע יעשה שימוש במנגנוני הגנה אפקטיביים המונעים חדירת קוד עוין, כגון שימוש במערכות "הלבנת קבצים".

9) אבטחת מידע בתהליכי רכש ופיתוח

א) גוף מוסדי יגדיר דרישות אבטחת מידע בכל תהליך רכש או פיתוח של מערכות חדשות, ובעת שדרוג מהותי של מערכות מידע קיימות.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

ב) שילוב אבטחת מידע בתהליכי פיתוח ותחזוקה יכלול לכל הפחות, את השלבים הבאים:

(1) אפיון מערכת: אפיון פרמטרים של אבטחת מידע בעת תכנון מערכת, כגון סיסמאות, הרשאות, הצפנה, נפח וטיפול בזיכרון וכדומה.

(2) פיתוח מערכת: מימוש דרישות אבטחת מידע המופיעות באפיון מערכת.

(3) בדיקת מערכת: בדיקות במהלך פיתוח ובדיקות קבלה, תוך יישום היבטי אבטחת מידע ולרבות ביצוע סקר אבטחת מידע כאמור בסעיף 5ג. שלהלן.

(4) קליטת מערכת: קבלה והתקנה מאובטחת ומאושרת של המערכת על ידי גורמים מוסמכים לכך, תוך וידוא יישום דרישות אבטחת המידע.

(5) שינויים במערכת: מנהל אבטחת מידע יקבל דיווח טרם ביצוע שינוי במערכות המידע, ויקבע את רמת המעורבות הנדרשת בהתאם לאופי השינוי, לרגישות נתונים ולהשפעה אפשרית של השינוי על סיכונים וחשיפות אבטחת המידע של המערכת.

ג) אבטחת מידע תוטמע בכל רכיבי המערכת, לרבות: תשתיות, אפליקציה, וברמת הלוגיקה העסקית המיושמת במערכת.

ד) בדיקות הקבלה יבוצעו בטרם הטמעת מערכות בגוף, על ידי גורם בלתי תלוי שאינו מעורב בפיתוח והטמעת המערכות.

ה) בדיקות הקבלה יכללו, לכל הפחות, את הנדרש בעת ביצוע סקר אבטחת מידע, בהתאם לסעיפים 5ג.1)ד)(1) ו-5ג.1)ד)(2).

ו) כחלק מן התקשרות לפיתוח מערכת מידע על ידי גורם חיצוני, גוף מוסדי יבטיח כי קוד המקור עבר בדיקה נגד פרצות אבטחת מידע ואי קיום קוד זדוני.

10) הפרדה בין סביבות ואבטחתן

א) סביבת יצור תופרד מסביבות אחרות, כגון פיתוח ובדיקות.

ב) הרשאות משתמשים לסביבות ייצור תנוהלנה בנפרד מההרשאות לסביבות האחרות.

ג) סביבות פיתוח ובדיקות לא יכילו נתונים אמיתיים, אלא אם אמצעי אבטחת המידע המיושמים בסביבות אלו זהים לאלה המיושמים בסביבת הייצור.

ד) העברת נתונים מסביבת ייצור לסביבה אחרת תתבצע באישור מנהל אבטחת מידע.

ה) העברת מערכות ונתונים מסביבות פיתוח ובדיקות לסביבת ייצור תיערך בצורה מבוקרת, בהתאם לנהלים, כדי למנוע פגיעה בנתונים בסביבת הייצור.

ב. אבטחה פיסית וסביבתית

1) אזורים מאובטחים

א) בקרות אבטחה פיסיות יתייחסו למכלול הסיכונים הפיסיים והסביבתיים.

ב) גוף מוסדי יחלק את סביבת העבודה לאזורים מאובטחים לפי רמת רגישות המידע אליו ניתן לגשת מאזורים אלו.

ג) גוף מוסדי יישם מעגלים של בקרות גישה פיסית. מעגלים אלו יכללו בקרות מונעות, כגון דלתות נעולות ושערים אלקטרוניים ובקרות מגלות, כגון מצלמות ומערכות אזעקה. רמת הבקרה הנדרשת תותאם לרמת רגישות המידע אליו ניתן לגשת מאזורים אלה.

ד) גוף מוסדי יאפשר גישה לאזורי העבודה בהתאם לצורך, וימנע באופן מידי את הגישה לאזורים אלה כאשר אין עוד צורך בגישה זו, לרבות בעת שינוי תפקיד או סיום ההעסקה.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

ה) על בקרת הגישה באזורים המוגדרים ברגישות גבוהה לכלול לפחות שער כניסה אחד הנפתח על ידי אמצעי זיהוי חזק, כגון אמצעי ביומטרי או כרטיס חכם.

ו) גופים מוסדיים, המעניקים שירותי קבלת קהל במשרדיהם, יפרידו בין האזור בו ניתנים שירותים אלו, לבין אזורי העבודה השוטפים בגוף. לא יתאפשר לגורם, שאינו מורשה, להסתובב במשרדי גוף מוסדי ללא פיקוח.

ז) אזורים ציבוריים המכילים מידע רגיש ימודרו בפני גישה של אנשים שאינם בעלי הרשאה למידע.

2) אבטחת ציוד וניירת

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

ב) ציוד המיועד להשמדה או תחזוקה או הנמסר אל גורם מחוץ לגוף לא יכיל מידע רגיש. בטרם הוצאה של מערכות מחשב מחוץ לגוף לצורך תחזוקה, תבוצע מחיקת נתונים באופן המונע אפשרות שחזור מידע.

ג) גוף מוסדי יבצע השמדה של ציוד רגיש (פיסי או דיגיטלי) שאין בו שימוש ויגדיר את אופן הטיפול והשמירה עד להשמדתם.

ג. סקרי אבטחת מידע

1) סקרי אבטחת מידע ומבחני חדירה

א) גוף מוסדי יישם כחלק מתכנית העבודה הרב-שנתית סקרי אבטחת מידע ומבחני חדירה המכסים את המערכות והתהליכים הארגוניים.

ב) הסקר והמבחנים יבחנו תאימות מערכות ותהליכים למדיניות ונהלי אבטחת המידע של הגוף, הן ברמת בדיקת קיום בקרות אבטחת מידע והתאמתן והן ברמת בדיקת אפקטיביות הבקרות.

ג) הסקר יכלול ממצאים והמלצות.

ד) תכנית העבודה לביצוע הסקרים והמבחנים תיישם לכל הפחות, את הנושאים הבאים:

(1) כיסוי של כל רמות האבטחה של התהליכים והמערכות, לרבות: הגנות פיסיות וסביבתיות, הגנות תשתיתיות הכוללות אחסון, מערכות הפעלה, רשתות, בסיסי נתונים, רכיבי Middleware וכדומה, הגנות אפליקטיביות, הגנות ברמת הלוגיקה העסקית המיושמת במערכת וכן התהליכים הסובבים את המערכת כגון ניהול משתמשים והרשאות, תהליכי גיבוי, ניטור וכדומה.

(2) ביצוע מבחני חדירה תקופתיים הכוללים: מבחן המדמה ניסיון תקיפה מרשתות חיצוניות (כגון רשת האינטרנט, חיבור לספקים או שותפים עסקיים), בדיקות הנדסה חברתית, התחזות ופישינג, לכל הפחות אחת לשנה.

(3) ביצוע סריקת חשיפות אבטחת מידע (Vulnerability Scan) תקופתית לכל הפחות אחת לרבעון. לזיהוי חשיפות אבטחת מידע טכנולוגיות במערכות הגוף. הסריקות תתייחסנה לחשיפות הנובעות מחיבור מערכות הגוף לרשתות חיצוניות ("סריקה חיצונית") ולחשיפות הנובעות מניסיונות תקיפה מתוך רשת הגוף ("סריקה פנימית").

(4) תדירות ביצוע סקרי אבטחת מידע תיקבע בהתאם למידת החשיפה של המערכת לאיומים, רגישות המידע המנוהל במערכת ושינויים שבוצעו במערכת או בסביבתה.

(5) תדירות ביצוע סקרים למערכות שיש אליהן גישה מרשת ציבורית או למערכות המנהלות מידע רגיש על לקוחות, לא תפחת מאחת ל-12 חודשים. תדירות ביצוע הסקרים עבור

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

מערכות שאין אליהן גישה מרשת ציבורית ושאינן מנהלות מידע רגיש, לא תפחת מאחת ל-24 חודשים.

(6) במקרים מיוחדים, ניתן להפחית את תדירות ביצוע סקר למערכת באמצעות קבלת אישור לכך מההנהלה, לאחר הנמקת הבקשה ופירוט הסיכונים והחשיפות הקיימים למערכת. התדירות לא תפחת מאחת ל- 36 חודשים.

(7) על אף האמור לעיל, טרם הטעמת שינוי משמעותי במערכת שהוערכה כבעלת סיכון גבוה, או בסביבתה הטכנולוגית, יבוצע סקר אבטחת מידע.

ה) סקרי אבטחת מידע ומבחני חדירה יבוצעו על ידי גורם מקצועי, עצמאי ובלתי תלוי שאינו מעורב בפיתוח והטמעת מערכות בגוף.

ו) גוף מוסדי יגדיר תכנית לביצוע סקרי אבטחת מידע אצל ספקי מיקור חוץ המאחסנים או מעבדים נתונים של הגוף המוסדי. רמת הכיסוי של סקרי אבטחת המידע תותאם לרגישות המידע ולרמת הסיכון, ותכלול בדיקות שמטרתן לוודא את עמידת הספק בדרישות אבטחת מידע ולזהות חשיפות אבטחת מידע. סקרי אבטחת המידע יבוצעו בתדירות המותאמת לרמת הסיכון ולקצב עדכון התהליכים ומערכות הספק, ולכל הפחות אחת ל-24 חודשים.

2) טיפול בממצאי סקרי אבטחת מידע ומבחני חדירה

א) גוף מוסדי יגדיר תהליך שוטף לטיפול בחשיפות אבטחת מידע המתגלות במהלך סקרים ומבחנים, וליישום ההמלצות לטיפול בחשיפות אלו.

ב) תמצית ממצאי סקרים ומבחנים תוצג בוועדת ההיגוי. במקרים בהם חשיפות לא טופלו במהלך שלושה חודשים מעת ביצוע הסקר, מנהל אבטחת המידע יציג את הסיבות לאי הטיפול בחשיפות אלו, ואת משמעויותיהן להערכת סיכוני אבטחת המידע של הגוף.

ד. הגנת מידע וסייבר, ניטור ובקרה

1) ניטור ובקרת מערכות מידע

א) גוף מוסדי יישם נתיב בקרה וניטור של פעולות המתבצעות בנכסי המידע כדי לאפשר להתחקות אחר פירוט הרישום לצורך ביקורת, זיהוי של פעילות בלתי מורשה, תחקור לאחר מעשה ומניעת התכחשות.

ב) נתיב הבקרה יתייחס לפעולות ושינויים המבוצעים במערכות וכן לשאילתות וגישה לנתונים. יתועדו גם ניסיונות לביצוע פעולות (לרבות ניסיונות חיבור למערכות, שאילתות ועדכוני נתונים) שלא צלחו בשל תקלה או בשל מחסור בהרשאות.

ג) נתיב הבקרה יישום בכל המערכות המנהלות מידע רגיש וכן במערכות שרמת החשיפה שלהן לביצוע פעילות בלתי מורשה הינה גבוהה, בהתאם להערכת הסיכונים של הגוף.

ד) נתיב בקרה יכלול מידע על מועד ביצוע הפעולה, מקור הפעולה, הגורם שביצע או ניסה לבצעה ועל מי בוצעה הפעולה. במערכות ליבה - לרבות ערך טרום ביצוע הפעולה ולאחריה.

ה) פרק הזמן לשמירת נתיב בקרה יתאים למטרות נתיב הבקרה, ובכל מקרה לא יפחת מחצי שנה, ובמקרה של פעילות המבוצעת על ידי לקוחות לא יפחת משנתיים.

ו) נתיב הבקרה יהיה מוגן מפני מחיקה או שינוי בלתי מורשה.

ז) גוף מוסדי ישתמש במערכות ותהליכים שיזהו ויתריעו על פעילות המוגדרת אסורה או חשודה. ההתרעות יתוכננו בהתבסס על הגדרת תרחישי איום ובהתאם להערכת הסיכונים.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

ח) זיהוי והתרעה בגין אירועים חריגים כאמור בסעיף 5ד.1)ז) יתייחס לפעולות שמקורן מחוץ לגוף או בתוכו, תוך שימת דגש על מערכות תשתית, מערכות אפליקטיביות ומערכות המנוהלות או מאוחסנות מחוץ לגוף.

ט) מנהל אבטחת מידע יבחן אירועים חריגים. ועדת ההיגוי תתחקר כל אירוע משמעותי, תפיק ממנו לקחים ותעביר המלצותיה להנהלה בהתאם.

י) כלל תחקירי האירוע יועברו לדיון בהנהלת החברה, תוך פרק זמן סביר שלא יעלה על שלושה חודשים.

יא) גוף מוסדי יבחן מעת לעת את חוקי הניטור שהוגדרו, תקינותם ואיכות האירועים שמתקבלים, ולכל הפחות אחת לשנה.

2) איסוף מודיעין

א) גוף מוסדי יאסוף וינתח מידע רלוונטי, ממקורות פנימיים וחיצוניים לצורך יצירת תפיסה כוללת ועדכנית של איום הסייבר וחשיפת הגוף המוסדי למול האיום, כבסיס לקבלת החלטות מושכלת, תעדוף של דרכי פעולה, וקיום הגנה אפקטיבית בזמן אמת.

ב) גוף מוסדי יבחן עבודה ישירה מול המרכז הלאומי להתמודדות עם איומי סייבר (Cert-il) ולשיתוף הדדי של מידע קיברנטי אופרטיבי עמו.

3) מוכנות לאירועים

א) גוף מוסדי יפעל להבטחת יכולת מוכנות והתגוננות בפני התקפות חיצוניות.

ב) גוף מוסדי יגדיר תכנית היערכות לאירועי אבטחת מידע וסייבר, בהתאם להערכת סיכונים ולניתוח תרחישי קיצון (כגון: גישה לא מורשית לנכסי הגוף, זליגת מידע, גניבת זהות, נוזקות, הונאה, מניעת שירות וכדומה).

ג) התכנית תכלול, לכל הפחות, התייחסות לנושאים הבאים:

(1) גילוי וזיהוי אירוע.

(2) פירוט שלבי פעולה בעת זיהוי אירוע אבטחת מידע וסייבר (בידוד, חקירה, איסוף ראיות, הסקת מסקנות וכדומה).

(3) פירוט אופן תגובה ודרכי פעולה של הגוף, בהתייחס לתרחישים שונים.

(4) התקשרות עם גורמים פנימיים וחיצוניים, ובכללם לקוחות, בהתאם לתרחישים שונים.

(5) אופן הדיווח על אירועים, גורם מדווח, נמען הדיווח וזמן התגובה הסביר לדיווח.

ד) התכנית תעודכן על בסיס שנתי, בהתאם להערכת סיכונים מעודכנת, ותכלול התייחסות גם לעובדים חדשים ולמיקור חוץ.

ה) גוף מוסדי יגדיר תכנית התאוששות ויעדי התאוששות מאירוע אבטחת מידע וסייבר עד לתפקוד מלא בעת חזרה לשגרה, תוך התייחסות לתרחישי הייחוס ויעדי השירות בחירום שקבע לעצמו וליעדי השירות שהוגדרו כאמור בחוזר "ניהול המשכיות עסקית בגופים מוסדיים" 11-9-2013.

ו) גוף מוסדי יקיים, לכל הפחות, אחת לשנה תרגול שמטרתו להכין אותו להפעלת התוכניות שהוזכרו לעיל ולשיפורן בהתאם ללקחי התרגול.

ז) גוף מוסדי יקבע מנגנון דיווח על אירועי אבטחת מידע שיהיה נגיש לעובדים.

ח) מנהל אבטחת מידע ידווח לוועדת ההיגוי דוח המסכם את כלל ניסיונות התקיפה ואירועי אבטחת מידע שהתרחשו (לרבות כאלה שלא הובילו לפגיעה חמורה), אחת לרבעון.

ט) גוף מוסדי ידווח בהקדם האפשרי לממונה על שוק ההון, ביטוח וחיסכון על כל אירוע אבטחת מידע משמעותי שכתוצאה ממנו, באופן ישיר או עקיף:

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

(1) נפגעו או הושבתו מערכות ייצור המכילות מידע רגיש למשך של יותר מ-3 שעות.

(2) עולה החשש שמידע רגיש של לקוחות גוף מוסדי או עובדיו נחשף או דלף אל מחוץ לכותלי הגוף.

ה. אבטחת מידע במשאבי אנוש וגיוס עובדים

1) אבטחת מידע בתהליך גיוס העובדים

א) עבור משרות שיוגדרו כרגישות על ידי מנהל אבטחת המידע (כגון כאלה המאפשרות גישה למידע רגיש או שיש להן הרשאות העלולות לסכן את הגוף המוסדי), יבוצעו בדיקות לבחינת אמינות המועמדים.

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

ג) חוזה של גוף מוסדי עם חברות כוח אדם/השמה או עם חברות המספקות שירותי מיקור חוץ, יכלול התייחסות לסעיפים לעיל.

2) אבטחת מידע בסיום העסקת עובדים

א) לעובדים (לרבות עובדים במיקור חוץ) המסיימים את העסקתם ייחסמו הרשאות הגישה למידע ובסיום העסקה לא יישארו נכסי מידע של גוף מוסדי בידי העובד.

ב) גוף מוסדי יגדיר בקרות אבטחת מידע נוספות המתייחסות לתקופת הזמן שבין החלטה על סיום העסקה של עובד ובין ביטול הרשאות הגישה שלו, כגון מעקב מוגבר של מנהל אבטחת המידע אחר בקשות של העובד להרשאות או פעולות חריגות שמבוצעות על ידו.

3) מודעות אבטחת מידע והדרכה

א) גוף מוסדי יגדיר תכנית להעלאת רמת מודעות של עובדים לסיכוני אבטחת מידע וסייבר (בסעיף זה: "**התכנית**").

ב) התכנית תשולב במערך הדרכה של גוף מוסדי ותכלול התייחסות לאוכלוסיות העובדים השונות, לרבות מיקור חוץ.

ג) התכנית תגדיר הדרכות תקופתיות לעובדים לפי סוג התפקיד ובמהלך התפקיד ותתייחס להדרכה הנדרשת בעת קבלת עובדים או בעת מעבר לתפקיד חדש.

ד) התכנית תפעל להשגת המטרות הבאות:

(1) העלאת רמת הידע לגבי סיכוני אבטחת מידע וסייבר שגוף מוסדי חשוף אליהם והנגזרות מאופי התפקיד.

(2) העלאת המודעות הארגונית נדרשת כדי לזהות ולהגיב לסיכונים הנובעים מאופי תפקיד העובדים, כגון סיכוני "הנדסה חברתית".

(3) הטמעת נהלי אבטחת מידע של גוף מוסדי תוך הדרכת עובדים באשר לנהלים הרלוונטיים לאבטחת מידע במסגרת תפקידם.

ו. ניהול משתמשים והרשאות

1) ניהול משתמשים

א) גוף מוסדי יגדיר נהלים המתייחסים לתהליכים שונים במחזור חיים של ניהול חשבונות משתמש במערכות מידע של הגוף, החל מיצירת חשבון משתמש ואופן אישורו, ועד לאופן נעילת החשבון בתום העסקה.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

ב) תינתן התייחסות מיוחדת ליצירת חשבונות משתמשים עבור ספקים חיצוניים, עובדי מיקור חוץ, ועובדים זמניים, לרבות הגדרת אופן אישור חשבונות אלה, הגבלת השימוש בהם והמעקב אחר ביטולם בתום תקופת העסקה או תום פרויקט.

ג) חשבון משתמש ישויך לעובד מסוים, ותוגדר אחריותו של העובד על חשבון זה ועל הפעולות המבוצעות במערכות גוף מוסדי באמצעות חשבון זה.

ד) ככלל, יעשה שימוש בחשבונות משתמש אישיים. עם זאת, במקרים בהם יש צורך בקיום חשבונות משתמש שאינם אישיים, כגון כאלה המיועדים לשימוש על ידי תהליך ממוכן, יוגדרו תהליכים מיוחדים לשמירה על סודיות אמצעי הזדהות של החשבון, להגבלת השימוש בו, ככל הניתן, ויוגדר גורם האחראי על חשבון המשתמש.

ה) גוף מוסדי יגדיר תהליכי סקירה תקופתיים ומתועדים שמטרתם לוודא את הצורך בקיום חשבונות המשתמשים. תהליכי הסקירה לכלל החשבונות, יבוצעו לכל הפחות אחת לשנה.

ו) גוף מוסדי יגדיר את אופן נעילת חשבון משתמש במקרה של אי שימוש בחשבון במשך תקופה ממושכת, ואת תהליך אישור שחרור נעילה זו.

2) סיסמאות ואמצעי הזדהות

א) גוף מוסדי יגדיר אופן הזדהות למערכות מידע, באופן המתאים לרמת רגישות המידע המנוהל במערכת ולסיכונים השונים בתהליך ההזדהות.

ב) גוף מוסדי יגדיר נהלים המתייחסים למסירת אמצעי הזדהות, כגון מסירת אמצעי הזדהות באופן מאובטח למשתמש לאחר זיהויו, שמירה על סודיות הסיסמה והחלפת סיסמה ראשונית על ידי המשתמש.

ג) יש לאמת זהות משתמש כאשר נמסרת סיסמה ראשונית למערכת. המשתמש יחויב לשנותה בהתחברות הראשונה למערכת. תוקף הסיסמה הראשונית ייקבע למינימום אפשרי, בהתאם לאופי השימוש בחשבון ולא יעלה על 7 ימים.

ד) סיסמאות או אמצעי הזדהות אחרים לא יישמרו באופן גלוי (Clear Text) או באופן הניתן לשחזור ברשומות, בזיכרון או במאגרי מידע.

ה) גוף מוסדי יקבע את חוזק אמצעי ההזדהות, כגון הצורך בסיסמה חד-פעמית או מורכבות הסיסמה בהתאם להערכת הסיכונים. גוף מוסדי יגדיר אמצעי בקרה על מערך ההזדהות, כגון נעילת חשבון משתמש לאחר ניסיונות גישה כושלים או אי שימוש ממושך בחשבון, החלפה תקופתית של סיסמה ובקרה על מורכבותה.

3) ניהול הרשאות ובקרת גישה

א) גוף מוסדי יגדיר תהליכים מתועדים לשם מתן הרשאות גישה למערכות ושירותים, לרבות: אחריות גורמים עסקיים על אישור הרשאות למערכות עסקיות, התאמת הרשאות לצרכי תפקיד, רמת הסיכון מהרשאות, שינוי הרשאות בעת שינוי תפקיד וביטול הרשאות בעת סיום העסקה.

ב) גוף מוסדי יגדיר תהליכי סקירה תקופתיים, שמטרתם לוודא את הצורך בקיום הרשאות משתמשים. תהליכי הסקירה לכלל ההרשאות, יבוצעו לכל הפחות אחת לשנה.

ג) תהליכי סקירה תקופתיים של חשבונות ספקים חיצוניים, עובדי מיקור חוץ ועובדים זמניים יבוצעו בתדירות גבוהה יותר.

ז. מיקור חוץ (OUTSOURCING)

בהמשך לחוזר מיקור חוץ בגופים מוסדיים 2013-9-6, גוף מוסדי יישם את ההוראות הבאות הנוגעות לאבטחת מידע וסייבר בעת השימוש במיקור חוץ:

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

1) דרישות אבטחת מידע בהסכמי מיקור חוץ

א) גוף מוסדי יגדיר נוהל לדרישות אבטחת מידע ביחס לסיכוני מיקור חוץ. נוהל זה ייושם בעת התקשרות עם גורם מיקור חוץ חדש.

ב) במסגרת הסכם התקשרות עם קבלת שירותי מיקור חוץ:

(1) יאסר על נותן השירות להעביר לצד שלישי מידע שקיבל במסגרת ההתקשרות, או להשתמש במידע שאליו נחשף אגב ביצוע ההתקשרות, לכל מטרה אחרת שלא קשורה לביצוע ההתקשרות.

(2) תיבחן דרישה לעמידה בתקן ת"י ISO 27001 של מכון התקנים הישראלי.

2) שירות למערכות גוף מוסדי על ידי נותן שירות מיקור חוץ

אספקה של שירותי תחזוקה מרחוק (מידע, תוכנה או ציוד תקשורת) על ידי גורמי מיקור חוץ, תתבצע בתנאים הבאים:

א) נותן שירות מיקור חוץ יקבל אישור פוזיטיבי להתחברות, לפני תחילת עבודתו. מנהל אבטחת מידע יקבע מי בעל הסמכות לאשר התחברות מסוג זה.

ב) גישה מרחוק תתאפשר באמצעות משתמש ייעודי לכל נותן שירות מיקור חוץ ובתיאום מראש עם הגוף המוסדי לאופן ההתקשרות ותדירותה.

ג) גישה מרחוק תתאפשר לזמן מוגבל על פי סוג הפעילות אותה יבצע נותן שירות מיקור החוץ.

ד) גוף מוסדי יישם הזדהות חזקה לצורך כל גישה מרחוק של נותן שירות מיקור חוץ.

ה) גוף מוסדי ינטר כל פעילות שבוצעה בגישה מרחוק.

ו) חשיפת נותן שירות מיקור חוץ למידע אודות לקוחות תצומצם עד למינימום הכרחי, ובמידת האפשר תחסם במלואה.

3) שירותי מחשוב ענן

שימוש בשירותי מחשוב ענן כפוף להנחיות לעניין מיקור חוץ, ולרבות:

א) בטרם הפעלת שימוש במערכות מבוססות ענן, על גוף מוסדי לבצע הערכת סיכונים ייעודית, לדון בנושא סיכונים אפשריים בוועדת ההיגוי ולאשרם בדירקטוריון.

ב) גוף מוסדי לא יאחסן מידע או נתוני לקוחות בענן מחוץ לגבולות מדינת ישראל, אלא אם בדק ווידא שספק הענן מקיים את רמת ההגנה בהתאם לתקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס"א-2001 ולדירקטיבה על הגנת המידע במדינות האיחוד האירופי.

ג) במקרים בהם נתוני גוף מוסדי מאוחסנים במערכת שאינה לשימושו הבלעדי של גוף מוסדי (Multi-tenant), יעשה שימוש בטכנולוגיות כגון הצפנה, מיסוך נתונים או טוקניזציה, במטרה למנוע חשיפה של מידע רגיש של לקוחות או של גוף מוסדי לגורמים שאינם מורשים.

ד) גוף מוסדי יכלול בהסכם ההתקשרות עם ספק מחשוב ענן יכולת שליטה ובקרה שלו על הספק וכן אפשרות חד צדדית להפסקת השימוש בשירותי ספק מחשוב הענן תוך מחיקת המידע ממערכותיו והתחייבותו שלא ניתן לאחזר מידע זה במערכותיו.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

6. אבטחת ערוצי קשר עם לקוחות

א. אבטחת ערוצי תקשורת

1) גוף מוסדי ימפה את ערוצי התקשורת שלו עם לקוחותיו (בסעיף זה לרבות צדדים שלישיים).

2) גוף מוסדי יישם מערך של בקרות אבטחת מידע להגנה על ערוצי התקשורת, הכולל:

א) הצפנת ערוצי תקשורת למניעת האזנה או התערבות.

ב) אמצעי הגנה למזעור סיכונים הנובעים מרמת אבטחה לקויה של ציוד הקצה של לקוחות, כגון מחיקה של נתונים בתום הפעילות באתר, אי שמירה של נתונים במחשב הלקוח או יישום מנגנונים לזיהוי שינוי נתונים בתקשורת בין הלקוח ובין מערכות הגוף.

ג) ניטור ייעודי לזיהוי התקפות על ערוצי תקשורת עם לקוחות, כגון: ניסיונות התחזות, התקפות שונות על מנגנוני אימות זהות לקוח (אותנטיקציה), התקפות "הנדסה חברתית", התקפות על מנגנוני שחזור סיסמה וכדומה.

ד) אמצעים מקובלים למניעת התקפות על ערוצים אלה כגון ניחוש שמות משתמשים (user harvesting), ניחוש סיסמאות (Brute force), מניעת שירות באמצעות נעילת חשבונות וכדומה.

3) גוף מוסדי יוודא כי סיכונים שעלולים להיווצר בעת שינויים במערכות מקוונות או בתהליכי הזדהות של לקוחות לשירותים אלקטרוניים, יטופלו באופן מספק, טרם ביצוע השינוי.

ב. רישום מבוטחים/עמיתים לפעילות

1) וידוא זהות בתהליך הרישום

א) גוף מוסדי יוודא זהות לקוח בטרם השלמת רישום לשירותים אלקטרוניים.

ב) וידוא זהות לקוח יעשה באמצעות שימוש בערוץ תקשורת המבוסס על מידע מוקדם שיש לגוף על הלקוח (כגון: משלוח מכתב לכתובת הלקוח שנמסרה לגוף מבעוד מועד, משלוח הודעת SMS למספר טלפון שהלקוח מסר לגוף מבעוד מועד וכדומה).

ג) במקרים בהם לא קיים ערוץ תקשורת המבוסס על מידע מוקדם, ניתן לוודא זהות לקוח באמצעות אוסף פרטי מידע שיש לגוף על הלקוח, ושאינם ידועים לגורם אחר מלבד הלקוח ובלבד שייבחנו סיכונים רלוונטיים (כגון: התחזות) וייושמו מנגנוני אבטחה לצמצומם (כגון: ניטור שמטרתו לזהות ניסיונות התחזות). דוגמאות לפרטי מידע מסוג זה, יכולים להיות: תאריך הנפקת תעודת זהות, פרטים שהלקוח מילא בעבר בשאלון של הגוף המוסדי, פרטים מתוך אמצעי התשלום של הלקוח וכדומה.

2) הסכמה מפורשת של לקוחות בטרם רישום לפעילות

א) רישום לקוח לפעילות בערוצים מקוונים, תחייב קבלת הסכמה מפורשת של הלקוח בכתב באמצעות טופס ידני או טופס אלקטרוני שתתועד אצל הגוף המוסדי.

ב) תינתן לעמית הזכות לחזור בו מהסכמתו כאמור.

ג. הזדהות לקוחות לערוצי שירות

1) גוף מוסדי יגדיר אופן הזדהות לקוחות לערוצי שירות שונים, באופן המתאים לאופי הערוץ, לרמת הרגישות של המידע והפעולות המבוצעות באמצעות הערוץ, ולסיכונים השונים לתהליך ההזדהות, כגון גניבת זהות, האזנה לתווך התקשורת וכדומה.

2) גוף מוסדי ישתמש באמצעי הזדהות חזקים או אמצעי הזדהות שאינם קבועים, כגון סיסמאות חד פעמיות הנשלחות בהודעת SMS, לשם אימות זהות הלקוח (אותנטיקציה) תוך צמצום סיכון התחזות.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

3) גוף מוסדי יגדיר נהלים המתייחסים למסירת אמצעי הזדהות, כגון משלוח סיסמה ראשונית באמצעות דואר לכתובת לקוח, או באמצעות ערוץ אחר המאפשר מסירת אמצעי ההזדהות באופן ודאי ללקוח, וצמצום הסיכון לגניבת או העתקת אמצעי זה בדרך אל הלקוח.

4) גוף מוסדי יוודא כי לעובדיו אין גישה לאמצעי הזדהות של לקוחות, העלולה לאפשר ניצול לרעה של חשבון לקוח.

5) גוף מוסדי יגדיר נהלים לווידוא חוזק סיסמה, שמירה על סודיותה, החלפת סיסמה ראשונית על ידי המשתמש ותוקף הסיסמה הראשונית.

6) גוף מוסדי יגדיר נהלים המאפשרים ללקוח שחזור סיסמה באמצעים האמורים בסעיף 2.ג6).

ד. שליחת מידע באמצעים אלקטרוניים

1) גוף מוסדי ישלח מידע רגיש ללקוחות באמצעים אלקטרוניים, בכפוף לתנאים הבאים:

א) גוף מוסדי יצפין את המידע, כך שיימנע חשיפתו לגורם זר או לשיבושו.

ב) גוף מוסדי יוודא כי שלח את ההודעה ליעד.

ג) גוף מוסדי ישמור כל מידע תפעולי הנחוץ לצורך בקרה, ניהול ומעקב אחר קיום תנאי שליחת מידע באמצעים אלקטרוניים.

ד) גוף מוסדי יתעד את קבלת ההודעה על ידי הלקוח.

2) מידע שנשלח באמצעים אלקטרונים ולא נפתח במשך 30 ימים ממועד שליחתו, ישלח שנית בדואר רגיל.

3) גוף מוסדי יספק ללקוחותיו מידע והנחיות שיסייעו להם לנקוט באמצעי זהירות נדרשים לשמירה על פרטיות מידע, וינחה אותם כיצד לנהוג במקרה של חשד לאירוע אבטחת מידע.

ה. שיווק מוצרים באמצעים אלקטרוניים (ומסחר אלקטרוני)

שיווק מוצרים באמצעים אלקטרוניים יתבצע בכפוף לתנאים הבאים:

1) ערוץ תקשורת המשמש את תהליך הרכישה יוצפן באמצעות הצפנה חזקה בהתאם לתקנים המקובלים בשוק, שתבטיח את שלמות המידע וסודיותו, תוך שימוש בתעודת הצפנה (Certificate) חתומה על ידי גוף מוכר ואמין.

2) פרטי אמצעי התשלום של המבוטחים הנשמרים בשרתי החברה, ישמרו בהתאם לתקנים המקובלים בשוק.

3) גוף מוסדי יישם אמצעים למניעת הכחשה, וכן יבקר וינטר את אמצעי המסחר האלקטרוני במטרה למנוע התחזות ללקוח, הונאה או ניצול לרעה של תהליכי המכירה.

7 . אבטחת ערוצי קשר עם גורמים חיצוניים

א. אבטחת ערוצי קשר בין גופים מוסדיים למתווכים פיננסיים

1) למתווכים פיננסיים שאינם עובדי החברה לא תותר גישה ישירה אל מערכות המידע ברשת הפנימית (קישור ישיר ל LAN) של גוף מוסדי, אלא דרך מערכת שער מאובטחת (Secure Gateway), הממוקמת באזור מפורז מחוץ לרשת הפנימית שתיזום את ההתקשרות לרשת הפנימית בשם המתווך.

2) בכל חיבור של מתווכים למערכות תפעוליות של גוף מוסדי, על הגוף להבטיח בקרת גישה מאובטחת. בקרת הגישה תכלול הזדהות חזקה, הצפנת תווך התקשורת מקצה לקצה, חלוקת הרשאות על בסיס "הצורך לדעת" ויישום בקרות למניעה ואיתור של אירועים חריגים.

3) לכל עובד במשרדי המתווכים הפיננסיים יהיה זיהוי חד ערכי מול מערכות המידע של הגוף המוסדי.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

4) גוף המוסדי יגדיר לכל עובד במשרדי המתווכחים הפיננסיים הרשאות גישה למערכות השונות על פי צורך בלבד. הרשאות אלו יותאמו לסטטוס ההתקשרות הנוכחי עמו.
5) גוף מוסדי יבחן את הרשאות הגישה הניתנים לכל מתווך פיננסי מעת לעת, ולכל הפחות אחת לשנה.
6) כל גישה של מתווכחים פיננסיים למערכות בגוף מוסדי תבוצע על תווך תקשורת מוצפן מקצה לקצה.
7) לא יותר שימוש בתוכנות השתלטות על מחשבי מתווכים פיננסיים באופן העלול לגרום לחשיפת מידע רגיש בין גוף מוסדי למשנהו.
8) גוף מוסדי יגדיר כללים מתועדים בתחום אבטחת המידע אותם יישמו מתווכים פיננסיים. שיתוף פעולה בין גוף מוסדי לבין מתווך פיננסי יותנה בעמידה בכללים שהוגדרו.
9) תיבחן דרישה ממתווכים פיננסיים לעמוד בתקן ת"י ISO 27001 של מכון התקנים הישראלי.

ב. אבטחת ערוצי קשר בין גופים מוסדיים

בעת יצירת ערוצי העברת מידע בין גופים מוסדיים תיושמנה בקרות אבטחת מידע הכוללות הצפנת תווך התקשורת או הנתונים מקצה לקצה, אפשרות מעקב אחר הגעת הנתונים ליעדם והגבלת הגישה לנתונים על בסיס "הצורך לדעת".

8 . החלת ההוראה

א. תחולה

הוראות חוזר זה חלות על כל הגופים המוסדיים.

ב. תחילה

תחילתו של חוזר זה החל מ-1.4.2016

ג. ביטול תקפות

חוזר גופים מוסדיים 6-9-2006, "הוראה לניהול סיכוני אבטחת מידע של הגופים המוסדיים", בטל.

דורית סלינגר

הממונה על שוק ההון ביטוח וחסכון

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il