מדינת ישראל
משרד האוצר - אגף שוק ההון, ביטוח וחסכון

י״ב באלול התש״ע
22 באוגוסט 2010

חוזר גופים מוסדיים 4-9-2010
סיווג: כללי

ניהול טכנולוגיות מידע בגופים מוסדיים

בתוקף סמכותי לפי סעיף 2(ב) לחוק הפיקוח על שירותים פיננסיים (ביטוח), התשמ״א–1981, (להלן: ״**חוק הפיקוח**״), סעיף 39(ב) לחוק הפיקוח על שירותים פיננסיים (קופות גמל), התשס״ה–2005 ותקנה 8(20) לתקנות הפיקוח על שירותים פיננסיים (ביטוח) (דירקטוריון וועדותיו), התשס״ז-2007 (להלן: ״**תקנות הדירקטוריון וועדותיו**״) ולאחר התייעצות עם הועדה המייעצת, אני מורה כדלקמן:

1. **כללי**

הליבה העסקית והתפעולית של גופים מוסדיים העוסקים בתחומי הביטוח והפיננסים נתמכת בצורה מהותית על ידי מערכות טכנולוגיות שונות. לאור חשיבותן של אלו, על הגופים המוסדיים חלה חובה לנהל את תחום טכנולוגיות המידע על פי תקנים מקצועיים מקובלים ועל בסיס עקרונות ממשל תאגידי נאותים הכוללים התייחסות לשיטות, לתהליכים ולבקרות הנדרשים בניהול תחום טכנולוגיות המידע, וזאת במטרה להבטיח את ניהולן התקין ואת תמיכתן בפעילות העסקית על פי הוראות הדין ולהקפיד על שמירת זכויות העמיתים והמבוטחים.

להלן עיקרי הוראות החוזר לפי סדר הופעתם:

ממשל טכנולוגיות מידע - אחריותו הישירה של הגוף המוסדי בקביעת מדיניות ואסטרטגיה בתחום טכנולוגיות המידע, בביצוע בקרה ופיקוח שוטפים ובניהול תקין של תחום טכנולוגיות המידע.

הבטחת ציות - קיומם של תהליכים סדורים לעמידה בדרישות הציות החיצוניות והפנימיות בתחום טכנולוגיות המידע.

ניהול סיכוני טכנולוגיות המידע - קיומם של תהליכים סדורים לניהול סיכונים בתחום טכנולוגיות המידע.

בקרות מידע וניהול נתונים - הוראות לניהול ובקרת מידע לצורך הבטחת אמינות המידע, שלמותו, זמינותו והרלוונטיות שלו לתפקוד הגוף המוסדי.

רכש ופרויקטים - עקרונות ונוהלי עבודה מקובלים בביצוע רכש ופרויקטים מהותיים בתחום טכנולוגיות המידע.

ניהול שינויים - קיומה של מערכת הולמת לניהול שינויים במערכות המידע בגוף מוסדי, במטרה להבטיח כי השינויים האמורים מתועדים ונתונים לפיקוח ובקרה באופן שוטף.

רח׳ קפלן 1, ירושלים 91030 ת.ד. 3100 טל׳ 02-5317111 פקס׳ 02-5695342
www.mof.gov.il

מיקור חוץ (Outsourcing) - קביעת עקרונות ונוהלי עבודה להבטחת ניהולם התקין של תהליכים המבוצעים על ידי מיקור חוץ בתחום טכנולוגיות המידע, תוך מודעות לסיכונים ולחשיפות של הגוף ובמטרה להבטיח שליטה ובקרה על התהליכים והמידע המנוהלים במיקור חוץ.

2. **הגדרות**

"**ארכיטקטורת טכנולוגיות מידע**" - תיאור עקרונות היסוד לעיצוב רכיבי טכנולוגיות המידע של הפעילות העסקית ומערכת הקשרים ביניהם;

"**גוף מוסדי בעל היקף פעילות נמוך**" – כל אחד מאלה:

א. חברת ביטוח המורשית לעסוק בענף ביטוח יחיד; לעניין זה יראו עיסוק בענפי ביטוח השקעות של רוכשי דירות, מתן ערבויות, ביטוח אשראי וביטוח סיכוני סחר חוץ כמשמעותם בפסקאות (16), (20), (23) ו-(24) בסעיף 1א' בהודעת הפיקוח על עסקי ביטוח (ענפי ביטוח), התשמ"ה - 1985, בכולם או בחלקם, כעיסוק בענף ביטוח יחיד;

ב. חברת ביטוח שההון העצמי הנדרש ממנה הוא סכום ההון הראשוני לפי תקנה 2 לתקנות הפיקוח על עסקי ביטוח (הון עצמי מינימאלי הנדרש ממבטח), התשנ"ח-1998;

ג. חברה מנהלת שהיקף נכסי קופות הגמל שבניהולה אינו עולה על 5 מיליארד ש"ח, ולגבי חברה מנהלת של קופות גמל משלמות לקצבה – היקף נכסי קופות הגמל המשלמות לקצבה שבניהולה אינו עולה על 2 מיליארד ש"ח והיקף נכסי קופות הגמל האחרות שבניהולה, ככל שישנן, אינו עולה 5 מיליארד ש"ח;

"**טכנולוגיות מידע**" - החומרה, התוכנה, התקשורת והאמצעים האחרים המופעלים לקליטה, אחסון, עיבוד, תפעול, העברה ופלטי נתונים;

"**מיקור חוץ בתחום טכנולוגיות המידע**" - התקשרות בין גוף מוסדי לבין ספק, לפיה הספק מקבל על עצמו לספק שירותים או מוצרים הקשורים למערכות המידע בארגון, ביניהם פיתוח, תחזוקה ותפעול של מערכות מידע או תשתיות בגוף המוסדי, למעט רכישת שירותי כוח אדם המצויים בשליטתו המלאה של הגוף המוסדי;

"**מערכות ליבה**" - המערכות אשר הוגדרו על ידי הגוף המוסדי 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, לרבות כל אחת מאלה:

א. מערכות ביטוח חיים;

ב. מערכות ביטוח כללי;

ג. מערכות ביטוח בריאות;

ד. מערכות תפעול זכויות עמיתים ומבוטחים;

רח' קפלן 1, ירושלים 91030 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

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 הליבה העסקית בגוף מוסדי, לרבות התשתיות והטכנולוגיות התומכות בתפעולן;

"**סיכונים בתחום טכנולוגיות מידע**" - הסיכון הנובע משימוש או מהיעדר שימוש של גוף מוסדי בטכנולוגיות מידע או מהתלות של הגוף המוסדי בהן.

3. **<u>ממשל טכנולוגיות מידע</u>**

ממשל טכנולוגיות מידע עוסק באחריותם הישירה של האורגנים השונים בגוף המוסדי בקביעת אסטרטגיה ומדיניות בתחום טכנולוגיות המידע, בביצוע בקרה ופיקוח שוטפים ובניהול תקין של תחום טכנולוגיות המידע, במטרה להבטיח את תמיכתם בפעילות העסקית ואת תאימותם למדיניות וליעדים העסקיים של הגוף המוסדי.

א. **תפקיד הדירקטוריון**

לאור חשיבות נושא טכנולוגיות המידע והמורכבות המקצועית בתחום ולצורך ביצוע תפקידו בכל הקשור לתחום זה, על דירקטוריון של גוף מוסדי לקיים דיון בנושא טכנולוגיות המידע לכל הפחות אחת לחצי שנה, לבצע את הפעולות הבאות:

1) לאשר אסטרטגיה ומדיניות בתחום טכנולוגיות המידע ולאשר את תכנית העבודה השנתית והרב-שנתית בתחום;

2) להבטיח את קיומם של מנגנוני פיקוח ובקרה נאותים על פעילות הגוף המוסדי בתחום טכנולוגיות המידע[1], לקבוע יעדי בקרה (Control Objectives) ולבצע פיקוח ומעקב על שינויים מהותיים ופרויקטים מרכזיים בתחומי הליבה של הגוף המוסדי כדי להבטיח עמידתם ביעדי ביצוע ביחס למתוכנן ואת עמידתם במסגרת התקציבית ובלוחות הזמנים;

3) להבטיח את קיומם של מנגנוני אכיפה פנימיים על מנת להבטיח את עמידת הגוף המוסדי בדרישות הציות החיצוניות והפנימיות בתחום טכנולוגיות המידע;

4) לקבוע הוראות דיווח פרטניות לדירקטוריון בתחום טכנולוגיות המידע.

ב. **תפקיד הנהלת גוף מוסדי**

על הנהלת גוף מוסדי חלה החובה להבטיח את ניהולו התקין של תחום טכנולוגיות המידע באופן המבטיח שימוש יעיל, אפקטיבי והולם בטכנולוגיות המידע בגוף המוסדי התואם ליעדים, למדיניות ולצורכי הגוף המוסדי. במסגרת זו עליה לפעול לביצועם של לפחות כל אחד מאלה:

[1] מסגרת ה - COBIT הינה מסגרת בקרה מקובלת מומלצת לעניין קיום מנגנוני בקרה ופיקוח יעילים בתחום טכנולוגיות המידע.

רח' קפלן 1, ירושלים 91030 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

1) לגבש תכנית עבודה שנתית ותכנית עבודה רב-שנתית בתחום טכנולוגיות המידע ולפקח באופן שוטף אחר ביצוען;

2) להבטיח תאימות בין תכניות העבודה בתחום טכנולוגיות המידע לבין תכניות העבודה של היחידות העסקיות והתאמתן של תוכניות העבודה ליעדי הגוף המוסדי. במסגרת זו על הנהלת הגוף המוסדי להבטיח תאימות של המשאבים המוקצים לתחום טכנולוגיות המידע, לרבות התאמת התקציב השוטף, תקציבי ההצטיידות וההשקעות הכלליות בתחום זה, במטרה להבטיח תמיכה של מערכות המידע בתהליכים העסקיים בהתאם לאסטרטגיה וליעדי הגוף המוסדי;

3) לקיים מסגרת נהלים מתאימה בתחום ניהול טכנולוגיות המידע.

4) להבטיח תמיכה נאותה של תחום טכנולוגית המידע בצרכים העסקיים השוטפים והעתידיים של הגוף המוסדי;

5) לקיים מנגנוני בקרה ופיקוח נאותים בתחום טכנולוגיות המידע המבוססים, לפי העניין, על עקרונות ניהול סיכונים;

6) לקיים מנגנוני פיקוח ובקרה על ביצועי טכנולוגיות המידע, ולבחון את האפשרות לעשות שימוש במדדי ביצוע המותאמים ליעדים ולאסטרטגיה של הגוף המוסדי, לתוכניות העבודה ולנוהלי העבודה הפנים-ארגוניים;

7) לערוך מיפוי של נכסי טכנולוגיות המידע הקשורים למערכות הליבה בגוף המוסדי, ולעדכנו אחת לתקופה מוגדרת, לרבות: מאגרי נתונים, אפליקציות, ונכסים טכנולוגיים אחרים, כגון: מערכות הפעלה, חומרות, מולטימדיה, רשתות תקשורת, ציוד ותשתיות;

8) להגדיר את מסגרת הסמכויות של הגורמים העוסקים בתחום ואת אחריותם על כל אחד מנכסי טכנולוגיות המידע בגוף המוסדי, תוך כדי שמירה על עקרונות הפרדת תפקידים וסמכויות והבטחת התאמה של מערך ההרשאות לאמור;

9) לקיים מבנה ארגוני הולם בתחום טכנולוגיות המידע בארגון ולהגדיר את נוהלי התיאום והשיתוף בין המחלקות הפנימיות בארגון, את הממשקים ואת קשרי העבודה ביניהן, לרבות לעניין התהליכים העסקיים והבקרות הנדרשות והשתלבותם במבנה הארגוני, במטרה להבטיח מתן מענה מיטבי לצרכי היחידות העסקיות ולהבטיח את תמיכתן בהוראות הדין;

10) לקיים תהליך סדור לתעדוף דינאמי של המשימות המהותיות הקשורות לתחום טכנולוגיות המידע, על בסיס השינויים ביעדים העסקיים, בסביבה הרגולטורית וביחס לצורכי היחידות העסקיות ולהגדיר לוחות הזמנים לביצועם בשיתוף עם יחידת מערכות המידע;

11) לקיים תכניות הדרכה למשתמשים הכוללות התייחסות להטמעת מערכות חדשות לשימור הרמה המקצועית ולעדכון שוטף של משתמשי המערכות.

12) להבטיח קיומה של המשכיות הפעילות העסקית בכל הקשור למערכות המידע (BCP) בתחומים השונים ולתת מענה לתרחישים אפשריים.

רח' קפלן 1, ירושלים 91030 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

13) מינוי ועדת היגוי בתחום טכנולוגיית המידע

על גוף מוסדי שאינו בעל היקף פעילות נמוך למנות ועדת היגוי מקצועית בראשות המנהל הכללי של הגוף המוסדי שתעסוק בתחום טכנולוגיות המידע. בין חבריה הקבועים יכללו מנהל מערכות המידע והמשתמשים המרכזיים בטכנולוגיות המידע בגוף המוסדי (להלן – **ועדת ההיגוי**).

על הגוף המוסדי להגדיר בכתב מינוי, אשר יאושר על ידי הדירקטוריון, את תפקידיה וסמכויותיה של הוועדה, להגדיר את החברים בה ולקבוע את מועדי התכנסותה ובלבד שלא יפחתו מאחת לרבעון.

קבוצת חברות אשר הינן תחת אותו בעל שליטה, יכולה לקיים ועדת היגוי אחת לקבוצת החברות (להלן – **ועדת היגוי קבוצתית**) ובלבד שהגורמים המוסמכים לכך בכל גוף מוסדי בקבוצה, יאשרו את מינוי ועדת ההיגוי הקבוצתית כועדת ההיגוי של הגוף המוסדי.

מונתה ועדת היגוי קבוצתית, ניתן שיתקיימו דיונים משותפים הרלוונטיים לכל חברות הקבוצה ובלבד שבנוסף, יתקיימו דיונים בנושאים פרטניים הייחודיים לכל חברה בקבוצה, בנושאים שבהם נדרש גוף מוסדי בקבוצה לדון בועדת ההיגוי בהתאם להוראות חוזר זה.

לדיונים הפרטניים יוזמנו כל הגורמים אשר הוגדרו בחוזר זה ו/או גורמים אשר הוסמכו לכך מטעם הגוף המוסדי שבקבוצת החברות.

תפקיד הוועדה לסייע לגוף המוסדי בביצוע תפקידיו בכל הקשור לניהול התקין של תחום טכנולוגיות המידע בגוף המוסדי, לבצע מעקב אחר יישום תכנית העבודה בתחום, להבטיח קיומם של מנגנוני בקרה ופיקוח נאותים ולסייע לגוף המוסדי בקבלת ההחלטות בכל הקשור לנושא טכנולוגיות המידע מתוך ראיה אינטגרטיבית של התחום ברמת החברה.

על הוועדה לדווח לדירקטוריון, לכל הפחות אחת לחצי שנה, על פעילותה ועל מסקנותיה והמלצותיה בנושאים שהוסמכה לעסוק בהם ולערוך פרוטוקולים של ישיבותיה.

ג. **תפקיד מנהל מערכות המידע**

גוף מוסדי שאינו בעל היקף פעילות נמוך ימנה מנהל מערכות מידע בעל הכשרה מקצועית וניסיון מוכח בתפקיד ניהולי בתחום טכנולוגיות המידע.

על הדירקטוריון לאשר את המינוי כאמור.

מנהל מערכות המידע ישא באחריות על כל הפעילויות בתחום טכנולוגיות המידע בגוף מוסדי ויהיה במעמד חבר הנהלה או יהיה כפוף ישירות למנכ"ל.

מנהל טכנולוגיות המידע ינהל את נכסי טכנולוגיות המידע בגוף המוסדי ויפקח על התהליכים והפעילויות הכלולות במערכות המידע בגוף המוסדי. במסגרת זו עליו לבצע כל אחד מאלה:

1) בחינה והערכה של ההתפתחויות בתחום טכנולוגיות המידע הקשורות לפעילות העסקית של הגוף המוסדי;

2) ניהול, שליטה ובקרה על טכנולוגיות המידע במערכות הליבה בגוף המוסדי;

רח' קפלן 1, ירושלים 91030 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

3) ניהול יחידת טכנולוגיות המידע אשר אמורה לספק שירותי הקמה, תחזוקה ושימור של מערכות המידע התומכות בתהליך העסקי ופיקוח עליה ;

4) הבטחת רמה מקצועית נאותה לתמיכה בצרכי הגוף וביעדיו תוך יצירת רמת מיומנות מקצועיות נאותה ;

5) ניהול התמיכה הטכנולוגית במאגרי המידע של הגוף המוסדי ;

6) גיבוש מסגרת נהלים ותהליכי עבודה בתחום טכנולוגיות המידע ;

7) תמיכה בצורכי המשתמשים ובתשתיות הטכנולוגיות של הגוף המוסדי ועמידה ברמות שירות (SLA) וברמות תפעול (OLA) מוגדרות מול המשתמשים הפנימיים והחיצוניים לארגון ;

8) גיבוש מבנה ארכיטקטורת טכנולוגיות המידע בגוף המוסדי ברמת פירוט התואמת את צורכי הגוף המוסדי ויעדיו ולעדכנו באופן שוטף.

4. **<u>הבטחת ציות בתחום טכנולוגית מידע</u>**

במטרה להבטיח את עמידתו של גוף מוסדי בדרישות ציות חיצוניות שמקורן בגורמים שמחוץ לגוף לרבות הוראות רגולטוריות וכיוצא באלו וכן בדרישות ציות פנימיות שמקורן בנוהלי עבודה פנימיים והוראות גורמי הנהלה ופיקוח בתחום טכנולוגיות המידע, על הגוף המוסדי לפעול לביצוע כל אחד מאלה :

א. לקיים תהליך סדור לזיהוי ולניתוח של השפעת דרישות הציות החיצוניות והפנימיות על תחום טכנולוגיות המידע ולקבוע מהם האמצעים ההולמים את מתן המענה לדרישות אלה, לרבות הגדרת נהלים ומנגנוני אכיפה פנימיים להבטחת העמידה בדרישות הציות ;

ב. להגדיר גורם אחראי מקצועי ליישום הוראות הציות ולדיווח על ביצועם ;

ג. לערוך סקר ציות שמטרתו להבטיח תמיכת מערכות המידע בהוראות הציות החלות על הגוף המוסדי ולוודא קיומו של תהליך מחזורי לעדכון סקר הציות.

5. **<u>ניהול סיכוני טכנולוגיות המידע</u>**

על הגוף המוסדי לגבש מסגרת עבודה לניהול סיכונים בתחום טכנולוגיות מידע, להגדיר תכנית לניהול סיכוני טכנולוגיות מידע ולמנות גורם אחראי ליישום הוראות התוכנית ועדכונה.

א. תכנית ניהול סיכוני טכנולוגיות מידע תבטיח, לכל הפחות, כל אחד מאלה :

1) זיהוי הנכסים החשופים לסיכוני טכנולוגיות מידע על בסיס מיפוי נכסי טכנולוגיות המידע כאמור בסעיף 7.ב.3 לעיל ;

2) הערכת ההשפעה הפוטנציאלית של סיכוני טכנולוגיות המידע על הגוף המוסדי תוך הערכת היקף הנזק הפוטנציאלי וההסתברות להתרחשותם. על ההערכה לכלול, בין היתר, נסיבות או אירועים שונים בעלי פוטנציאל לגרימת נזק, לרבות כשלים, הונאות או מעילות הקשורות למערכות המידע ;

ההערכה תכלול התייחסות רחבה לכל הסיכונים הגלומים בכל אחד מתהליכי הליבה הנתמכים באמצעות מערך טכנולוגיות המידע, לרבות לעניינים אלו :

רח' קפלן 1, ירושלים 91030 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

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;

ה) רגישות המידע;

ו) מיקור חוץ;

ז) מידת התלות של הגוף המוסדי במערכת.

3) הערכת הבקרות הקיימות בגוף המוסדי המשפיעות על הסיכון הכולל שהגוף חשוף אליו וגיבוש המלצות לחיזוק הבקרות או לביצוע פעולות אחרות שמטרתן למתן או להפחית את הסיכון לרמות מקובלות.

ב. הערכת הסיכונים תכלול התייחסות לבקרות כלליות ולבקרות יישום פרטניות ביחס לכל תהליך ליבה, בהתאם לסוג הבקרה, כגון: בקרה מגלה, מונעת או מתקנת, בקרה ידנית או אוטומטית ובמידת הצורך - בקרה מפצה;

ג. גוף מוסדי יגבש תכנית פעולה על בסיס הערכת הסיכונים והבקרות לגבי הצעדים שיש לנקוט על מנת למזער את הסיכון השיורי לפגיעה אפשרית במערך טכנולוגיות המידע לרמות מקובלות, בהתאם ליעדי הבקרה שנקבעו;

ד. תוצאות הערכת הסיכונים ותוכנית הפעולה לחיזוק הבקרות תועלנה לדיון בוועדת ההיגוי ותוצגנה לדירקטוריון של הגוף המוסדי. יש לעדכן באופן שוטף את ההערכה ביחס לשינויים במערכות החברה ולבצע בחינה תקופתית של ההערכה הכוללת.

6. **<u>בקרות מידע וניהול נתונים</u>**

על גוף מוסדי לוודא כי המידע המנוהל על ידו עומד בקריטריונים של **אמינות, שלמות, זמינות, יעילות, סודיות ואפקטיביות**. על מנת להבטיח קיומם של אלה על הנהלת הגוף המוסדי לקיים ולהפעיל מערכת בקרה פנימית הולמת על המידע ועל הנתונים המהווים את הבסיס למידע הארגוני והעסקי ולבצע כל אחד מאלה:

א. מיכון התהליכים המהותיים המנוהלים במסגרת מערכות הליבה בגוף המוסדי, לרבות: הגדרת הממשקים החיוניים עם מערכות אחרות, קיום מנגנוני תיעוד של המידע והתהליכים המנוהלים באמצעותם, קיום מערך גיבויים והרשאות, קיום מנגנוני בקרה ונתיבי ביקורת מובנים, תיעוד שינויים שנערכו במערכות וכד';

ב. על מנת לעמוד בדרישות המיכון המפורטות בסעיף 6.א לעיל, על הגוף המוסדי לערוך מיפוי של מערכות הליבה במטרה לזהות פערי מיכון ולקבוע תכנית עבודה מפורטת להשלמת הפערים. על ועדת ההיגוי והדירקטוריון לדון בתוכנית, לאשר אותה ולערוך מעקב ופיקוח אחר ביצועה;

ג. תיעוד ושמירת מידע, אשר בנוסף ליתרות התקופתיות של המבוטחים והעמיתים יכלול גם פירוט תנועות מרכזיות שבוצעו בנתוני המידע במערכות הגוף המוסדי. לשם כך, על הגוף המוסדי לנהל יומן מעקב ממוחשב לתיעוד פעולות המתבצעות במערכות הליבה

רח' קפלן 1, ירושלים 91030 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

לצורך אבטחת נתיב בקרה ומעקב אחר שינויים ותנועות שבוצעו במערכות הליבה, לרבות מועד ביצוען והגורמים שביצעו כל תנועה;

ד. הגדרת נוהלי בקרת איכות וניסוח מדדים כמותיים ובני השגה במטרה להבטיח את אמינות המידע במערכות המידע בארגון;

ה. גיבוש נהלים לניהול תקלות במערכות הליבה. על הנהלים לכלול התייחסות לסוגי התקלות בהתאם לאופיין ולהשפעתן. כמו כן, הגוף המוסדי יגדיר גורם אחראי לריכוז המידע על התקלות ויקבע את חובות הדיווח עליהן ואת מסלולי הדיווח.
הגוף המוסדי יתעד וינהל את המידע באופן שיאפשר ניתוח של התקלות לצורך הפקת לקחים, דיווח לגורמים שיוגדרו, לרבות לגורמים האחראים על בקרה, פיקוח וניהול הסיכונים, וזאת על מנת להבטיח טיפול נאות בתקלות וביצוע מעקב אחר תיקונן.

ו. הגדרת נוהלי בקרת מידע והתייחסות לבקרות כלליות ולבקרות יישומיות הכוללות: בקרות דיוק שלמות ואימות מידע, אמינות ותקפות העיבודים והתנועות, בקרות פלט, טיפול בשגויים ואימות ושלמות העברות עסקיות.

7. **<u>ביצוע רכש וניהול פרויקטים בתחום מערכות המידע</u>**

מדיניות ניהול מערכות המידע שתאושר על-ידי דירקטוריון של גוף מוסדי, תכלול התייחסות לביצוע רכש מהותי והקמת פרויקטים מרכזיים שיש להם השפעה על מערכות הליבה בגוף המוסדי וכן תכלול התייחסות לביצוע בקרה ופיקוח על הנושא. על הגוף המוסדי לפעול בהתאם למדיניות האמורה ולוודא קיומם של כל אחד מאלה:

א. נהלים בתחום רכש מהותי ופרויקטים מרכזיים, במטרה להבטיח את התאמתם לאסטרטגיית ההצטיידות הכלל-ארגונית בתחומי התשתיות, החומרה, התוכנה ושאר השירותים הנוגעים לתחום טכנולוגיית המידע;

ב. תהליך הערכת הסיכונים הגלומים בביצוע רכש מהותי או בכניסה לפרויקט מרכזי חדש בתחום טכנולוגיות המידע ובחינת המענה הנדרש לטיפול או להפחתה של הסיכונים האמורים;

ג. הבטחת יכולת הגוף המוסדי לבצע בקרה, פיקוח ומעקב אחר הנכסים, המערכות והתשתיות הכלולים בפרויקט או בתהליך הרכש.

ד. **מסגרת עבודה לניהול פרויקטים**

1) גוף מוסדי יגדיר מסגרת עבודה לניהול פרויקטים בהתאם למדיניות הכללית בנושא ניהול טכנולוגיות המידע של הגוף המוסדי וזו תקבל ביטוי בנוהלי הגוף המוסדי ותתייחס לשלבי היזום, התכנון, הביצוע, הבקרה וסיום הפרויקט. מסגרת העבודה תכלול תוכנית אב (אם הוגדרה כזו), הגדרת גורמים אחראיים ויחסי הגומלין בין הגורמים השונים, הגדרת יעדים ותוצרים, עקרונות לתעדוף והקצאת משאבים, אישור משתמשים, תכנית בדיקות פורמאלית, אבטחת איכות וכד';

2) במסגרת ניהול הפרויקט הגוף המוסדי יתן את הדעת לסיכונים המהותיים הגלומים בפרויקט תוך תכנון, זיהוי, ניתוח ובקרה של אירועים ותרחישים בעלי פוטנציאל לסיכון בפרויקט;

רח' קפלן 1, ירושלים 91030 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

3) הגוף המוסדי יוודא קיומה של בקרה על השינויים הנערכים בכל פרויקט בכדי להבטיח כי כל שינוי מהתכנית הבסיסית של הפרויקט ייסקר, יאושר וישולב בתוכנית הפרויקט;

4) הגוף המוסדי יבחן הגדרת הדרישות ואת מדדי האיכות לפרויקט וכן את מנגנוני הניטור והדיווח של עמידה בהם בהתאם ללוחות זמנים או לביצוע;

5) בסיום כל פרויקט יקיים הגוף המוסדי תהליך בחינה להערכת עמידת תוצרי הפרויקט ביעדים שהוגדרו לו, יזהה ויתעד חריגות וכן יפיק לקחים.

8. **ניהול שינויים**

הגוף המוסדי יבטיח את ניהולם התקין של השינויים הנערכים במערכות הליבה, בהתאם לנוהל ביצוע שינויים שיבטיח כל אחד מאלה:

א. קיומה של מערכת ניהול שינויים הולמת המגדירה כללים לביצוע שינויים במערכות הליבה בגוף המוסדי;

ב. גיבוש תהליך פורמאלי לניהול שינויים שיכלול בין היתר:

1) הגדרת סוגי השינויים;

2) הוראות לעניין השלבים והתהליכים הכלולים בתהליך השינוי, לרבות הגדרת הגורמים המוסמכים לביצועו ולאישורו והבקרות על ביצוע השינוי[2];

3) קיום מנגנון תיעוד מסודר של כל אחד מהשלבים שהוגדרו בנוהל. במידה שהוחלט על ידי הגוף המוסדי שלא לבצע אחד משלבי השינוי שנכללו בנוהל ניהול השינויים האמור לעיל, יש לתעד את הסיבות להחלטה בצירוף הנימוקים לכך;

4) קיום תהליכי בקרה וביקורת על תהליכי השינוי, לרבות הפרדה מלאה של תפקידים וסמכויות וכן הפרדה בין סביבות הפיתוח, סביבת הבדיקה וסביבת הייצור;

5) הגדרת הגורמים המוסמכים לבצע את תהליך השינוי והגורמים המוסמכים לאשרו – אישור השינוי יכלול בחינה של השפעת השינוי על תשתיות, יישומים, תהליכים ומערכות קשורות;

6) מנגנוני דיווח על שינויים לגורמים שהוסמכו לכך, שיכללו התייחסות למהות השינוי, להשפעותיו, למדרג וכד'.

7) טיפול בשינויי חירום

שינויי חירום - שינויים בטכנולוגיית המידע הנדרשים באופן מיידי ולא ניתן לבצעם על פי סדר הפעולות והשלבים הכלולים בנוהל השינוי הרגיל, ואשר הוגדרו על ידי הגורמים המוסמכים ככאלה, כגון: תקלה, ליקוי או חסר מהותי;

הטיפול בשינויי חירום יכלול, בין היתר:

א) הגדרת שינוי חירום לרבות התייחסות לפרמטרים והמבחנים לקיומו;

[2] לעניין זה מומלץ לעשות שימוש בשלבים הכלולים בפרק העוסק בניהול שינויים מתוך מסמך:
IT Control Objective For Sarbanes Oxley

רח' קפלן 1, ירושלים 91030 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

ב) תיעוד הולם של שינוי החירום וקבלת אישור הגורם המוסמך בתחום טכנולוגיית מידע לפני יישומם;

ג) ביצוע הערכה של השפעה אפשרית של השינוי על תשתיות, יישומים, תהליכים ומערכות קשורות טרם מתן האישור לביצועו;

ד) תהליך בחינה בדיעבד של שלבי הבקרה והבדיקה שהיו אמורים להתבצע על פי הנוהל.

9. **מיקור-חוץ**

מיקור-חוץ בתחום טכנולוגיות מידע חושף את הגוף המוסדי לסיכונים נוספים מעבר לסיכונים הגלומים בפעילות העסקית הרגילה המנוהלת באמצעות מערכות טכנולוגיות. הגוף המוסדי יזהה את הסיכונים הללו וינהל אותם, בין היתר, בהתאם למפורט להלן:

א. **אחריות הדירקטוריון וההנהלה**

1) על הדירקטוריון לקבוע מדיניות מקיפה בנושא מיקור-חוץ בתחומי הליבה בגוף המוסדי, לרבות לעניין ניהול הפעילויות והתהליכים המבוצעים במסגרת זו ופיקוח עליהם. הגוף המוסדי יפעל בהתאם למדיניות האמורה ויגבש מסגרת פעולה מוכוונת סיכונים לניהול תהליכי מיקור-חוץ, בין היתר בהתאם לאמור בסעיף 3.9 לחוזר 6-9-2006, הוראה לניהול סיכוני אבטחת מידע של הגופים המוסדיים (להלן - **חוזר אבטחת מידע**);

2) על ועדת ההיגוי לקיים דיון בכל החלטה מהותית לקבלת שירותים במיקור-חוץ של מערכות ליבה בגוף המוסדי ולהגיש להנהלה ולדירקטוריון חוות דעת הכוללת את המלצותיה בעניין;

3) גוף מוסדי יבצע פיקוח ומעקב אחר מערכות הקשרים עם ספקי השירות השונים במיקור-חוץ;

4) גוף מוסדי יגדיר בנוהל את הגורמים המוסמכים לאשר החלטה לרכישת שירותים או מערכות ליבה במיקור-חוץ בהתאם לקריטריונים שיוגדרו. על הנוהל לכלול התייחסות למכלול הסוגיות הניהוליות והתפעוליות הנגזרות, לרבות לכל אחד מהנושאים המפורטים להלן:

א) להבטיח שהסדרי מיקור-חוץ לא יפגעו ביכולת הגוף המוסדי לעמוד בהתחייבויותיו כלפי לקוחותיו וביכולתו למלא אחר הוראות הדין;

ב) להבטיח כי השירות המסופק במיקור-חוץ יספק מענה ראוי לצורכי הגוף המוסדי וככל שניתן לחזות, גם לצרכים הצפויים בעתיד;

ג) להבטיח שבידי הגוף המוסדי תיוותר רמה נאותה של שליטה ובקרה ולהבטיח שלא תיפגע יכולתו של הממונה על שוק ההון, ביטוח וחיסכון (להלן - **הממונה**) לפקח על פעולת הגוף המוסדי המבוצעת באמצעות מיקור-חוץ;

רח' קפלן 1, ירושלים 91030 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

ד) להבטיח קיומם של מנגנוני פיקוח אפקטיביים על הפעילות הכלולה במיקור-חוץ ובכלל זאת, קיומם של כלים לזיהוי, למדידה, לניטור ולבקרה של הפעילות האמורה ושל הסיכונים הכרוכים בה;

ה) להגדיר את מסגרות הדיווח שעל ספק השירותים לדווח לגורמים השונים בגוף המוסדי;

הגוף המוסדי נדרש לעגן את ההוראות האמורות בכל התקשרות שלו עם ספק שירות לקבלת שירותים במיקור-חוץ.

ב. **בחירת ספק השירות**

בהליך בחירת ספק השירות על הגוף המוסדי לבצע פעולות אלו:

1) להעריך את הצעות ספקי השירות ביחס לצרכי הגוף המוסדי;

2) להניח את דעתו בדבר יכולתו המקצועית של ספק השירות ואיתנותו הכלכלית אשר יאפשרו לו לתמוך במתן השירות נשוא מיקור-החוץ ברמה סבירה של ביטחון;

3) לוודא כי ספק השירות מקיים מנגנוני בקרה ופיקוח עצמאיים נאותים, וכן מאפשר בדיקה ובקרה באשר לנאותות מנגנונים אלו על ידי הגוף המוסדי. לעניין זה, אם ספק השירות סיפק לגוף המוסדי חוות דעת של רואה חשבון חיצוני בדבר ביצוע ביקורת על בסיס הנחיות SAS 70, רשאי הגוף המוסדי להתבסס על דיווח כאמור, לאחר שבחן את הדיווח ווידא כי הוא נותן מענה לצרכיו.

ג. **הסכמי מיקור-חוץ**

גוף מוסדי יסדיר את התקשרויותיו עם ספקי השירותים בהסכמים חתומים המתארים בצורה ברורה את כל הצדדים המהותיים בהסדרי מיקור-החוץ לרבות חובות וזכויות הצדדים בהתקשרות ואחריותם ומחויבותם לעמידה בהוראות הדין בתחום. כמו כן, יתייחסו ההסכמים, ככל הניתן, לאירועים ולמצבים מהותיים שניתן לצפותם באופן סביר, לרבות למצב בו ידרשו הצדדים לסיום מוקדם של חוזה התקשרות ביניהם.

ד. **ניטור שוטף**

על הגוף המוסדי לנטר באופן שוטף את ביצועי ספק השירות ולקיים תהליכי בקרה על שינויים פוטנציאליים בדרישות הגוף המוסדי לאורך תקופת הסכם ההתקשרות, במטרה להבטיח עמידת הגוף בהוראות הדין, קיומם של תהליכי המשכיות עסקית ואבטחת מידע אפקטיביים. במסגרת כך על הנהלת גוף מוסדי לקיים תהליכי בחינה מחזוריים במטרה להבטיח ולזהות נושאים אלו:

1) עמידת ספק השירות בהסכמי רמת שירות (SLA) ובתנאי הסכם ההתקשרות;

2) שינויים מהותיים במצבו הפיננסי של ספק השירות;

3) שינויים בסביבת הבקרה הכללית של ספק השירות באמצעות קבלה ובחינה של דוחות ביקורת וסקירות בקרה פנימיות אחרות;

4) עמידה בכל העקרונות החלים על גוף מוסדי בגין האמור בחוזר אבטחת מידע, לפי העניין גם על ידי ספק השירות;

5) ניהול כיאות של מערכת הקשרים בין ספקי השירות השונים, לפי העניין.

רח' קפלן 1, ירושלים 91030 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

10. **תחולה**

הוראות חוזר זה יחולו על כל הגופים המוסדיים בישראל.

11. **תחילה**

א. תחילתו של חוזר זה ביום 1 בינואר 2011.

ב. על אף האמור בסעיף 11.א -

1) ביצוע סקר הציות כאמור בסעיף 4.ג לחוזר זה, יושלם לראשונה לא יאוחר מיום 31 במארס 2011 ;

2) הצגתה לראשונה של תכנית הערכת הסיכונים והבקרות לדירקטוריון כאמור בסעיף 5.ד לחוזר זה, תיערך לראשונה לא יאוחר מיום 30 ביוני 2011 ;

3) מיפוי המערכות בהתאם לאמור בסעיף 6.ב לחוזר זה יושלם לא יאוחר מיום 31 במרץ 2011, וגיבוש תכנית עבודה מפורטת להשלמת פערי המיכון בהתאם לאמור באותו הסעיף יושלם לא יאוחר מיום 30 ביוני 2011 ;

4) מיכון מערכות הליבה בהתאם לאמור בסעיף 6.א לחוזר זה יושלם לא יאוחר מיום 31 במארס 2012.

עודד שריג
הממונה על שוק ההון ביטוח וחסכון

רח' קפלן 1, ירושלים 91030 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il