



**בנק ישראל**

הפיקוח על הבנקים

אגף טכנולוגיה וחדשנות

יחידת הסדרה וביקורת בתחום טכנולוגיית המידע

ירושלים, י"ד בטבת תשפ"א

29 בדצמבר 2020

**חוזר ח-06-2643**

לכבוד

**התאגידים הבנקאיים וחברות כרטיסי אשראי**

### **הנדון: דיווח על אירועי כשל טכנולוגי ואירועי סייבר**

(ניהול בנקאי תקין הוראות מס' 361, 357, 367, 366, הוראות דיווח לפיקוח על הבנקים 848, 880)

#### **מבוא**

1. ההתפתחות הטכנולוגית המואצת מביאה להזדמנויות ולהרחבת מגוון השירותים הדיגיטליים ללקוחות. בד בבד עם התפתחות הטכנולוגית גדלה תלותם של התאגידים הבנקאיים בתשתית קריטית זו ואף יש בה בכדי להגביר את סיכוני הטכנולוגיה וסיכוני הסייבר. ניהול וטיפול יעיל באירועי כשל טכנולוגיים ואירועי סייבר הוא חיוני ומהווה אבן יסוד להמשך תפקוד ומתן שירותים על ידי התאגיד הבנקאי בעת אירוע מסוג זה. בהתאם לכך מצא הפיקוח על הבנקים לנכון להגדיר מחדש את דרישות הדיווח בתחומים אלה מתוך מטרה לוודא כי התאגידים הבנקאיים מנהלים כיאות את האירוע, לקבל תמונת מצב ולסייע במקרה הצורך, לצמצם השפעה מערכתית של האירוע ולוודא תהליך תחקור והפקת לקחים בעקבות האירוע.

2. חובת הדיווח של התאגידים הבנקאיים לפיקוח על הבנקים חלה עד היום בהוראות הבאות:

- 2.1. הוראת ניהול בנקאי מס' 357 בנושא "ניהול טכנולוגיית המידע" (להלן "הוראה 357"), הוראת ניהול בנקאי מס' 367 בנושא "בנקאות בתקשורת" (להלן "הוראה 367") והוראת ניהול בנקאי מס' 361 בנושא "ניהול הגנת הסייבר" (להלן "הוראה 361") דורשות מהתאגידים הבנקאיים לדווח לפיקוח על הבנקים במקרים מסוימים על אירועי כשל טכנולוגי ואירועי סייבר.
- 2.2. הוראת דיווח לפיקוח על הבנקים 848 בנושא "דיווח על אירוע סייבר" מנחה כיצד יש לדווח על אירוע סייבר.

3. מתוך כוונה לפשט וליעל את אופן הדיווח של התאגידים הבנקאיים לפיקוח על הבנקים על אירועי כשל טכנולוגי ואירועי סייבר ומכיוון שבמקרים רבים אופן הדיווח והטיפול בשלבים מסוימים באירועי כשל טכנולוגיים דומה לאופן הדיווח והטיפול באירועי סייבר, בוצע רענון ואיחוד הדיווחים הנדרשים מהתאגידים הבנקאיים בהוראות מעלה להוראת נב"ת דיווח אחת אחודה (להלן – "הוראת הנב"ת") ולצידה הוראת דיווח חדשה.

4. הוראת הנב"ת מגדירה את דרישות הדיווח על אירועי כשל טכנולוגי ואירועי סייבר והיא מחליפה את דרישות הדיווח הקיימות בנושאים אלה, כמפורט בסעיפים 13-16.

5. לאחר התייעצות עם הוועדה המייעצת בעניינים הנוגעים לעסקי בנקאות ובאישור הנגיד, קבעתי את הוראת הנב"ת ותקנתי את הוראה 357, הוראה 367 והוראה 361.

## מבנה ההוראה

6. ההוראה כוללת את הנושאים הבאים:

6.1. נושאים כלליים:

6.1.1. **מבוא ומטרות** – הוראת הנב"ת מסדירה את תהליך הדיווח לפיקוח על הבנקים תוך ניהול

וטיפול באירועי כשל טכנולוגי ואירועי סייבר.

6.1.2. **תחולה** – תחולת הוראת הנב"ת תואמת את תחולת הוראה 357, הוראה 367 והוראה 361.

6.1.3. **הגדרות** – מוגדרים בהוראת הנב"ת סוגי האירועים השונים לצורך יצירת שפה אחידה

והגדרת ציפיות. לעניין דיווח על אירוע סייבר, הגדרה זו תואמת את השלבים המפורטים

בהגדרה "ניהול אירוע סייבר" בנב"ת 361.

6.2. דיווח על אירוע כשל טכנולוגי או אירוע סייבר מהותי:

6.2.1. **סוגי אירועים המחייבים דיווח** – הוראת הנב"ת מגדירה את סוגי האירועים המחייבים

בדיווח לפיקוח על הבנקים.

6.2.2. **אחריות הדיווח** – הוראת הנב"ת מגדירה את אחריות הדיווח ומינוי אחראי דיווח בכל

תאגיד בנקאי.

6.2.3. **אופן הדיווח** – הוראת הנב"ת מפרטת את אופן ביצוע הדיווחים על פי שלבי האירוע –

דיווח ראשון על האירוע, דיווחים נוספים במהלך האירוע ודיווח על סיום האירוע.

6.2.4. **תחקור אירוע** – הוראת הנב"ת מחייבת ביצוע תחקיר אירוע והפקת לקחים והעברתו

לפיקוח על הבנקים.

## דגשים

7. הוראת הנב"ת מבקשת לתת את הדגש על דיווח אירועים מהותיים בלבד ולכך כוונו הגדרות סוגי

האירועים לדיווח בסעיף 6 להוראת הנב"ת.

8. יצוין כי הפיקוח על הבנקים יכול לשנות את תדירות הדיווח בהתאם למהות האירוע (הן לחומרא והן

לקולא).

9. אופן הדיווח

9.1. דיווח טלפוני יינתן תוך שתיים מזיהוי האירוע כאירוע המחייב דיווח על מנת להעביר לפיקוח על

הבנקים את המידע הראשוני הנדרש לגבי האירוע ולאפשר את היערכותו לטיפול באירוע תוך קשר

הדוק עם התאגיד המדווח.

9.2. עוקב אחריו יינתן בכתב דיווח ראשוני תוך 8 שעות ממסירת הדיווח הטלפוני על מנת לאפשר

לתאגיד המדווח זמן התארגנות וטיפול באירוע ומאידך לדייק ולפרט את הדיווח על הבנקים כך

שיאפשר טיפול מדויק וממוקד יותר באירוע.

9.3. בהמשך האירוע נדרש עדכון הדיווח על ידי התאגיד המדווח אחת ליום או בעת שינוי מהותי

בהתפתחות האירוע. זאת, עד לסיום האירוע. הדיווח יכלול את הפרטים הידועים לרגע הדיווח

ויהיה מצטבר.

9.4. בשלב הראשון של הטמעת תהליך העבודה על פי הוראת הנב"ת יועברו הדיווחים באמצעות מנגנון

הכספות בקבצי אקסל הבנויים במבנה לוח הדיווח בהוראת הדיווח החדשה. בשלב השני של

הטמעת ההוראה, בכוונת הפיקוח על הבנקים להטמיע מערכת דיווחים ממוחשבת שבאמצעותה יועברו הדיווחים. במקרים חריגים, כאשר יהיה כשל במנגנון הדיווח או סיווג המידע לא יאפשר העברתו באמצעות מנגנון הדיווח יונחה התאגיד הבנקאי למסירת המידע במנגנון דיווח חלופי.

10. בהגדרת "אירוע כשל טכנולוגי" נרחיב כי בהשפעה חמורה ונרחבת מדובר גם על הפעילות פנימה, כגון: נפילה במערכות הייצור במצב אקטיב אקטיב שהכניסה את הגיבוי לפעולה וכתוצאה מכך השירות לא נפגע או תקלה חמורה שקרתה ותוקנה לפני שהשפיעה בפועל (פוטנציאל טכנולוגי, להבדיל מפוטנציאל אירוע וסייבר).

11. בעת הכרזת סיום אירוע על ידי התאגיד הבנקאי, תתבצע בדיקה איכותית של הפיקוח על הבנקים כי אכן האירוע הסתיים.

12. אופן מילוי דרישות הוראת הנב"ת מפורט בהוראת הדיווח לפיקוח על הבנקים מס' 880 בנושא: "דיווח על אירוע כשל טכנולוגי ו/ או אירוע סייבר".

### **התיקונים להוראות**

#### **13. הוראת ניהול בנקאי מס' 357 בנושא "ניהול טכנולוגיית המידע":**

13.1. "(ב) תאגיד בנקאי ידווח למפקח על הבנקים על הנושאים והאירועים הבאים:

(1) אירועי כשל טכנולוגי בהתאם להוראת ניהול בנקאי תקין מס' 366 בנושא "דיווח על אירועי כשל טכנולוגי ואירועי סייבר";

(2) בטל; "

(פרק ח': שונות: פעולות הטעונות הסכמה ופעולות הטעונות דיווח: סעיף 30)

### **דברי הסבר**

נמחקו סוגי אירועים לדיווח, הנחיות לדיווח והפניות לדיווח ע"פ הוראות אחרות. נוספה הפניה לדיווח ע"פ הוראת הנב"ת.

13.2. "(ג) הודעות ודיווחים לפי סעיפים 29 ו- 30 לעיל יש לשלוח ליחידת הסדרה וביקורת בתחום

טכנולוגיית המידע בפיקוח על הבנקים בבנק ישראל.

(ד) הודעות לפי סעיפים (ב) (3) ו- (4) יש לשלוח 30 יום מראש.

(ה) בטל. "

(פרק ח': שונות: פעולות הטעונות הסכמה ופעולות הטעונות דיווח: סעיף 30)

### **דברי הסבר**

פעולות הטעונות הסכמה ופעולות הטעונות דיווח שנותרו בהוראה ידווחו ישירות ליחידת הסדרה וביקורת בתחום טכנולוגיית המידע באגף טכנולוגיה וחדשנות בפיקוח על הבנקים במקום ליחידה למידע ודיווח.

**14. הוראת ניהול בנקאי מס' 361 בנושא "ניהול הגנת הסייבר"**

התאגיד הבנקאי ידווח לפיקוח על הבנקים על אירוע סייבר או אירוע החשוד כאירוע סייבר בהתאם להוראת ניהול בנקאי תקין מס' 366 בנושא "דיווח על אירועי כשל טכנולוגי ואירועי סייבר".  
(דיווח על אירוע סייבר : סעיף 82)

**דברי הסבר**

דיווחים על אירוע סייבר או אירוע החשוד כאירוע סייבר יבוצעו בהתאם להוראת הנב"ת.

**15. הוראת ניהול בנקאי מס' 367 בנושא "בנקאות בתקשורת"**

סעיף 74 – בטל.

(פרק ט': דיווחים ואישורים : נושאים שנדרש לגביהם דיווח)

**דברי הסבר**

נמחקו סוגי אירועים לדיווח, הנחיות לדיווח והפניות לדיווח ע"פ הוראות אחרות (ראה גם חוזר ח-06 - 2645).

**16. הוראת דיווח לפיקוח על הבנקים 848 בנושא "דיווח על אירוע סייבר"**

הוראת הדיווח 848 תבוטל.

**תחילה והוראות מעבר**

17. תחילת האמור בהוראה זו והתיקונים להוראות הינם חודש מיום פרסומם.

**עדכון הקובץ**

18. מצ"ב דפי עדכון לקובץ ניהול בנקאי תקין, להלן הוראות העדכון :

| <u>להכניס עמוד</u>   | <u>להוציא עמוד</u>   |
|----------------------|----------------------|
| 357-1-14 [9] (12/20) | 357-1-15 [8] (11/18) |
| 361-1-19 [2] (12/20) | 361-1-19 [1] (3/15)  |
| 366-1-4 [1] (12/20)  | ----                 |

בכבוד רב,

יאיר אבידן



המפקח על הבנקים

## ניהול טכנולוגיית המידע

### תוכן העניינים

|               |                                                |               |
|---------------|------------------------------------------------|---------------|
| <b>357-2</b>  | <b>כללי</b>                                    | <b>פרק א'</b> |
| 357-2         | 1. מבוא                                        |               |
| 357-2         | 2. תחולה                                       |               |
| <b>357-3</b>  | <b>פיקוח וניהול</b>                            | <b>פרק ב'</b> |
| 357-3         | 3. דירקטוריון                                  |               |
| 357-3         | 4. הנהלה                                       |               |
| 357-3         | 5. נהלים                                       |               |
| 357-4         | 6. תיעוד, רישום ומעקב                          |               |
| 357-4         | 7. ביקורת פנימית                               |               |
| <b>357-5</b>  | <b>סיכונים</b>                                 | <b>פרק ג'</b> |
| 357-5         | 8. הערכת סיכונים                               |               |
| <b>357-6</b>  | <b>אבטחת מידע</b>                              | <b>פרק ד'</b> |
| 357-6         | 9. מנהל אבטחת מידע                             |               |
| 357-6         | 10. אבטחת מידע                                 |               |
| 357-7         | 11. סקר בטיחות וניסיונות חדירה מבוקרים         |               |
| 357-7         | 12. בקרת גישה                                  |               |
| 357-8         | 13. הצפנה                                      |               |
| 357-8         | 14. קישוריות התאגיד הבנקאי לאינטרנט            |               |
| <b>357-10</b> | <b>גיבוי והתאוששות</b>                         | <b>פרק ה'</b> |
| 357-10        | 15. דיון בהנהלה                                |               |
| 357-10        | 16. הסדרי גיבוי והתאוששות                      |               |
| <b>בטל</b>    | <b>מיקור חוץ</b>                               | <b>פרק ו'</b> |
| בטל           | 17. מיקור חוץ                                  |               |
| בטל           | 18. הסכם התקשרות                               |               |
| <b>בטל</b>    | <b>שירותי בנקאות בתקשורת</b>                   | <b>פרק ז'</b> |
| בטל           | 19. הגדרות                                     |               |
| בטל           | 20. הסכם התקשרות למתן שירותי בנקאות בתקשורת    |               |
| בטל           | 21. גילוי נאות                                 |               |
| בטל           | 22. אמצעי זיהוי והרשאות                        |               |
| בטל           | 23. ניהול סיסמאות                              |               |
| בטל           | 24. אמצעי בקרה                                 |               |
| בטל           | 25. עסקאות בתקשורת לטובת צד שלישי              |               |
| בטל           | 26. רשימת מוטבים                               |               |
| בטל           | 27. דואר אלקטרוני                              |               |
| בטל           | 28. ריכוז מידע                                 |               |
| <b>357-13</b> | <b>שונות</b>                                   | <b>פרק ח'</b> |
| 357-13        | 29. בנק חוץ                                    |               |
| 357-13        | 30. פעולות הטעונות הסכמה ופעולות הטעונות דיווח |               |

**פרק א': כללי****מבוא**

1. (א) מערך טכנולוגיית המידע הוא מרכיב מרכזי בתפעול ובניהול התקין של תאגיד בנקאי, לאור היותו של המידע, על כל היבטיו והשלכותיו, בעל השפעה מכרעת על יציבות התאגיד הבנקאי והתפתחותו.
- (ב) בשל גורמים אלו על הנהלת תאגיד בנקאי לייחס את החשיבות הראויה, הן בהיררכיה הניהולית והן במשאבים הכספיים ומשאבי האנוש הנחוצים, לניהול תקין של מערך טכנולוגיית המידע.
- (ג) מבלי לפגוע בכלליות האמור לעיל, נקבעה הוראה זו הכוללת הנחיות פרטניות וכלליות.
- (ד) הוראה זו תואמת את העקרונות בתחום הבנקאות האלקטרונית, שפירסמה הועדה הבינלאומית לפיקוח על הבנקים (ועדת באזל) ביולי 2003.

**תחולה**

2. הוראה זו תחול על תאגידים בנקאיים, וכן על תאגידים כאמור בסעיפים 11(א)(3), 11(א)(3)(ב) ו-11(ב) לחוק הבנקאות (רישוי), התשמ"א-1981 שהואגדו בישראל (להלן: תאגיד בנקאי).

**פרק ב': פיקוח וניהול****דירקטוריון**

3. (א) דירקטוריון של תאגיד בנקאי יקיים דיון תקופתי ויקבע את מדיניות ניהול טכנולוגיית המידע של התאגיד הבנקאי, בהתאם לאמור בסעיף 6(ד) להוראת ניהול בנקאי תקין מס' 301 (דירקטוריון).

(ב) מדיניות ניהול טכנולוגיית המידע תכלול, בין היתר, התייחסות ל:

- (1) אבטחת מידע;
- (2) עקרונות גיבוי והתאוששות במצבים של תקלות ואסונות;
- (3) מיקור חוץ;
- (4) מדיניות פיתוח, לרבות על-ידי משתמשי קצה;
- (5) בטל;

**הנהלה**

4. (א) הנהלת תאגיד בנקאי תמנה מנהל אחד שיהיה חבר הנהלה או כפוף למנכ"ל, אשר יישא באחריות למכלול נושאי טכנולוגיית המידע (להלן: מנהל טכנולוגיית המידע). מנהל זה יהיה בעל הכשרה מקצועית מתאימה וניסיון מוכח בתחום טכנולוגיית המידע וניהולו.  
(א1) על אף האמור בסעיף קטן (א), המפקח על הבנקים רשאי להתיר, במקרים חריגים, למנהל טכנולוגיית המידע בתאגיד הבנקאי לשמש מנהל טכנולוגיית המידע גם בתאגידים בנקאיים הנשלטים על ידי אותו תאגיד בנקאי או בתאגידים כמפורט בסעיפים 11(א)(3), 11(א)(ב3), ו-11(ב) לחוק הבנקאות (רישוי).

(ב) הנהלת תאגיד בנקאי תמנה מנהל אבטחת מידע, כמפורט בסעיף 9.

(ג) הנהלת תאגיד בנקאי תקיים דיון שנתי ביישום מדיניות ניהול טכנולוגיית המידע ותקצובה, ותקבל את ההחלטות הנגזרות, תוך הבחנה בין נושאים רלבנטיים לטווח הקצר לבין נושאים רלבנטיים לטווח הארוך.

(ד) הנהלת תאגיד בנקאי תייחד דיון שנתי ליישום מדיניות אבטחת המידע על כל היבטיה.

(ה) בקביעת המבנה הארגוני של היחידה המופקדת על ניהול טכנולוגיית המידע בתאגיד הבנקאי, ובהגדרת התפקידים של עובדי יחידה זו, תקיים הנהלת התאגיד הבנקאי הפרדת תפקידים וסמכויות נאותה.

(ו) הנהלת תאגיד בנקאי תגדיר את סוגי הפעילויות והאירועים שלגביהם יש לספק התראה להנהלה ולגורמים מוסמכים אחרים, לרבות אלו המחייבים התראה בזמן אמת.

**נהלים**

5. תאגיד בנקאי יקבע נהלים מפורטים לכל שלב ולכל תהליך המטפלים בניהול, תפעול, אבטחה, גיבוי, שרידות ובקרה של טכנולוגיית המידע, ויקיים בקרה נאותה על ביצועם. נהלים אלה יעודכנו באופן שוטף בהתאם לשינויים החלים הן בסביבה העסקית הרלבנטית והן בסביבה הטכנולוגית.

**תיעוד, רישום ומעקב**

6. (א) תאגיד בנקאי יקיים תיעוד מתאים ועדכני למערך טכנולוגיית המידע שלו.

(ב) (1) תאגיד בנקאי יקיים נתיב ביקורת שיתבסס על רישום ממוכן (log) של עצם הגישה

ושל פעולות ושאלות המבוצעות במערכות המידע של התאגיד הבנקאי, אשר יכלול, בין היתר, את זיהוי מורשה הגישה, המקום, הזמן וכן פרטים על נשוא הגישה.

(2) על אף האמור בפסקה (1) לעיל, לגבי שאלות של עובדי התאגיד הבנקאי יקיים התאגיד הבנקאי נתיב ביקורת על פי שיקול דעתו, תוך התבססות על הערכת הסיכונים.

(3) תאגיד בנקאי יקבע את פרק הזמן לשמירת הרישומים כאמור בפסקה (1), ובלבד שפרק הזמן לשמירת הרישומים לא יקטן מ- 60 יום לרישומי שאלות ו- 6 חודשים לרישומי פעולות.

(ג) תאגיד בנקאי יידע את לקוחותיו ואת עובדיו לגבי עצם קיומם של הליכי שמירה של פעולותיהם.

(ד) בכפוף לאמור בסעיף 4(ו), מערכות ניהול הרישומים תספקנה לגורמים המוסמכים לכך, התראות על פעילויות חיצוניות בלתי מורשות וכן על פעילויות חריגות של המשתמשים לסוגיהם.

**ביקורת פנימית**

7. (א) תאגיד בנקאי יכלול, במסגרת הביקורת הפנימית שלו, יחידה ארגונית לביקורת טכנולוגיית המידע שלו. האחראי על הביקורת הפנימית בתחום טכנולוגיית המידע יהיה בעל הכשרה מקצועית וניסיון רלבנטיים לביצוע הביקורת בתחום זה.

(ב) תאגיד בנקאי יעמיד לרשות הביקורת הפנימית את הכלים הדרושים לביצוע ביקורת ובקרה בסביבת מערך טכנולוגיית המידע.

(ג) בכל מקרה בו נעשה שימוש במיקור חוץ של ביקורת פנימית בתחום טכנולוגיית המידע, יש לשמור על יכולת ההערכה בידי הביקורת הפנימית של התאגיד הבנקאי.



## **פרק ג': סיכונים**

### **הערכת סיכונים**

8. (א) הנהלת תאגיד בנקאי תבצע הערכת סיכונים (Risk Assessment) של מערך טכנולוגיית

המידע. על הערכת הסיכונים להתייחס למכלול הסיכונים הפוטנציאליים הקשורים בניהול

מערך טכנולוגיית המידע, כגון:

- משתמשי המערכת הפנימיים והחיצוניים לתאגיד הבנקאי;

- סביבת המערכת;

- פעילות המערכת והשלכותיה על עסקי התאגיד;

- רגישות המידע;

- מיקור חוץ.

(ב) תהליך הערכת הסיכונים יהיה מתמשך, והערכת הסיכונים תתעדכן בהתאם לשינויים

בגורמי הסיכון השונים.

(ג) בהתאם להערכת הסיכונים על התאגיד הבנקאי לנקוט באמצעים הנדרשים למזעור

אפשרות פגיעה במערך טכנולוגיית המידע על כל חלקיו, ומזעור נזק פוטנציאלי.

**פרק ד': אבטחת מידע****מנהל אבטחת מידע**

9. (א) (1) מנהל אבטחת מידע יהיה כפוף לחבר הנהלה של התאגיד הבנקאי.
- (א1) על אף האמור בסעיף קטן (1), המפקח על הבנקים רשאי להתיר, במקרים חריגים, למנהל אבטחת המידע בתאגיד הבנקאי לשמש מנהל אבטחת המידע גם בתאגידים בנקאיים הנשלטים על ידי אותו תאגיד בנקאי או בתאגידים כמפורט בסעיפים 11(א)(3), 11(א)(ב3), ו-11(ב) לחוק הבנקאות (רישוי).
- (2) מנהל אבטחת מידע לא יעסוק בתפקידים ביצועיים אשר עלולים לגרום ניגוד עניינים, ובכלל זה לא ישמש כמנהל טכנולוגיית המידע.
- (3) הנהלת תאגיד בנקאי תקבע את תחומי אחריותו של מנהל אבטחת המידע ואת הנושאים שהחלטות לגביהם טעונות התייחסותו. תחומי אחריותו יכללו, בין היתר:
- אחריות כוללת ליישום מדיניות אבטחת המידע בתאגיד הבנקאי;
  - פיתוח ומעקב של יישום תוכניות אבטחת המידע בתאגיד הבנקאי ובחינה של אפקטיביות מערכת אבטחת המידע;
  - טיפול באירועים חריגים בתחום אבטחת המידע.
- (4) הנהלת תאגיד בנקאי תעמיד לרשות מנהל אבטחת המידע את המשאבים הדרושים למילוי תפקידו.
- (ב) מנהל אבטחת מידע יהיה בעל הכשרה מקצועית וניסיון רלבנטיים בתחום עיסוקו.

**אבטחת מידע**

10. (א) הנהלת תאגיד בנקאי תרכז את עקרונות אבטחת המידע במסמך כתוב, אשר יובא לאישור הדירקטוריון. מסמך זה יעודכן אחת לתקופה.
- (ב) תאגיד בנקאי יישם אמצעי אבטחה - פיזית ולוגית, למניעה, גילוי, תיקון ותיעוד של חשיפות במערך טכנולוגיית המידע ודיווח עליהם, בהתאם להערכת הסיכונים ותוך התייחסות גם להיבטים הבאים:
- (1) זיהוי ואימות (Identification & Authentication);
  - (2) סודיות ופרטיות (Privacy);
  - (3) שלמות ומהימנות של הנתונים (Integrity);
  - (4) מניעת הכחשה (Non Repudiation).
- (ג) תאגיד בנקאי ינהל מעקב שוטף אחר ההתפתחויות הטכנולוגיות, ויתאים את רמת האבטחה ובקרת הגישה למערכותיו על פי השינויים ברמת הסיכונים הנגזרים משינויים טכנולוגיים אלו.
- (ד) תאגיד בנקאי יפעל להפרדת סביבת הייצור (Production) מסביבת הפיתוח והניסוי (Test).

### סקר בטיחות וניסיונות חדירה מבוקרים

11. (א) (1) אחת לתקופה, בהתאם להערכת הסיכונים, ייזום מנהל אבטחת המידע סקר בטיחות של מערך טכנולוגיית המידע של התאגיד הבנקאי (להלן: הסקר). בסקר שיבוצע תוערך האפקטיביות של אמצעי ההגנה, בהתייחס להערכת הסיכונים, ויוצעו דרכים לתיקון הליקויים שיימצאו.
- (2) לגבי מערכות שהוגדרו על-ידי התאגיד הבנקאי כבעלות סיכון גבוה, לרבות מערכות בנקאות בתקשורת, יש לערוך סקר במתכונת כאמור בפסקה (1) לעיל לפני הטמעת שינויים משמעותיים במערכות אלו, כאשר חלו שינויים משמעותיים בסביבה הטכנולוגית בה המערכות פועלות, וכן לקראת הכנסתן לשימוש של מערכות חדשות כאמור, ולפחות אחת ל-18 חודשים.
- (3) תוצאות הסקר יכללו דוח מפורט על הממצאים וההמלצות, ותמצית ניהולית שתציג את עיקרי הדברים.
- (ב) מנהל אבטחת מידע ייזום ניסיונות חדירה מבוקרים למערך טכנולוגיית המידע של התאגיד הבנקאי לבחינת עמידתו בפני סיכונים פנימיים וחיצוניים. פעולה זו תיעשה בתדירות ההולמת את הסיכונים הספציפיים של המערכות השונות, בהתאם להערכת הסיכונים.
- (ג) (1) סקר הבטיחות וניסיונות החדירה המבוקרים, כאמור לעיל, יערכו על ידי גורמים מקצועיים, עצמאיים, בלתי תלויים, חיצוניים לתאגיד הבנקאי, תוך מניעת ניגודי עניינים ונקיטת אמצעי הזהירות המתחייבים.
- (2) הנהלת תאגיד בנקאי תשלים את דיוניה בממצאי סקר הבטיחות וניסיונות החדירה המבוקרים והשלכותיהם, ותקבל את ההחלטות המתחייבות, לרבות קביעת לוח זמנים ליישומן, תוך פרק זמן סביר לאחר מועד תחילת ביצועם.
- (ד) ממצאים מהותיים שעלו בסקר הבטיחות ובניסיונות החדירה המבוקרים יובאו לידיעת הדירקטוריון או ועדה דירקטוריונית מתאימה.

### בקרת גישה

12. (א) (1) תאגיד בנקאי יבצע זיהוי אישי חד-ערכי של כל גורם בעל גישה למערכת מידע (להלן: מורשה גישה) כתנאי מוקדם למתן הגישה.
- (2) על אף האמור בפסקה (1) לעיל, במקרים חריגים של ספקים ועובדים בהם לא ניתן לקיים את האמור לעיל, יישם התאגיד הבנקאי אמצעים חלופיים מתאימים.
- (ב) (1) תאגיד בנקאי יקבע כללים וכלים לזיהוי ולמתן הרשאות לגורמים שונים לרכיבי טכנולוגיית המידע. כללים אלו יביאו בחשבון את רמות הסיכון הנגזרות מטווח האחריות והסמכות של המשתמשים (על-פי סיווג לקבוצות), מהיישום עצמו, מרגישות המידע ומשאר רכיבי טכנולוגיית המידע.
- (2) הסיווג לקבוצות משתמשים יתייחס לגורמים הפנימיים בתאגיד הבנקאי ולגורמים החיצוניים (לרבות לקוחות, ספקים וכו').
- (3) תאגיד בנקאי יפעיל כלים לניהול ולבקרה של מערכת ההרשאות.
- (4) אמצעי הגישה למערכות המידע יהיו בטכניקות מקובלות לעניין זה.
- (ג) (1) לצורך בקרת גישה למערכות מידע שהוערכו כבעלות סיכון גבוה, ובכל מקרה של גישה מרחוק למערך טכנולוגיית המידע של התאגיד הבנקאי על ידי עובדים, ספקים ונותני

שירותים, ישתמש התאגיד הבנקאי בטכנולוגיה המשלבת זיהוי ואימות של המשתמש, סודיות ושלמות הנתונים ומניעת הכחשה.

(2) על אף האמור בפסקה (1) לעיל, רשאי תאגיד בנקאי להשתמש בטכנולוגיה חלופית במקרים הבאים:

- במערכות בסיכון גבוה שלא באמצעות גישה מרחוק, על פי שיקול דעתו של התאגיד הבנקאי, שתתועד בכתב;
- בגישה מרחוק של ספקים ונותני שירותים, כאשר שימוש בטכנולוגיה כאמור אינו אפשרי מסיבות שאינן תלויות בתאגיד הבנקאי.

(ד) תאגיד בנקאי יקבע קריטריונים להפעלת מנגנון ניתוק התקשורת (Time-out) לאחר פרק זמן שבו לא היתה פעילות מצד מורשה הגישה. פרק הזמן ייקבע תוך התחשבות בהערכת הסיכונים.

(ה) על אף האמור בסעיפים (א) – (ג) לעיל, על לקוחות המשתמשים בשירותי בנקאות בתקשורת כהגדרתם בהוראת נ.ב.ת. מספר 367 בנושא: "בנקאות בתקשורת" יחולו הסעיפים הרלבנטיים בהוראה זו.

## הצפנה

13. תאגיד בנקאי יבחן את הצורך בהצפנה של נתונים, לרבות בתוך התקשורת, במערכות שהוגדרו בהתאם להערכת הסיכונים כבעלות סיכון גבוה, ובלבד שבמקרים הבאים תתקיים הצפנה:

(א) בטל.

(1א) בטל.

(ב) גישה מרחוק למחשב התאגיד הבנקאי, בכפוף לאמור בסעיף 12(ג). האמור בסעיף זה אינו חל על חל לקוחות המשתמשים בשירותי בנקאות בתקשורת כהגדרתם בהוראת נ.ב.ת. מספר 367 בנושא: "בנקאות בתקשורת".

(ג) סיסמאות של מורשי גישה.

## קישוריות התאגיד הבנקאי לאינטרנט

14. (א) תאגיד בנקאי ינקוט באמצעים לאיתור התחזות לאתר האינטרנט שלו, ויספק ללקוח כלים מתאימים לוודא את זהות האתר של התאגיד הבנקאי.

(ב) קישוריות התאגיד הבנקאי לאינטרנט תיעשה במקרים הבאים בלבד:

- (1) קישוריות עובדים לאינטרנט, כמפורט בסעיפים קטנים (ג) ו-(ד);
- (2) מתן שירותי בנקאות בתקשורת, כמפורט בהוראת ניהול בנקאי תקין מספר 367;
- (3) שימוש אחר שאושר מראש על-ידי המפקח, כאמור בסעיף 30(א).

(ג) הנהלת תאגיד בנקאי תקבע את השימושים המותרים לעובדי התאגיד הבנקאי באמצעות קישוריות לאינטרנט, על פי הערכת סיכונים ותוך נקיטת אמצעי בקרה נאותים ובכפוף לאמור בסעיף קטן (ד).

(ד) קישוריות עובדי התאגיד הבנקאי לאינטרנט מתחנות עבודה תתאפשר בהתקיים אחד מאלה:

(1) תחנת העבודה קשורה אך ורק לאינטרנט או לרשת שקשורה אך ורק לאינטרנט

(Stand Alone) ושאין עליה יישומים בנקאיים או מידע רגיש;

(2) הקישוריות לאינטרנט תיעשה באמצעות שרת נפרד של התאגיד הבנקאי, ותבוקר

באופן שוטף על ידי האמצעים האמורים בסעיף קטן (ה). בתצורה זו, הקישוריות

לאינטרנט תבוצע לצורכי גלישה ודואר אלקטרוני בלבד;

(ה) בהתאם לאמור בסעיף 10(ג), קישוריות של רשת התאגיד הבנקאי לאינטרנט תאובטח

לפחות על-ידי אנטי וירוס, מסנני תוכן (Content-Filtering), מערכת לאיתור ניסיונות

חדירה (IDS) ו-Firewall.

(ו) התאגיד הבנקאי יישם, על פי הערכת הסיכונים, אמצעים ממוכנים לבקרת אפליקציה

ולסריקת חולשות המערכת.

(ז) האמור בסעיפים קטנים (ה) ו-(ו) יחול על כל אתרי התאגיד הבנקאי, לרבות האתר

השיווקי.

**פרק ה': גיבוי והתאוששות****דיון בהנהלה**

15. (א) אחת לתקופה תקיים הנהלת תאגיד בנקאי דיון בעקרונות הגיבוי וההתאוששות ותקבל החלטות בתחום זה, תוך התייחסות מפורטת להערכת הסיכונים ולעניינים הבאים:
- (1) הגדרת מצבי תקלות (לרבות אצל ספקי התאגיד הבנקאי) ואסונות (לרבות אסונות טבע, שריפות, מלחמה ושעת חירום) עבור מכלול היחידות הארגוניות, והשלכותיהם על המשך הפעילות של התאגיד הבנקאי;
  - (2) קביעת התהליכים העסקיים החיוניים גם במצבי תקלות ואסונות, מערכות המידע הרלבנטיות לתפעולם ואופן תפעולן של מערכות אלו במצבים כאמור;
  - (3) רכיבי התוכנה, החומרה והתקשורת השונים;
  - (4) היבטי הגיבוי וההתאוששות, לרבות התייחסות לגיבוי שוטף, משך הגיבוי, תדירות הגיבוי, מדיית הגיבוי, זמני השבתה מרביים, ותהליך החזרה לשגרת העבודה;
  - (5) הסתמכות על גורמי חוץ בעת קיומן של הפרעות לפעולה סדירה של מערכות המידע, וזמן ההתאוששות הנחוץ לתאגיד הבנקאי להחזרת מערכות המידע לפעולה סדירה.
- (ב) במסגרת הדיון יוחלט על הסדרי הגיבוי השוטף (לרבות גיבוי לכוח אדם ולתיעוד) ועל השקעות במתקני גיבוי ובהסדרי גיבוי אחרים עבור מערכות מהותיות שנקבעו על פי האמור בסעיף קטן (א)(2) לעיל.

**הסדרי גיבוי והתאוששות**

16. (א) (1) תאגיד בנקאי יקיים תכנית מפורטת להפעלת מערך טכנולוגיית המידע שלו במקרים של תקלות ואסונות (להלן: תכנית התאוששות מאסון), כאמור בסעיף 15.
- (2) תאגיד בנקאי יבחן ויעדכן את תכנית ההתאוששות מאסון על-פי השינויים שחלו בתקופה שחלפה מהעדכון הקודם (לרבות שינויים במערך החירום ובהערכת הסיכונים) לפחות אחת לשנתיים וכן בעת ביצוע שינוי מהותי.
- (ב) לפחות אחת לשנתיים וכן בעת ביצוע שינוי מהותי במערך החירום, יקיים תאגיד בנקאי ניסוי של כל הסדרי הגיבוי וההתאוששות שלו.
- (ג) אחסון גיבויי ציוד, תוכנה ומידע חיוניים יהיה במקום מרוחק ממקום אחסון המקור, כך שאירועים כאסון טבע, מלחמה ודומיהם לא יפגעו בו-זמנית בציוד, בתוכנה ובמידע המקוריים ובגיבוי, ולא ימנעו שימוש בהם.
- (ד) תאגיד בנקאי ינקוט באמצעים שיבטיחו אפשרות שחזור מידע מעותקי גיבוי, לרבות מידע שנשמר באמצעים שחדלו לשמש אותו.

**פרק ו': מיקור חוץ**

בטל.

|

**פרק ז': שירותי בנקאות בתקשורת**

בטל.



**פרק ח': שונות****בנק חוץ**

29. ההוראה תחול כלשונה על בנק חוץ, למעט השינויים המפורטים להלן:
- (א) בכל מקום בהוראה, הביטוי "מערך טכנולוגיית מידע" יוחלף בביטוי "מערך טכנולוגיית המידע המקומי, לרבות הממשקים של מערך זה עם מערך הבנק בחו"ל".
- (ב) סעיף 3 יחול על ההנהלה במקום על הדירקטוריון.
- (ג) לסעיף קטן 11(א)(3) יתווסף המשפט:
- "עמותה מהתמצית הניהולית יועבר לידעית הממונה על אבטחת המידע בבנק האם".
- (ד) לסעיף 16 להוראה יתווסף הסעיף הבא:
- "(ה) בנק חוץ ישמור בכל עת, במערכות המידע המקומיות בסניפיו בישראל, נתונים מלאים המכילים את כל הפרטים האישיים והמנהליים לגבי בעלי החשבונות, מיופי הכח וזכויות החתימה, וכן את כל היתרות העדכניות של החשבונות המנוהלים בסניפיו בישראל".
- (ה) הסעיפים המפורטים להלן יכולים להתבצע על ידי בנק האם, ולא ישירות על ידי בנק החוץ, ובלבד שבנק החוץ יבצע במידת הצורך את ההתאמות הנדרשות כדי לעמוד בסעיפי ההוראה הבאים כלשונם: 5, 6(א), 6(ב), 7, 8(א), 10(א), 10(ב), 12, 13, 14, 16(ד), ובכדי לעמוד בהוראת ניהול בנקאי תקין מספר 367.
- (ו) במקרים חריגים, בנק חוץ הסבור כי סעיפים מסוימים בהוראה זו אינם ישימים לגביו, רשאי לפנות למפקח על מנת לתאם תחולתם ו/או דרך יישומם לגביו, כמפורט בסעיף 30(א).

**פעולות הטעונות הסכמה ופעולות הטעונות דיווח**

30. (א) תאגיד בנקאי המעוניין לבצע את אחת מהפעולות הבאות יודיע מראש למפקח. לא הודיע המפקח לתאגיד הבנקאי, תוך 90 יום, על אי אישור הפעילות, יוכל התאגיד הבנקאי לראות זאת כאישור:
- (1) בטל;
- (א1) מינוי מנהל טכנולוגיית המידע כמפורט בסעיף 4(א1) ו/או מינוי מנהל אבטחת מידע כמפורט בסעיף 9(א)(א1).
- (ב1) בטל.
- (2) קישוריות התאגיד הבנקאי לאינטרנט על-פי סעיף 14(ב)(3);
- (3) בטל;
- (4) בטל;
- (5) התאמת תחולת סעיפי ההוראה עבור בנק חוץ, כמפורט בסעיף 29(ו).
- (ב) תאגיד בנקאי ידווח למפקח על הבנקים על הנושאים והאירועים הבאים:
- (1) אירועי כשל טכנולוגי בהתאם להוראת ניהול בנקאי תקין מס' 366 בנושא "דיווח על אירועי כשל טכנולוגי ואירועי סייבר";
- (2) בטל;
- (3) הקמת תאגיד עזר שעיסוקו בתחום טכנולוגיית המידע;

(4) החלטה על שינויים מהותיים צפויים במדיניות ניהול טכנולוגיית המידע, הסבה

מהותית של מערכות המחשוב ומחשוב מחדש של מערכות מרכזיות ודומיהם ;

(5) בטל ;

(6) בטל.

(ג) הודעות ודיווחים לפי סעיפים 29 ו- 30 לעיל יש לשלוח ליחידת הסדרה וביקורת בתחום

טכנולוגיית המידע בפיקוח על הבנקים בבנק ישראל.

(ד) הודעות לפי סעיפים (ב)(3) ו- (4) יש לשלוח 30 יום מראש.

(ה) בטל.

\* \* \*

#### עדכונים

| חוזר 06 מס' | גרסה | פרטים                                | תאריך    |
|-------------|------|--------------------------------------|----------|
| 830         |      | חוזר מקורי                           | 31/12/79 |
| -----       | 1    | שיבוץ בהוראות ניהול בנקאי תקין       | 8/91     |
| -----       | 2    | גרסה מחודשת של קובץ ניהול בנקאי תקין | 12/95    |
| 1890        | 3    | עדכון                                | 27/8/97  |
| 2118        | 4    | החלפת הוראה 357 + הוראה 412          | 14/9/03  |
| 2292        | 5    | עדכון                                | 30/1/11  |
| 2334        | 6    | עדכון                                | 29/4/12  |
| 2507        | 7    | עדכון                                | 21/7/16  |
| 2579        | 8    | עדכון                                | 13/11/18 |
| 2643        | 9    | עדכון                                | 29/12/20 |

#### עדכונים הוראה 412 (בנקאות בתקשורת)

| חוזר 06 מס' | גרסה | פרטים                                | תאריך   |
|-------------|------|--------------------------------------|---------|
| 103/16      |      | חוזר מקורי                           | 25/9/88 |
| -----       | 1    | שיבוץ בהוראות ניהול בנקאי תקין       | 8/91    |
| -----       | 2    | גרסה מחודשת של קובץ ניהול בנקאי תקין | 12/95   |
| 1814        | 3    | עדכון                                | 17/4/96 |
| 1822        | 4    | עדכון                                | 30/6/96 |
| 1889        | 5    | עדכון                                | 27/8/97 |
| 2118        |      | ביטול ההוראה                         | 14/9/03 |

**ניהול הגנת הסייבר****פרק א': כללי****מבוא**

1. להתפתחות המתמשכת ולחדשנות הטכנולוגית נודעת השפעה מרחיקת לכת על האופן שבו תאגידים בנקאיים מנהלים את עסקיהם ועל האופן שבו הם מתקשרים עם לקוחות, ספקים ושותפים.
2. קצב השינויים המהיר בתשתית הטכנולוגית, החדשנות המתמדת במתן שירותים בנקאיים ללקוחות, זמינותם של השירותים "בכל עת, בכל מקום", הקישור של מערכות מידע ותיקות של התאגיד הבנקאי לתשתיות מחשוב מודרניות ו"פתוחות", כמו גם התלות הגוברת בשירותי מחשוב ותקשורת המסופקים על ידי צד שלישי, יוצרים כר נרחב מאוד להיווצרות חולשות במערכי ההגנה של התאגיד הבנקאי אשר עלולות לחשוף אותו לסיכוני סייבר משמעותיים.
3. בד בבד, חל גידול משמעותי בעצמת איומי הסייבר, הן מבחינת היקפם, הן בבחינת גורמי האיום והן בהיבטי תחכום וזמינות כלי התקיפה.
4. התממשותם של סיכוני סייבר עלולה לשבש את פעילותו התקינה והמאובטחת של התאגיד, ולגרום בין היתר, למניעת שירות מלקוחותיו, לחשיפת מידע פרטי, למחיקה ושיבוש נתונים של התאגיד הבנקאי ושל לקוחותיו, לירידה באמון הציבור, לפגיעה בתדמית התאגיד הבנקאי וביכולתו לנהל את נכסיו ואת נכסי לקוחותיו באופן נאות. בתרחיש קיצון התממשותם של סיכונים אלו עלולה לפגוע ביציבותו של התאגיד הבנקאי.
5. אשר על כן, על התאגידים הבנקאיים לתת דגש מיוחד ולנקוט בצעדים הדרושים לצורך ניהול אפקטיבי של הגנת הסייבר. בפרט, נדרשים התאגידים הבנקאיים להרחיב ולהעמיק את יכולות ההתמודדות הקיימות של אבטחת המידע באופן אשר יאפשר להם להתמודד כנגד איומי הסייבר.
6. ניהול סיכוני סייבר מהווה חלק מהמערך הכולל של ניהול סיכונים בתאגיד הבנקאי. הוראה זו נועדה להוסיף ולהרחיב על ההוראות המפורטות בסעיף 8 בהמשך, בכל הנוגע לניהול תקין של סיכוני הסייבר.

**עקרונות יסוד לניהול הגנת הסייבר**

7. ניהול הגנת הסייבר של תאגיד בנקאי יתבסס על עקרונות היסוד המפורטים בהוראה זו. עקרונות אלו מהווים קווים מנחים, אשר מקנים את הגמישות הנדרשת לאור קצב השינויים המהיר בתחום הסייבר, ומתוך הכרה שלכל תאגיד פרופיל סיכונים ייחודי, הדורש התאמה של תכנית הגנת הסייבר למאפייני הפעילות ולצרכים העסקיים הפרטניים של כל תאגיד.

8. התאגיד הבנקאי ינהל את סיכוני הסייבר בראייה משולבת כלל תאגידיית במסגרת ובהתאם לכללים לניהול ולבקרת סיכונים כאמור בהוראות ניהול בנקאי תקין, ובפרט בהוראות הבאות :

- (א) הוראה מספר 310 - "ניהול סיכונים" ;
  - (ב) הוראה מספר 350 - "ניהול סיכונים תפעוליים" ;
  - (ג) הוראה מספר 355 - "ניהול המשכיות עסקית" ;
  - (ד) הוראה מספר 357 - "ניהול טכנולוגיית המידע".
9. במסגרת תהליך ניהול הסיכונים התפעוליים, כאמור בהוראת ניהול בנקאי תקין מס' 350, תאגיד בנקאי יביא בחשבון, באופן מתועד, את סיכוני הסייבר הרלוונטיים.
10. בכל הנוגע לניהול המשכיות עסקית, בהתאם להוראת ניהול בנקאי תקין מס' 355, יתייחס התאגיד הבנקאי גם לתרחישי אירועי סייבר שיש בהם כדי להשפיע על פעילות התאגיד, ספקים ונותני שירותים, זמינות תשתיות תומכות וכיו"ב, כל זאת בכדי לשפר את עמידותו של התאגיד בעת התרחשות שיבושים תפעוליים, הנגרמים מהתממשות סיכוני סייבר, וכן להקטין את ההשפעה ששיבושים מסוג זה עלולים לגרום לרציפות הפעילות העסקית בתאגיד ובמשק.
11. ניהול נאות של סיכוני הסייבר מחייב הרחבה והתאמה של המסגרת הקיימת של ניהול סיכוני טכנולוגיית המידע בתאגיד הבנקאי בהיבטי תפיסת מרחב האיום ויכולות ההגנה הנדרשות, כמפורט בהוראה זו.

## תחולה

12. הוראה זו תחול על :
- (א) תאגיד בנקאי, כהגדרתו בחוק הבנקאות (רישוי), התשמ"א-1981 (להלן – חוק הבנקאות (רישוי)) ;
  - (ב) תאגיד כאמור בסעיפים 11(א3), 11(א3ב) ו-11(ב) לחוק הבנקאות (רישוי), שהינו בשליטה, במישרין או בעקיפין, של התאגיד הבנקאי, כאילו היה תאגיד בנקאי.
  - (ג) המפקח רשאי לקבוע הוראות נוספות על אלה המפורטות להלן, שיחולו על תאגידים בנקאיים מסוימים.

## הגדרות

13. בהוראה זו למונחים הבאים תהיה המשמעות כמפורט להלן :

|                                                                                                                                                                                                                                                                                |                                 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| איום להתרחשות אירוע סייבר.                                                                                                                                                                                                                                                     | <b>"איום סייבר"</b> -           |
| אירוע סייבר הינו אירוע אשר במהלכו מתבצעת תקיפת מערכות מחשב ו/או מערכות ותשתיות משובצות מחשב על ידי, או מטעם, יריבים (חיצוניים או פנימיים לתאגיד הבנקאי) אשר עלולה לגרום להתממשות סיכון סייבר. יצוין, כי בהגדרה זו נכללים גם ניסיון לביצוע תקיפה כאמור גם אם לא נגרם נזק בפועל. | <b>"אירוע סייבר"</b> –          |
| פעולות שנועדו לבחון את תקינות יישומן בפועל של בקורות ההגנה (ניהוליות, תפעוליות וטכניות), התפעול השוטף שלהן, ואת האפקטיביות שלהן אל מול דרישות ההגנה הרלבנטיות.                                                                                                                 | <b>"הערכת בקורות הגנה"</b>      |
| ידיעה המתייחסת לאירוע סייבר מתוכנן, או אירוע שכבר התרחש, או עודו מתרחש, אך טרם זוהה על ידי הגורם המותקף.                                                                                                                                                                       | <b>"התרעה על אירוע סייבר"</b> - |
| בהקשר הוראה זו: יחיד, קבוצה, ארגון, או גורמים מדינתיים שבכוונתם להסב נזק לתאגיד בנקאי.                                                                                                                                                                                         | <b>"יריב"</b> (adversary) –     |

**"ניהול אירוע סייבר" -**

תהליך מובנה, אשר מתייחס לשלבים הבאים :

(א) **זיהוי (Detection)** - ביצוע בירור ראשוני בדבר קיומו של אירוע סייבר וגיבוש מהיר ככל האפשר של דפוס הפעילות הדרוש לשלב הבא אחריו.

(ב) **ניתוח (Analysis)** - ביצוע בירור מקיף ומעמיק ככל האפשר לגבי אירוע הסייבר, לצורך קבלת החלטות ברמה האופרטיבית, גיבוש רשימת חלופות של דפוסי פעולה אפשריים לבלימת התקיפה והחלטה על דרך הפעולה העיקרית לשלב ההכלה.

(ג) **הכלה (Containment)** - השגת שליטה ראשונית באירוע לצורך הכללתו ועצירת החמרתו והשגת יעדיו. ביצוע תהליך השתלטות על מערך התקיפה, בתוך התאגיד הבנקאי המותקף, ועצירה מלאה של ווקטור הנזק.

(ד) **הכרעה (Eradication)** - נטרול רכיבי התקיפה שמצויים במערכות התאגיד הבנקאי, תוך שאיפה לבטל או למזער, ככל שניתן, את הנזק שכבר נגרם.

(ה) **השבה (Recovery)** - חזרה לתקינות ופעילות מלאה של כל פעילות אצל התאגיד הבנקאי המותקף שהושבת, הוגבל או הופרע תפקודו.

כל שלב כולל דיווח לגורמים הפנימיים והחיצוניים הרלוונטיים.

**"נזק" -**

תוצאה בלתי רצויה, לרבות שיבוש/הפרעה/השבתה של פעילות; גניבת נכס; איסוף מודיעין; פגיעה במוניטין/אמון הציבור.

**"סיום אירוע סייבר"**

-(Post-Incident Activity)

תהליך מובנה, אשר מתייחס לשלבים הבאים :

(א) **תחקור והפקת לקחים** - תהליך בחינה וניתוח מתודולוגי של ניהול אירוע הסייבר מראשיתו לסופו בהיבטי אנשים, תהליכים וטכנולוגיה. התהליך מבוצע בסמוך ככל שניתן למועד הטיפול האופרטיבי באירוע, במטרה לספק לקחים ותובנות אשר יאפשרו טיפול יעיל ומהיר יותר באירוע סייבר עתידי.

(ב) **מעקב אחר יישום הלקחים ותובנות** - תהליך בחינה הבא לוודא כי כל הלקחים והתובנות שעלו באירוע ימומשו בפועל.

**"סיכון סייבר" -**

פוטנציאל לנזק שנובע מהתרחשות אירוע סייבר, בהתחשב ברמת סבירותו וחומרת השלכותיו.

## **פרק ב': ממשל תאגידי**

### **דירקטוריון והנהלה בכירה**

14. התאגיד הבנקאי ינהל את סיכוני הסייבר בהתאם לעקרונות האמורים בהוראת ניהול בנקאי תקין מס' 350. הדירקטוריון והנהלה הבכירה של תאגיד בנקאי ייצרו מסגרת אפקטיבית לניהול סיכוני הסייבר.

15. הדירקטוריון של התאגיד הבנקאי יהיה אחראי על הנושאים הבאים:

- (א) התווית אסטרטגית הגנת סייבר כלל תאגידית ואישורה;
- (ב) אישור מסגרת לניהול סיכוני הסייבר ומדיניות הגנת הסייבר התאגידית;
- (ג) קביעת אופן המעקב והפיקוח על ההנהלה הבכירה, ביישום מסגרת ניהול סיכוני הסייבר;

(ד) קבלת דיווח על אירועי סייבר משמעותיים.

16. ההנהלה הבכירה של התאגיד הבנקאי תהיה אחראית על הנושאים הבאים:

- (א) יצירת מסגרת כוללת לניהול סיכוני הסייבר וקיום פיקוח נאות עליה;
- (ב) גיבוש מדיניות הגנת הסייבר התאגידית;
- (ג) יישום עקבי ותחזוקה של מסגרת העבודה לניהול סיכוני סייבר בכל חלקי התאגיד הבנקאי, לרבות הקצאת משאבים נאותים;
- (ד) מעקב אחר האפקטיביות של מערך הגנת הסייבר ותיאום פעילותו מול גורמי ניהול סיכון פנימיים וחיצוניים, כאמור בהוראה זו;
- (ה) קבלת דיווח על תמונת מצב עדכנית של איומי הסייבר ודרכי ההתמודדות מולם, בהתאם לתוצאות הערכת הסיכונים כאמור בהוראה זו;
- (ו) קבלת דיווח תקופתי על אירועי סייבר רלבנטיים (פנימיים וחיצוניים) וניתוח המשמעות הנגזרות מהם;
- (ז) דיון בהשלכות האופרטיביות, חוצות ארגון, של סיכוני סייבר והנחיה ובקרה על ביצוע שינויים או התאמות במערך ההגנה ו/או בפעילות העסקית, לפי הצורך.

### **מנהל הגנת הסייבר**

17. התאגיד הבנקאי ימנה עובד בכיר בעל ידע וניסיון מתאימים כמנהל הגנת הסייבר ויגדיר את תחומי אחריותו וסמכויותיו.

(א) מנהל הגנת הסייבר יהיה כפוף לחבר הנהלה של התאגיד הבנקאי, ויהיה בעל מעמד וסמכות להשפיע על החלטות המשליכות על החשיפה של התאגיד הבנקאי לסיכוני סייבר.

(ב) מיקומו הארגוני של מנהל הגנת הסייבר יקבע באופן בו ימנעו, ככל הניתן, ניגודי עניינים.

(ג) מנהל הגנת הסייבר לא יישא באחריות נוספת שיש בה כדי להפריע לתפקודו;



(ד) ממשקי העבודה והדיווח הנדרשים בין מנהל הגנת הסייבר לבין בעלי התפקידים הרלבנטיים בארגון ייקבעו ויאושרו על ידי ההנהלה.

18. מנהל הגנת הסייבר יעמוד בראש מערך הגנת הסייבר ויהיה אחראי בין היתר על הנושאים הבאים :

- (א) תכלול היבטי ניהול הגנת הסייבר בתאגיד הבנקאי ;
- (ב) ייעוץ להנהלה הבכירה בתחום ניהול הגנת הסייבר ;
- (ג) סיוע להנהלה בגיבוש ויישום מדיניות הגנת הסייבר ;
- (ד) גיבוש מתודולוגיה תאגידית לניהול סיכוני סייבר ;
- (ה) פיתוח, מעקב אחר יישום, וניטור של תכנית מקיפה ופרטנית להתמודדות התאגיד הבנקאי עם סיכוני הסייבר כאמור בהוראה זו ;
- (ו) הגדרת מדיניות פרטנית ונוהלי עבודה למימוש בקורות הגנת סייבר ;
- (ז) יצירת מודעות לאיומי הסייבר והדרכה לעניין דרכי ההתמודדות מולם, בקרב עובדים, ספקים, שותפים ולקוחות התאגיד הבנקאי ;
- (ח) עבודה עם הגורמים הרלבנטיים בתאגיד הבנקאי (טכנולוגיים ועסקיים) בכדי לנתח ולהעריך את רמות הסיכון המובנה בפעילות, את הבקורות הנדרשות ובהתאם, את רמות הסיכון השיווי והחשיפות לאיומי סייבר ;
- (ט) קביעת מסגרת הדיווחים שיקבל מגורמים שונים בתאגיד הבנקאי ;
- (י) תיאום וקישור מול גורמים חיצוניים בנושאי הגנת סייבר ;
- (יא) פיתוח מדדים רלבנטיים, הכנת דוחות ומתן דיווחים שוטפים כאמור בהוראה זו ;
- (יב) תכלול ובקרה של ניהול אירועי סייבר בתאגיד הבנקאי ;
- (יג) ייזום וביצוע תרגולים ;
- (יד) הובלה ותיאום של תהליכים הנוגעים לניהול הגנת הסייבר ;
- (טו) הערכת בקורות הגנת הסייבר ;
- (טז) ניתוח אירועי סייבר משמעותיים בישראל ובעולם, הפקת לקחים ויישום המסקנות הרלוונטיות לתאגיד הבנקאי.

19. המפקח על הבנקים ראשי להתיר למנהל הגנת הסייבר בתאגיד הבנקאי לשמש מנהל הגנת הסייבר גם בתאגידים בנקאיים הנשלטים על ידי אותו תאגיד בנקאי או בתאגידים כמפורט בסעיפים 11(א), 11(א3), 11(א3ב) ו- 11(ב) לחוק הבנקאות (רישוי).

## ביקורת פנימית

20. ניהול הגנת הסייבר ואופן יישומה יבוקרו באופן תקופתי ע"י הביקורת הפנימית.

## מערכי ניהול, תיאום ובקרה משיקים

21. כחלק מניהול סיכוני הסייבר בראייה משולבת כלל תאגידית, מערך הגנת הסייבר יפעל באופן מתואם עם מערכי ניהול, תיאום ובקורות משיקים בתוך התאגיד הבנקאי ומחוץ לו.

22. יחסי הגומלין וזרימת המידע בין המערכים שבתוך התאגיד הבנקאי יוגדרו בכתב. מערכי ניהול, תיאום ובקרה משיקים בתאגיד הבנקאי כוללים, בין היתר : אבטחת מידע, אבטחה פיזית, ממשל מערכות מידע, תפעול מערכות מידע, ניהול סיכונים, הונאות, ניהול כח אדם, המשכיות עסקית, ניהול יחסי לקוחות, דוברות, וייעוץ משפטי.
23. בפרט, מנהל הגנת הסייבר יקיים ממשקי עבודה מול מנהל הסיכונים הראשי והביקורת הפנימית תוך התאמה להוראות הרלבנטיות.
24. יחסי הגומלין וזרימת המידע בין המערכים שבתוך התאגיד הבנקאי לבין מערכים חיצוניים לתאגיד יוגדרו בכתב. מערכים חיצוניים לתאגיד הבנקאי כוללים, בין היתר : גורמי רגולציה, גורמי חקירה ואכיפה, מטה הסייבר הלאומי, גורמי ניהול סיכוני סייבר מקבילים במגזר הפיננסי, גורמי ניהול סיכונים אצל ספקים ושותפים עסקיים ומערכי שיתוף מידע בנוגע לסייבר.

## פרק ג': אסטרטגיית הגנה ומסגרת לניהול סיכוני הסייבר

### תפיסת הגנת הסייבר

25. התאגיד הבנקאי ירחיב ויעמיק את יכולות ההתמודדות הקיימות של אבטחת המידע (דהיינו: מניעה - Prevention, גילוי - Detection, תגובה - Response), באופן אשר יאפשר לו להתמודד כנגד איומי הסייבר. בפרט, התאגיד הבנקאי יפתח וירחיב יכולותיו בתחומים הבאים: חיזוי - Prediction, זיהוי והטעיה, ושרידות - Resilience.

26. התאגיד הבנקאי יקיים מערך הגנת סייבר אפקטיבי ויעיל, הפועל מתוך ראייה תהליכית ומביא לידי ביטוי, בין היתר, את העקרונות הבאים:

(א) תפיסה כוללת של מרחב הפעילות - מערך הגנת הסייבר יתחשב במקומו של התאגיד הבנקאי במכלול שרשרת האספקה של שירותי בנקאות, בשימוש בתשתיות ושירותים כלליים (כגון רשתות חברתיות), ובסיכונים הנובעים מאופי הפעילות אל מול הגורמים השונים במרחב, לרבות בחו"ל, חברות בנות (בישראל ובחו"ל), ספקים, נותני שירותים ולקוחות;

(ב) שיתוף מכלול הגורמים הרלבנטיים בתאגיד הבנקאי בגיבוש ויישום אסטרטגיית ומדיניות הגנת הסייבר;

(ג) פרואקטיביות – יכולות מודיעין, ניטור ותגובה בזמן אמת של מערך ההגנה, אל מול האיומים ושיתוף מידע ומודיעין;

(ד) העמקת יכולות ההתמודדות כנגד איום ממוקד, באמצעות יצירת מערכי הגנת סייבר המשלבים תשתיות ארגוניות ואנושיות, נהלים ותהליכי עבודה, וטכנולוגיות (People, Processes, Technologies) ופריסתם בשכבות בתצורת הגנה לעומק (Defense in Depth) בכדי למזער את החשיפה לאיום ולהשלכותיו;

(ה) שילוב יכולות מתקדמות במערך ההגנה (לרבות הונאת התוקף, פריסת מלכודות וזיהוי דפוסים חשודים ואנומאליות) גם ברמת תשתיות המחשוב והתקשורת וגם ברמת הפעילות העסקית (למשל: זיהוי הונאות);

(ו) מתן דגש למערכי הגילוי, החקירה והתגובה, מתוך הכרה במורכבות האיום ויכולות היריב, בהתבסס על ההנחה שמניעה מוחלטת של התממשות הסיכון היא בלתי אפשרית, ובהתייחס גם לאיומים שהסבירות להתממשותם היא נמוכה, אולם פוטנציאל הנזק שלהם הוא גבוה.

(ז) עמידות – מיפוי וחקר הסביבה, חיזוי וחקר איומים, מערך הגנה ממוקד משימה שיאפשר לתאגיד הבנקאי לספוג את השלכותיו של שיבוש תפעולי משמעותי (ישיר או עקיף) עקב התקפת סייבר ולהמשיך לנהל תהליכים ולספק שירותים חיוניים.

(ח) מתן דגש להגנה על פרטיות לקוחות התאגיד הבנקאי ונכסיהם, ושמירה על רמות אמינות, נאותות וזמינות גבוהות של השירותים המסופקים על ידי התאגידים הבנקאיים.

#### אסטרטגיית הגנת סייבר

27. אסטרטגיית הגנת סייבר כלל תאגידית תעוגן במסמך שיכלול, בין היתר, את הנושאים הבאים:

- (א) מקומה וחשיבותה של הגנה הסייבר בתאגיד הבנקאי;
  - (ב) תפיסת איום הסייבר והאתגרים מולם עומד התאגיד הבנקאי;
  - (ג) גישת התאגיד הבנקאי לניהול סיכוני סייבר, קביעה וניטור של רמת חשיפה לאיומי סייבר;
  - (ד) עיקרי אסטרטגיית הגנת הסייבר: יעדים, עקרונות הפעלה ויישום.
28. האסטרטגיה תעודכן על פי הצורך ובכל מקרה לפחות פעם בשלוש שנים.

#### מסגרת לניהול סיכוני הסייבר

29. המסגרת לניהול סיכוני הסייבר תעוגן במסמך שיכלול, בין היתר, את הנושאים הבאים:
- (א) זיהוי מבני הממשל התאגידי המשמשים לניהול סיכוני הסייבר, לרבות תחומי אחריות וקווי דיווח;
  - (ב) תיאור הכלים והמתודולוגיות להערכת הסיכונים ואופן השימוש בהם;
  - (ג) תיאור תהליכי ואמצעי הגנה עיקריים ואופן בקרתם והערכתם.

#### מדיניות הגנת סייבר

30. התאגיד הבנקאי יגדיר מדיניות הגנת סייבר כלל תאגידית, אשר תתייחס למכלול הבקורות ודרכי הפעולה להשגת יעדי ההגנה בהתאם לאסטרטגיה. המדיניות תעבור הערכה מדי שנה ותעודכן במידת הצורך.
31. המדיניות תתייחס, בין היתר, לנושאים הבאים: יעדי הגנת הסייבר; הגדרת תחומי אחריות, בעלי תפקיד וגורמים מעורבים (לרבות ממשקי עבודה); מבנים ארגוניים; מבנה וממשל תהליך ניהול סיכוני הסייבר בתאגיד הבנקאי; המסגרת הנוהלית הפנימית של התאגיד הבנקאי; פירוט הבקורות הנדרשות והמסגרת ליישומן; מערכי ניטור ותגובה; קידום מודעות; איסוף, מחקר ושיתוף מידע; שימוש במדדי יישום, בשלות ואפקטיביות; הערכה, בקרה ודיווח.
32. בהתאם למדיניות הגנת הסייבר, התאגיד הבנקאי ייקבע מדיניות פרטנית עבור בקורות ההגנה המיושמות. מסמכי המדיניות הפרטניים יעודכנו על פי הצורך.

### תכניות עבודה

33. על בסיס האסטרטגיה והמדיניות, וכנגזרת מניתוח הסיכונים וחיפוף הסייבר, יגבש התאגיד הבנקאי תכנית עבודה רב-שנתית, אשר תתווה ותתעדף את דרכי יסום הבקרות השונות לצמצום סיכוני הסייבר. התכנית תאושר בידי הנהלת התאגיד הבנקאי אשר תקצה משאבים הולמים להשגת יעדי התכנית.

## **פרק ד': ניהול סיכוני הסייבר**

### **ניהול סיכוני הסייבר : זיהוי סיכונים, הערכת סיכונים**

34. תהליך אפקטיבי לזיהוי והערכת סיכוני סייבר מתייחס, בנוסף לאמור בסעיף 26 להוראת ניהול בנקאי תקין מס' 350, לגורמי האיום השונים, לסביבות הפעילות השונות של התאגיד (הפנימיות והחיצוניות) ולמגוון תרחישים, לרבות התייחסות לסיכונים הנובעים מפשיעת סייבר, תלות בתשתיות תומכות ועבודה עם ספקי שירות חיצוניים.
35. התאגיד הבנקאי יבצע, אחת לשנה לכל הפחות, הערכה של סיכונים ובקורות סייבר, אשר מזהה את הסיכון המובנה, את האפקטיביות של סביבת הבקרה, ואת הסיכון השירי.
36. תהליך זיהוי והערכת סיכוני הסייבר צריך להיות מתמשך ולהתבצע בהתאם לשינויים פנימיים וחיצוניים, ובכללם שינויים עסקיים, ארגוניים וטכנולוגיים.
37. התאגיד הבנקאי יודא כי הערכת סיכוני הסייבר ותשתית הבקורות לניהול מתעדכנות בהתאם לשינויים והמגמות במערך האיומים ובהתאם לקצב הגידול או השינויים במוצרים, פעילויות, תהליכים ומערכות.
38. לצורך ניתוח והערכת איומי הסייבר יתחשב התאגיד הבנקאי בנתונים האמורים בסעיף 28 להוראת ניהול בנקאי תקין מס' 350, בדגשים ובשינויים כמפורט להלן:
  - (א) ממצאי ביקורות וסקרים וכל מידע שוטף אשר יש בהם כדי להצביע על חולשות בבקורות הרלבנטיות;
  - (ב) איסוף וניתוח נתונים חיצוניים שביכולתם להצביע על נקודות תורפה אפשריות או להוביל לגילוי חשיפות לסיכונים שלא זוהו בעבר;
  - (ג) איסוף וניתוח נתונים של אירועי סייבר בתאגיד;
  - (ד) מיפוי תהליכים עסקיים, לצורך חשיפת סיכונים ספציפיים, קשרי תלות הדדית בין סיכונים, ותחומי חולשה בבקורות או בניהול הסיכונים;
  - (ה) שימוש במדדים לצורך כימות החשיפה לסיכוני סייבר תוך שימוש במדדי הערכה איכותיים ו/או כמותיים, באופן אשר יאפשר מעקב אחרי שינויים בערכים אלו מעת לעת.
  - (ו) שימוש במדדי בשלות תהליכים (Process Maturity), אינדיקטורים עיקריים לסיכון (KRI) ולביצוע (KPI) וכיו"ב, בכדי לספק תובנות על סטטוס מנגנוני הבקרה ותכנית הגנת הסייבר;
  - (ז) ניתוח תרחישים בשיתוף עם מנהלי קווי העסקים ומנהלי הסיכונים במטרה לזהות אירועים פוטנציאליים של התממשות הסיכון, להעריך את תוצאותיהם האפשריות, ולשפר את יכולת הזיהוי והתגובה לאותם אירועים;
  - (ח) ניתוח השוואתי של תוצאות של כלי הערכה שונים, בכדי לספק מבט מקיף יותר על פרופיל סיכון הסייבר של התאגיד הבנקאי.

39. מתודולוגיות זיהוי, מדידה והערכת סיכוני הסייבר בתאגיד הבנקאי תהיינה מתועדות ומאושרות בידי ההנהלה הבכירה.

#### **הערכת בקורות הגנת הסייבר**

40. מנהל הגנת הסייבר יודא קיום מנגנונים ניהוליים, תפעוליים וטכניים לביצוע הערכת בקורות הגנת הסייבר ויזום הפעלת מנגנוני הערכה ובקרה כאמור, לפי הצורך.

41. תכנון מערך הערכת בקורות הגנת הסייבר ייגזר מתפיסת מכלול מערך איומי הסייבר על התאגיד הבנקאי, ובהתחשב בסוגי הסיכונים, תרחישי אירוע סייבר שונים, הסתברות התממשותם ובתוצאות סקרים קודמים.

42. מנגנוני הערכת בקורות הגנת הסייבר יתואמו וישולבו במנגנוני הערכה קיימים בתאגיד, בין היתר, בסקרי פגיעויות (Vulnerability Assessments) ובדיקות חוסן/מבדקי חדירה מבוקרים (Penetration Tests) בהתאם להוראת ניהול בנקאי תקין מס' 357, תהליכי ביקורת פנימית על פי הוראת ניהול בנקאי תקין מס' 307, תהליכי ציות לחקיקה/תקנים וכיו"ב.

43. המדדים להערכת סיכוני הסייבר יעודכנו, מעת לעת, בהתאם לתוצאות הערכת בקורות ההגנה.

44. הערכת בקורות הגנת הסייבר תכלול ניתוח מצב הבקורות בהתייחס לאיומי הסייבר, לחולשות ולסיכונים הרלבנטיים, בחתכי הפעילות השונים לרבות: גישה פיזית; מנהל וארגון; ניהול מחזור חיי מערכות מידע (Information System Lifecycle) בסביבות השונות; ניהול תשתיות תקשורת ומחשוב בסביבות השונות, לרבות מערכות תומכות קריטיות; פעילות מול לקוחות, לרבות התקנים שבשימוש הלקוחות; גישה מרחוק; שירותי העברת הודעות; ניהול הרשאות וזהויות; עבודה עם שותפים עסקיים וספקי שירותים, לרבות ערוצי העברת מידע ונתונים; תרבות ארגונית ומודעות עובדים; נוכחות מקוונת (Online Presence) לרבות בנקאות ישירה/בתקשורת ושימוש ברשתות חברתיות, והמשכיות עסקית.

45. ממצאים מהותיים שנתגלו בעקבות או במהלך פעולות הערכת בקורות הגנת הסייבר ידווחו להנהלה והדירקטוריון, יחד עם הפקת הלקחים ותכנית לתיקון הממצאים, כאמור בהוראה זו.

#### **דיווח על סיכונים**

46. הדוחות הסדירים המוגשים להנהלה והדירקטוריון בנושאי סיכונים תפעוליים כאמור בהוראת ניהול בנקאי תקין מס' 350, יכללו התייחסות פרטנית לסיכוני הסייבר.

47. דוחות סיכוני סייבר יכללו:

(א) מצב עדכני ומנומק של מדדי סיכוני הסייבר;

(ב) פירוט של אירועי סיכון/נזק משמעותיים בתאגיד ;

(ג) אירועים ונתונים חיצוניים רלבנטיים שיש בהם השפעה פוטנציאלית על התאגיד הבנקאי.



**פרק ה': יעדי בקרה ובקורות הגנת סייבר****כללי**

48. כחלק מניהול הגנת הסייבר, התאגיד הבנקאי יבסס מערך בקורות אפקטיבי להפחתת רמת סיכוני הסייבר.

49. מערך הבקורות יהיה מושתת על שילוב חוצה ארגון של טכנולוגיות, תהליכים, נהלים, ואנשים אשר יאפשרו לתאגיד הבנקאי לצמצם את החשיפה לאיומי הסייבר לרמה הנדרשת.

50. התאגיד הבנקאי ינקוט בצעדים הנדרשים להשגת יעדי הבקורות ולמימוש הבקורות כמפורט בפרק זה.

**אבטחת סביבת הפעילות**

51. התאגיד הבנקאי ימפה את סביבת הפעילות שבה הוא פועל, יזהה את סיכוני הסייבר הכרוכים בפעילותו, ויגדיר מדיניות להתמודדות עם סיכונים אלו, בהתאם לרמת הסיכון ואופי הקשר.

52. במסגרת זו, התאגיד הבנקאי יבחן את מכלול השירותים העסקיים והתפעוליים, לרבות: ספקים, תאגידים קשורים, לקוחות, ספקי תשתית מחשוב ותקשורת, מיקור חוץ, ספקי שירותים (למשל: עו"ד, רו"ח, משרדי פרסום, בתי דפוס וכיו"ב), וגורמי חו"ל.

53. התאגיד הבנקאי יקבע מנגנונים נאותים להגנה על נוכחותו המקוונת (Online Presence) ובפרט, למול הסיכונים הכרוכים בפעילותו ברשתות חברתיות.

54. התאגיד הבנקאי יקבע את הפעולות הנחוצות לוודא, ככל שניתן, שהגורמים הרלבנטיים, לרבות גורמים חיצוניים, נוקטים באמצעים הנדרשים להפחתת חשיפתו לסיכוני סייבר, לרבות ביצוע בדיקות נאותות וניטור באותם גורמים (או גופים) שזוהו כמהותיים לפעילות העסקית התקינה ולאספקת השירותים ברמה הנדרשת.

**הגנת סייבר פרואקטיבית**

55. התאגיד הבנקאי יבסס מערך דינאמי של הגנת סייבר, בעל יכולות פרואקטיביות, בין היתר, ע"י:

(א) מיפוי והכרת הסביבה – ביצוע מיפוי וניתוח עדכניים של הסביבה התפעולית הפנימית והחיצונית בה הוא פועל, על מנת לזהות גורמים, מערכות ותהליכים קריטיים, לרבות נקודות תורפה, חולשות ו/או תלות הדדית ביניהם;

(ב) חיזוי וחקר איומים – איסוף מידע תוך זיהוי וניתוח שוטפים של שיטות ודרכי תקיפה, כוונות ופעילות של גורמי איום במרחב הסייבר, ושיתוף מידע עם גורמים רלוונטיים אחרים לצורך הפקת מידע אופרטיבי, ניתוח תרחישים ו"חשיבה מחוץ לקופסה", אשר יסייעו לחיזוק מערך הגנת הסייבר והסביבה התפעולית כנגד מתקפות פוטנציאליות;

(ג) תמונת מצב עדכנית (Situational Awareness) – תפיסת מצב הגנת הסייבר של התאגיד, בפרק הזמן הנוכחי, אל מול האיומים, ביצוע ניטור מקיף של הסביבה הפנימית

והחיצונית לתאגיד הבנקאי לצורך זיהוי חולשות ו/או איומים ו/או אירועי אבטחה ו/או סממנים לקיומם של אלה, תוך שימוש ביכולות זיהוי שונות - למשל: ניתוח דפוסים, זיהוי אנומאליות, כריית מידע (Big Data Analysis) - ותעדוף של האירועים בהתחשב ברמת הסיכון ופוטנציאל הנזק הגלום בהם, כבסיס לקבלת החלטות אופרטיביות;

(ד) תגובתיות – פיתוח יכולת תגובה מהירה ואפקטיבית לאירוע סייבר וניהולו, על מכלול היבטיו ולאורך כל שלביו, זאת על מנת לצמצם באופן מרבי התרחשות הנזק לתאגיד הבנקאי;

(ה) הטעה, הסטה ועיכוב – שימוש בטכניקות ובטכנולוגיות ייעודיות (כדוגמת "מלכודות דבש" (Honeypots), הסטת תקשורת וכיו"ב) במטרה להטעות ולעכב את התוקף בדרכו לייעד התקיפה ובכדי לאפשר זיהוי וניתוח של כלים ושיטות (Tactics, Techniques and Procedures) בהן עושה התוקף שימוש;

(ו) עמידות סייבר והתאוששות – יכולת לספוג את השלכותיו של שיבוש תפעולי משמעותי כתוצאה מאירוע סייבר, תוך המשך ניהול תהליכים ושירותים חיוניים, ושיקום הפעולות העסקיות לאחר שחל שיבוש כאמור עד לרמה מספקת לצורך מילוי התחייבויות העסקיות;

(ז) חקירה, תחקיר ומיצוי הדין – יכולת לבצע שימור ראיות וניתוח מעמיק של אירועים לצורך איסוף ראיות, הערכת הנזק שנגרם, זיהוי מקורות וגורמים תוקפים, ביצוע תחקיר, הפקת לקחים ושימור ידע. כל זאת, תוך שימוש במנגנונים חוקיים ושיתוף פעולה עם גורמי אכיפה, במידת הצורך, לצורך מיצוי הדין עם האחראים.

### צמצום מעטפת התקיפה (Attack Surface)

56. התאגיד הבנקאי יפעל באופן שוטף לצמצום החשיפה לאיומי סייבר. במסגרת זו, ינקוט התאגיד הבנקאי, בין היתר, בפעולות הבאות: הקשחת מערכות ותשתיות; פיתוח מאובטח; צמצום הרשאות של משתמשים על פי העקרונות של "הצורך לדעת" (Need to Know) והרשאות מינימליות (Least Privileged); בקרה וחסימה של התקנים ניידים; סינון סוגי קבצים נכנסים למערכות התאגיד הבנקאי; חסימת מתחמי כתובות ו/או סוגי רשתות המשמשות כמקור להתקפות.

### הגנה לעומק (Defense in Depth)

57. הגנה לעומק מאופיינת על ידי שימוש בבקורות שונות בנקודות שונות בתהליך, כך שחולשה בבקרה אחת מפוצה על ידי חוזקה של בקרה אחרת. מימוש הגנה לעומק על ידי יישום אבטחה רב שכבתית (Multi-Layer Defense) יכול לחזק באופן משמעותי את האבטחה הכוללת של תהליכים עסקיים, מערכות מידע, מוצרים ושירותים בנקאיים וכן להיות יעיל בהגנה על מידע רגיש ללקוח, מניעת גניבת זהות ומניעת הפסדים כתוצאה משימוש בלתי מורשה.

58. בפריסת ההגנה לעומק התאגיד הבנקאי יתחשב בניתוח סיכוני הסייבר, מצב הבקורות והחשיפות למול האיומים.

#### ראיה תהליכית

59. התאגיד הבנקאי ימפה את תהליכי הגנת הסייבר, יקבע מדדי ביצוע ואינדיקטורים, יעריך את רמת בשלות היישום של התהליכים בתאגיד הבנקאי, יזהה את הנקודות הטעונות שיפור, ויישם את השינויים הדרושים בהתאם לתכנית העבודה.

60. תהליכי הגנת הסייבר רלבנטיים גם לתהליכים חוצי ארגון, לרבות: ניהול סיכוני סייבר, ניהול מחזור חיים של מערכת, ניהול נכסים, תצורה וטלאים (Asset, Configuration and Patch Management); ניהול זהויות (Identity Management); ניטור ובקרה; שיתוף מידע ודיווח; ניהול אירועים ותגובה; ניהול שרשרת אספקה ותלות בגורמי חוץ (Supply Chain); הדרכה ומודעות; ניהול תכנית הגנת הסייבר.

61. התאגיד הבנקאי יעדכן את הערכת בשלות התהליכים אחת לשנה, לכל הפחות.

#### הגורם האנושי

62. מתוך הכרה במרכזיותו של הגורם האנושי במערך הגנת הסייבר, התאגיד הבנקאי יגדיר את הבקורות הנחוצות בהיבטי מיון, גיוס וקליטת כח אדם (לרבות עובדים וספקים), ניהול זהויות, מתן הרשאות, הפרדת רשויות, נידוד, מעבר ועזיבה.

63. התאגיד הבנקאי יגדיר ויישם תכנית הדרכה ומודעות מקיפה לנושאי הגנת הסייבר. התכנית תקיף את מכלול קהלי היעד, לרבות עובדים, מנהלים, מפתחים, מנהלי מערכות ותשתיות, גורמי חוץ, ספקים, לקוחות וכיו"ב. התכנית ותכניה יעודכנו מעת לעת בהתאם לתמונת האיומים ולהערכת הסיכון העדכנית.

#### שיתוף מידע ומודיעין

64. התאגיד הבנקאי יאסוף וינתח מידע רלבנטי, ממקורות פנימיים וחיצוניים, לצורך יצירת תפיסה כוללת ועדכנית של תמונת איום הסייבר והחשיפה של התאגיד הבנקאי למולו, כבסיס לקבלת החלטות מושכלת, תעדוף של דרכי פעולה, וקיום הגנה אפקטיבית בזמן אמת.

65. תמונת האיום וחשיפת הסייבר תיגזר, בין היתר, מהמידע הבא: מיפוי גורמי איום רלבנטיים, בחתך מוטיבציה ויכולות; טכניקות, טקטיקות, תרחישים ואמצעי תקיפה; חולשות, הגדרות מערכת, ו/או פגיעויות שעלולות לשמש כר להתקפות; פעולות שננקטו בעבר בתגובה להתקפה, התקפות שאירעו בעבר (בתאגיד הבנקאי ו/או בסביבת הפעילות); דרכים ואינדיקטורים לגילוי וזיהוי התקפות; דרכי התמודדות עם התקפות.

66. התאגיד הבנקאי ישתף מידע שעשוי לסייע לתאגידים בנקאיים אחרים בהתמודדות מול איומי סייבר.

67. איסוף ושיתוף המידע יתבצע בהתאם להנחיות המפקח ובכפוף לדין.

### ניטור, בקרה וזיהוי אירוע סייבר

68. התאגיד הבנקאי יקיים מערך ניטור ובקרה אפקטיבי, אשר יהיה מאויש באופן רציף (7X24X365), יקבל דיווחים בזמן אמת מהמערכות השונות, לרבות מערכות תפעוליות ועסקיות, יזהה אינדיקטורים להתרחשות אירוע סייבר, ויזום פעילויות דיווח ותגובה במידת הצורך.
69. על אף האמור בסעיף 68 לעיל, המפקח על הבנקים רשאי להתיר, במקרים חריגים, איוש שאינו רציף כאמור, ובלבד שמערך הניטור והבקרה יעבוד בתצורת עבודה המספקת רציפות תפקודית.
70. לצורך זיהוי אירועי סייבר יעשה התאגיד הבנקאי שימוש גם באמצעים לזיהוי חריגות (אנומאליות) ברמה הטכנולוגית (פעילות המערכות) וברמת הפעילות העסקית.
71. התאגיד הבנקאי יקבע את פרק הזמן הנחוץ לשמירת המידע הדרוש לצורך זיהוי אירועים, לרבות אירועים בחתימה נמוכה, כדי לאפשר ביצוע תחקירי אירוע.
72. מערכות הניטור ישולבו עם מערכות אחרות בתאגיד הבנקאי בכדי לאפשר תהליך אפקטיבי של זיהוי וטיפול באירועי סייבר, לרבות: זיהוי אינדיקטורים לפעילות חריגה, אחזור והעשרת מידע, חקירה ותיעוד, ניהול ידע וקבלת החלטות, יצירה וניהול התראות ודיווחים, תקשורת עם גורמים רלבנטיים וביצוע שינויים במערכות בזמן אמת.
73. התאגיד הבנקאי יבחן מעת לעת תרחישי אירוע סייבר לצורך הערכת יכולתו לזהותם, ויעדכן בהתאם את מערך הניטור והזיהוי.

### תגובה וניהול אירוע סייבר

74. בניהול אירוע סייבר יזהה התאגיד הבנקאי את השלב בו נמצא האירוע (ראה סעיף 13 לעיל) וינהלו בהתאם למאפייניו. סיום אירוע סייבר יתקיים רק לאחר סיום הטיפול בכל שלביו.
75. התאגיד הבנקאי יקבע נוהלי דיווח, ניהול, תגובה וסיום של אירוע סייבר ושל התרעה על אירוע סייבר, בהתאם לחומרתו ובהתאם לשלבי הטיפול באירוע.
76. לצורך ניהול אירוע סייבר יקים התאגיד הבנקאי חדר מצב, ויגדיר בראיה משולבת כלל-תאגידית, את קבוצת העובדים אשר יאיישו אותו, את תפקידיהם, סמכויותיהם, גורמי דיווח פנימיים וחיצוניים, דרכי תקשורת, כלי עבודה וכן נוהלי עבודה פרטניים.
77. התאגיד יבצע רישום ומעקב מסודר של אירועים שטופלו והפעולות שנקטו בידי הגורמים הרלבנטיים. בפרט, התאגיד ינהל "יומן אירועים" בו יתועדו, בסמוך ככל הניתן למועד ההתרחשות, מכלול הידיעות, ההחלטות והפעולות שבוצעו בקשר לאירוע סייבר.
78. התאגיד הבנקאי יגדיר מאגר של פעילויות תגובה (כדוגמת שינויי קונפיגורציה, הגבלה ו/או הסטה של תקשורת, פריסה של תוכנות וכיו"ב) בהתאם לתרחישים השונים, ויגדיר את התנאים שבהם יינקטו פעילויות התגובה, את אופן יישומן הפרטני, את בעלי הסמכות

להורות על הפעלתן, את ערוצי היידוע והאישורים הנדרשים, ואת אופן הערכת יעילות התגובה באירוע המסוים שבמסגרתו הופעלה.

79. התאגיד הבנקאי יגדיר סולם של רמות כוננות ופעילויות נדרשות, בהתאם להתראות ולתרחישים השונים, כגון: צפי לביצוע התקפה מאורגנת; כמות וחומרת התקפות שזוהו בתאגיד הבנקאי, במגזר, או במדינה; גילוי חולשה מהותית או זיהוי כלי תקיפה המהווה איום ישיר על התאגיד הבנקאי.

#### תרגולים

80. התאגיד הבנקאי יגדיר תכנית לביצוע תרגולים של מערכי התגובה השונים בתאגיד, תוך התחשבות בסוגי תרגול שונים (דימוי התקפות, "משחקי מלחמה", תרגילים "מועמדים" וכיו"ב) ובהתייחס לגורמים המעורבים (למשל: גורמים טכניים, צוותי ניהול משבר, דרגי מקבלי החלטות, דוברות וכיו"ב).

#### דיווח על אירוע סייבר

81. התאגיד הבנקאי יקיים מערך דיווח פנימי נאות כחלק מניהול סיכונים ואירועי סייבר. במסגרת זו תוגדר מדיניות דיווח מפורטת, שתקבע בין היתר את הגורמים הפנימיים והחיצוניים אליהם יתבצעו הדיווחים, את מתכונתם ואת תדירותם.

82. התאגיד הבנקאי ידווח לפיקוח על הבנקים על אירוע סייבר או על אירוע החשוד כאירוע סייבר, בהתאם להוראת ניהול בנקאי תקין מס' 366 בנושא "דיווח על אירועי כשל טכנולוגי ואירועי סייבר".

#### עדכונים

| חוזר 06 מס' | גרסה | פרטים        | תאריך    |
|-------------|------|--------------|----------|
| 2457        | 1    | הוראה מקורית | 16/3/15  |
| 2643        | 2    | עדכון        | 29/12/20 |

## דיווח על אירועי כשל טכנולוגי ואירועי סייבר

### מבוא ומטרות

1. התאגידים הבנקאיים הינם נדבך מהותי הנחוץ לפעילותו התקינה של הסקטור הפיננסי בישראל. מאחר ומערך טכנולוגיות המידע של התאגידים הבנקאיים מהווה תשתית קריטית לפעילותם העסקית, נדרשים התאגידים הבנקאיים לזהות ולטפל מהר ככל הניתן ובאופן היעיל ביותר באירועי כשל טכנולוגי ואירועי סייבר, תוך שהם ממשיכים לנהל תהליכים ולספק שירותים חיוניים. בהתאם לכך, מדיניות התאגיד הבנקאי ונהליו לטיפול באירועים מסוג זה נדרשים להתייחס בין היתר לתהליך הדיווח לפיקוח על הבנקים.
2. לדיווח על אירועי כשל טכנולוגי ואירועי סייבר לפיקוח על הבנקים יש מספר מטרות וביניהן:
  - 2.1. לוודא כי התאגיד הבנקאי בו מתרחש האירוע מנהל את האירוע בצורה תקינה ולסייע בהתמודדות עם האירוע במידת הצורך.
  - 2.2. לספק את היכולת להעריך תמונת מצב עדכנית על מנת לקבל החלטה מושכלת האם ואילו פעילות הפיקוח על הבנקים נדרש לנקוט.
  - 2.3. זיהוי פוטנציאל לאירוע מערכתי וצמצום השפעת האירוע ככל שניתן על תאגידים בנקאיים נוספים.
  - 2.4. זיהוי התחומים אשר התאגיד הבנקאי או המערכת הבנקאית בכללותה נדרשים לנקוט לגביהם צעדים למניעת הישנות אירועים מסוג זה או צעדים שישפרו את עמידות התאגידים הבנקאיים בעתיד בהתרחשות אירועים מסוג זה.
  - 2.5. הערכות הפיקוח על הבנקים לתרחישים דומים בעתיד בהתבסס על הערכת סיכונים מתאימה למערכת הבנקאית.
  - 2.6. ווידוא תהליך תחקור והפקת לקחים בעקבות האירוע.

### תחולה

3. (א) הוראה זו תחול על התאגידים הבאים כהגדרתם בחוק הבנקאות (רישוי), התשמ"א 1981 (להלן: "תאגיד בנקאי"):
  - (1) תאגיד בנקאי;
  - (2) תאגיד כאמור בסעיפים 11 (א) (א3) ו-(ב3);
  - (3) תאגיד כאמור בסעיף 11 (ב);
  - (4) סולק כהגדרתו בסעיף 36ט;
- (ב) המפקח רשאי לקבוע הוראות מסוימות שונות מאלו המפורטות להלן, שיחולו על תאגיד בנקאי מסוים, או לפטור, במקרים חריגים, תאגיד בנקאי מהוראה מסוימת, כאשר קיימים טעמים מיוחדים שבהם ראה לנכון לעשות כן, ומנימוקים שירשמו.
4. הדיווח יחול על כל תאגיד בנקאי בנפרד, גם אם האירוע מתרחש בו זמנית במספר תאגידים בנקאיים השייכים לקבוצה בנקאית אחת.

## הגדרות

5. בהוראה זו למונחים הבאים תהיה המשמעות כמפורט להלן :

**אירוע כשל טכנולוגי** אירוע, התרחשות או תוצאה שאינם צפויים או שאינם מתוכננים כחלק מהפעילות התקינה של התאגיד הבנקאי ואשר יש להם השפעה משבשת על הפעילות התקינה של מערך טכנולוגיית המידע או של השירותים הניתנים על ידו.

**אירוע כשל טכנולוגי מהותי** אירוע כשל טכנולוגי הגורם לשיבוש פעילות עסקית, תהליך או פונקציה אשר יש להם השפעה חמורה ונרחבת על הפעילות של התאגיד הבנקאי, על השירותים שהוא מעניק ללקוחותיו או על המערכת הבנקאית.

**אירוע סייבר** כהגדרתו בהוראת נב"ת מס' 361 בנושא "ניהול הגנת הסייבר".

**נזק** כהגדרתו בהוראת נב"ת מס' 361 בנושא "ניהול הגנת הסייבר".

**סטטוס האירוע** תיאור השלב בו נמצא האירוע המדווח :

זיהוי – זיהוי קיום אירוע.

ניתוח – איתור מקור האירוע והיקפו.

עצירת החמרה/ הכלה – עצירת החמרת האירוע.

טיפול/ הכרעה - ביצוע פעולות תיקון/ נטרול רכיבי התקיפה שמצויים בתאגיד הבנקאי.

תוקן/ השבה – חזרה לתקינות ולפעילות מלאה.

**שעות עבודה מקובלות** שעות העבודה המקובלות לעניין הוראה זו בלבד הן : ימים א'-ה' שהינם ימי עסקים במערכת הבנקאית, בין השעות 08:00 ל- 18:00.

## סוגי אירועים המחייבים דיווח

6. להלן סוגי אירועים אשר מחייבים דיווח לפיקוח על הבנקים :

6.1. אירוע כשל טכנולוגי מהותי.

6.2. אירוע החשוד כאירוע סייבר, אשר מטופל ברמת מנהל הגנת הסייבר, ואשר הטיפול בו לא הסתיים תוך ארבע שעות ממועד זיהויו הראשוני או תוך שעתיים במידה וכבר ידוע על נזק כלשהו בגינו.

6.3. אירוע סייבר המשפיע על מספר רב של לקוחות ו/או שהינו בעל מאפייני תקיפה חדשים.

6.4. כל אירוע דלף מידע מהותי שלא נכלל בסעיפים 6.1 – 6.3.

## אחריות הדיווח

7. תאגיד בנקאי יקבע חבר הנהלה שבאחריותו קיום האמור בהוראת דיווח זו.

## 8. אחראי דיווחים :

- 8.1. תאגיד בנקאי יקבע אחראי דיווחי אירועי כשל טכנולוגי ואחראי דיווח אירועי סייבר.
- 8.2. כל אירוע כשל טכנולוגי ו/ או אירוע סייבר כאמור בסעיף 6 לעיל ידווח ע"י האחראי לכך מטעם התאגיד הבנקאי אל הפיקוח על הבנקים.
- 8.3. יכולה להתקיים זהות בין שני האחראים המנויים בסעיף 8.1 לעיל, בהתאם להחלטת התאגיד הבנקאי.
- 8.4. ניתן למנות ממלא מקום קבוע לכל אחד מאחראי הדיווח.
9. תאגיד בנקאי יעביר את פרטי האחראים שימונו בהתאם לסעיפים 7 ו- 8 לעיל, לאגף טכנולוגיה וחדשנות בפיקוח על הבנקים ויעדכן אותו בכל שינוי במינויים אלה, לרבות שינוי בפרטיהם.

## אופן הדיווח

### 10. דיווח ראשון על האירוע –

- 10.1. תאגיד בנקאי ידווח דיווח טלפוני עד שעתיים מזיהוי האירוע כאירוע המחייב דיווח בהתאם לסעיף 6 לעיל, ולאחר מכן ישלים דיווח ראשוני בכתב עד 8 שעות ממועד הדיווח הטלפוני. הפיקוח על הבנקים רשאי להאריך או לקצר את המועד האמור לדיווח בכתב בהתקיים נסיבות המצדיקות זאת.
- 10.2. הדיווח הטלפוני יתבצע בכל שעה ובכל יום, ללא תלות בשעות העבודה המקובלות.
- 10.3. הדיווח הטלפוני יועבר, לפי העניין, למנהל/ת יחידת הסדרה וביקורת בתחום טכנולוגיית המידע ו/או למנהל/ת יחידת הסייבר הפיקוחית באגף טכנולוגיה וחדשנות בפיקוח על הבנקים.
- 10.4. היה ומועד הדיווח הראשוני בכתב הינו בשעות שאינן בשעות העבודה המקובלות - הדיווח הראשוני בכתב יועבר עם תחילת שעות העבודה המקובלות של היום העוקב.
11. אירוע כשל טכנולוגי מהותי ידווח כאירוע שקיים בו חשד לאירוע סייבר (בשדה המתאים בטופס הדיווח) כל עוד לא הוכח שאין חשד כאמור.

### 12. דיווחים נוספים במהלך האירוע -

- 12.1. תאגיד בנקאי נדרש לשלוח בכתב, על גבי טופס הדיווח האחרון שנשלח ככתוב לעיל, נתונים מעודכנים על פרטי האירוע לכל הפחות אחת ליום או ככל שיחולו שינויים מהותיים בפרטי האירוע ו/או בהשלכותיו, לרבות הקריטריונים לדיווח המפורטים בסעיף 6. הפיקוח על הבנקים רשאי לאשר בקשת תאגיד בנקאי להפחית את תדירות הדיווח באירוע מסוים, בהתקיים נסיבות המצדיקות זאת. האישור כאמור יעמוד בתוקף כל זמן שלא חל שינוי מהותי בפרטי האירוע או בהשלכותיו.
- 12.2. מבלי לגרוע מהאמור בסעיף 12.1 לעיל, יובהר כי אירוע שדווח על בסיס אחד הקריטריונים המפורטים בסעיף 6 ובהמשך מתברר שעונה על קריטריונים נוספים אינו מחייב דיווח חדש נוסף בגינו, אלא שנדרש לעדכן אודות הקריטריון הנוסף במסגרת הדיווחים השוטפים.



12.3. במקרה בו חלה התפתחות משמעותית באירוע שכבר מצוי בתהליכי דיווח, בשעות שמעבר לשעות העבודה המקובלות, יש לעדכן טלפונית את הגורם האחראי באגף טכנולוגיה וחדשנות בפיקוח על הבנקים (כאמור בסעיף 10.3 לעיל), ולאחר מכן להעביר דיווח בכתב, כנדרש.

### 13. דווח על סיום האירוע -

- 13.1. תאגיד בנקאי נדרש לדווח על סיום האירוע.  
13.2. התאגיד הבנקאי יודא כי הטופס מלא ומכיל את כל הפרטים העדכניים ביותר למועד דיווח סיום האירוע.

### תחקור אירוע

14. תאגיד בנקאי יקבע נוהל תחקיר אירוע, בו ייקבעו בין היתר שיטת התחקיר והגורמים המשתתפים בו.  
15. תאגיד בנקאי יבצע תחקיר בסיום אירוע בהתאם לנוהל שקבע. התחקיר יכלול לכל הפחות את הנושאים הבאים:  
15.1. פרטים סופיים ומעודכנים אודות האירוע ונסיבות התרחשותו (תוך התייחסות לכלל הפרטים שדווחו לפיקוח על הבנקים).  
15.2. דו"ח הפקת לקחים, לרבות המלצות, יישום בקורות פנימיות, לו"ז לביצוע, פירוט הגורמים המעורבים בתחקיר ומאשר התחקיר.  
16. התחקיר יאושר על ידי חבר ההנהלה האחראי על קיום ההוראה, כאמור בסעיף 7 לעיל, ויועבר לפיקוח על הבנקים בתוך עד 45 יום ממועד סיום האירוע או בתוך עד 60 יום ממועד זיהוי האירוע כאירוע המחויב בדיווח לפי סעיף 6 לעיל, לפי המוקדם מביניהם.

### עדכונים

| חוזר 06 מס' | גרסה | פרטים      | תאריך    |
|-------------|------|------------|----------|
| 2643        | 1    | חוזר מקורי | 29/12/20 |