בנק ישראל

הפיקוח על הבנקים

אגף טכנולוגיה וחדשנות

יחידת טכנולוגיה בבנקאות

ירושלים, ה בטבת תשפ״ג

29 בדצמבר 2022

חוזר ח- 06-

לכבוד

התאגידים הבנקאיים וחברות כרטיסי אשראי

הערות לטיוטת ההוראה יש לשלוח לתיבת המייל:

Pikuah_directive_drafts@boi.org.il

הנדון: דיווח על אירועי כשל טכנולוגי ואירועי סייבר

(ניהול בנקאי תקין הוראה מס׳ 366, הוראת דיווח לפיקוח על הבנקים מס׳ 880)

מבוא

1. חוק ״שירות מידע פיננסי״ קובע (סעיף 31. (א) לחוק): ״אירע אירוע אבטחה חמור כמשמעותו בהוראות לפי סעיף 36 לחוק הגנת הפרטיות, יודיע על כך נותן השירות באופן מיידי למאסדר נותן השירות הנוגע בדבר, למקור המידע שאירוע האבטחה אירע לגבי מידע שהתקבל ממנו ולרשם כהגדרתו בסעיף 7 לחוק הגנת הפרטיות (בסעיף זה – הרשם), וכן ידווח למאסדר נותן השירות ולרשם על הצעדים שנקט בעקבות האירוע; קיבל נותן השירות את המידע מנותן שירות אחר שאסף אותו, בהתאם להוראות סעיף 29(א)(3) – יודיע על כך באופן מיידי גם לנותן השירות שממנו קיבל את המידע; קיבל מקור המידע הודעה לפי סעיף קטן זה, ידווח על כך ללא דיחוי למאסדר מקור המידע״.
2. מתוך רצון להקל על התאגידים הבנקאיים בדיווח על מגוון האירועים בהם הם חייבים בדיווח לפיקוח על הבנקים ולאחד אותם, קבע הפיקוח על הבנקים שאופן הדיווח על ״אירוע אבטחה חמור״ לפיקוח על הבנקים כמאסדר מקור המידע, במסגרת פעילותו של התאגיד הבנקאי כמקור מידע או כנותן שירות כאמור בחוק, יהיה בהתאם לקבוע בהוראת נב״ת 366.
3. לאחר התייעצות עם הוועדה המייעצת בעניינים הנוגעים לעסקי בנקאות ובאישור הנגיד, החלטתי על עדכון הוראת ניהול בנקאי תקין מס׳ 366 בנושא ״דיווח על אירועי כשל טכנולוגי ואירועי סייבר״.

התיקונים להוראת ניהול בנקאי תקין מס׳ 366

4. התוסף סעיף 6.6 הקובע כי גם אירוע אבטחה חמור כמשמעותו בסעיף 31 לחוק שירות מידע פיננסי (התשפ״ב-2021), המתרחש אגב פעילותו של התאגיד הבנקאי כמקור מידע או כנותן שירות מידע פיננסי בהתאם לחוק זה, יהיה סוג אירוע המחויב בדיווח לפיקוח על הבנקים באופן המפורט בהוראה.

התיקונים להוראת דיווח לפיקוח על הבנקים מס' 880

5. נוסף בסעיף 15 "סוג אירוע": "5 – אירוע אבטחה חמור בהתאם לסעיף 6.6 בהוראת נב"ת 366".

תחילה והוראות מעבר

6. תחילת התיקונים להוראה החל מיום פרסומם.

עדכון הקובץ

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

להוציא עמוד	**להכניס עמוד**

בכבוד רב,

יאיר אבידן

המפקח על הבנקים

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. היערכות 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) (3א) ו-(3ב);
   (3) תאגיד כאמור בסעיף 11 (ב);
   (4) סולק כהגדרתו בסעיף 36ט;

   (ב) בטל.
4. חובת הדיווח תחול 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 8:00 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 של התאגיד הבנקאי, 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.

6.5. אירוע כאמור בסעיפים 6.1 – 6.4 לעיל, המתרחש בתאגיד שבשליטת תאגיד בנקאי שהוא עצמו אינו תאגיד בנקאי, ויש לו השפעה מהותית, בין היתר, בהיבטי טכנולוגיה, מוניטין ופיננסים, על התאגיד הבנקאי השולט בו, על הקבוצה הבנקאית או על המערכת הבנקאית.

6.6. אירוע אבטחה חמור כמשמעותו בסעיף 31 לחוק שירות מידע פיננסי, (התשפ"ב -2021), המתרחש אגב פעילותו של התאגיד הבנקאי כמקור מידע או כנותן שירות מידע פיננסי בהתאם לחוק זה.

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. **דווח 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 שעות 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 מסויים, 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 יוודא 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. הנוהל יתייחס גם למקרה בו התרחש אירוע בתאגיד שבשליטת תאגיד בנקאי שהוא עצמו אינו תאגיד בנקאי.

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 בקרות 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
2669	2	עדכון	30/09/21
2680	3	עדכון	24/11/21

דיווח על אירועי כשל טכנולוגי ואירועי סייבר

תחולה

1. הוראה זו חלה על התאגידים המנויים בסעיף 3(א) להוראת נוהל בנקאי תקין מס' 366 "דיווח על אירועי כשל טכנולוגי ואירועי סייבר".
2. הדיווח יחול על כל ישות בנפרד, גם אם האירוע מתרחש בו זמנית במספר תאגידים בנקאיים השייכים לקבוצה בנקאית אחת.

הרכב הדוח

3. הרכב הדוח:
לוח 01 – "דיווח על אירועי כשל טכנולוגי ואירועי סייבר"

דרך הדיווח

4. הדיווח הטלפוני יהיה לממונה האגפי כמפורט בנב"ת 366 "דיווח על אירועי כשל טכנולוגי ואירועי סייבר".
5. הדיווח על לוח 01 יהיה באמצעות תקשורת מקוונת, בטכנולוגיה המאובטחת, המשמשת את בנק ישראל לדיווחים.

הגדרות

6. משמעות כל מונח בהוראה זו יהיה כהגדרתו בהוראת ניהול בנקאי מס' 366 "דיווח על אירועי כשל טכנולוגי ואירועי סייבר".

אופן ומועדי הדיווח

7. **תהליך הדיווח יהיה כמפורט בזאת:**

7.1 **דיווח טלפוני**

דיווח טלפוני בתוך שעתיים מזיהוי האירוע כאירוע המחייב דיווח כהגדרתו בנב"ת 366 סעיף 6. הדיווח הטלפוני יתבצע ללא תלות בשעות העבודה המקובלות.

7.2 **דיווח ראשוני**

בתוך 8 שעות ממועד הדיווח הטלפוני יישלח דיווח בהתאם לפורמט לוח 01, עם כל המידע הידוע נכון למועד הדיווח.

7.3 **עדכון הדיווח**

7.3.1 ככל שיחולו שינויים מהותיים בפרטי האירוע, ולכל הפחות אחת ביום, יועבר דיווח מעודכן. גם אם לא חל שינוי בפרטי האירוע יש לדווח את המידע המעודכן ביותר נכון לאותו מועד אחת ליום.

7.3.2 הדיווח יתבצע בשעות העבודה המקובלות.

7.4 **דיווח על סיום האירוע**

7.4.1 עם סיום האירוע כהגדרתו על ידי הבנק, יישלח דיווח מעודכן עם כל המידע הידוע לאותו מועד.

7.4.2 לאחר קבלת דיווח על סיום אירוע, אחראי הדיווח מהפיקוח על הבנקים ישלח אישור על קבלת דיווח על סיום אירוע.

הנחיות כלליות

8. חובת דיווח חלה על כל אחד מסוגי האירועים הבאים המפורטים בנב"ת 366 בסעיף 6.
9. הנתונים המדווחים בכל אחד מהדיווחים יהיו מעודכנים, ככל שניתן, למועד הדיווח.
10. בדיווח על סיום אירוע - נתונים שאינם ידועים נכון לסיום האירוע ידווחו כ"טרם ידוע", ונתונים שאינם רלוונטיים ידווחו כ"לא רלוונטי".
11. יש לדווח באופן מצטבר כך שבכל דיווח יופיע המידע המצטבר המעודכן ביותר למועד הדיווח.

הנחיות ללוח 01

12. בכל סעיף בו נדרש לדווח על תאריך, הפורמט יהיה: DD/MM/YYYY.
13. בכל סעיף בו נדרש לדווח על שעה, הפורמט יהיה: HH:MM
14. בשורה 08 בסעיף "מספר האירוע" – יש לדווח את המס' המזהה של האירוע כפי שניתן על ידי האחראי על הדיווח בפיקוח על הבנקים. הדיווח הראשוני ישלח ללא מספר מזהה של האירוע, ולאחר קבלת מספר מזהה יש לדווח עליו בכל הדיווחים הנוספים בגין אותו אירוע.
15. בשורה 10 בסעיף " סוג האירוע" - יש לבחור בערך אחד או יותר, מתוך רשימת הערכים הבאה:
    1 – אירוע כשל טכנולוגי מהותי
    2 – אירוע סייבר העונה לקריטריונים בסעיף 6.2 בהוראת נב"ת 366
    3 – אירוע סייבר בעל השפעה רבה או מאפייני תקיפה חדשים
    4 – אירוע דלף מידע מהותי
    5 – אירוע אבטחה חמור בהתאם לסעיף 6.6 בהוראת נב"ת 366
16. בשורה 11 בסעיף "מס' סידורי של הדיווח" – יש לדווח את המס' הסידורי של הדיווח בגין אותו אירוע.

17. בשורה 12 בסעיף "סטטוס האירוע" - יש לבחור בערך אחד או יותר, מתוך רשימת הערכים הבאה:
    1 - זיהוי
    2 - ניתוח
    3 - עצירת החמרה/ הכלה
    4 - טיפול/ הכרעה
    5 - תוקן/ השבה
18. בשורה 20 בסעיף "האם האירוע חשוד כאירוע סייבר?" – רשימת בחירה עם הערכים: כן/לא. יש לבחור "לא" כאשר קיימת וודאות כי אין מדובר באירוע סייבר.
19. בשורה 21 בסעיף "האם האירוע דווח לרגולטורים אחרים" – רשימת בחירה עם הערכים כן/ לא.
20. בשורה 23 בסעיף "מס' אירוע קודם" – אם מדובר בהמשך של אירוע שהתרחש בעבר יש לציין מספר אירוע קודם.
21. בשורה 24 בסעיף "האם האירוע פורסם?" – רשימת בחירה עם הערכים: כן/לא.
22. בשורה 25 בסעיף "פרסום האירוע – פירוט" - יש לתת מידע נוסף כגון: מועד הפרסום, אמצעי הפרסום וכו'.
23. בשורה 26 בסעיף "תיאור האירוע" - יש לתת תיאור כללי של האירוע, ככל שידוע נכון למועד הדיווח.
24. בשורה 27 בסעיף "הערכת חומרת האירוע" – רשימת בחירה עם הערכים: 1-4. יש להעריך את חומרת האירוע נכון למועד הדיווח, כאשר 1- רמת חומרה נמוכה , ו- 4 – רמת חומרה גבוהה מאוד.
25. בשורה 28 בסעיף "תפקודים שנפגעו" – יש לפרט את הפונקציונליות / תהליכים עסקיים, לרבות מערכות מעורבות, שנפגעו כתוצאה מהאירוע. אם קיים חשש לפגיעה נוספת יש לפרט גם אותו.
26. בשורה 30 בסעיף "הגורם המזהה" - יש לציין את הגורם שזיהה את האירוע לראשונה, כגון: לקוח, התרעת מערכת וכו'.
27. בשורה 31 בסעיף "מקור האירוע" יש לתת מידע על הגורם שבגינו נגרם האירוע.
28. שורות 32- 39 ידווחו רק בגין אירוע סייבר.
29. בשורה 32 בסעיף "סוג התוקף" - יש לבחור מתוך רשימה בחירה אחד או יותר מהערכים הבאים:
    1 - עובד פנימי
    2 – ספק
    3 - גורמי פשע
    4 - גורמי טרור
    5 – ארגוני אקטיביזם
    6 - מדינה
    7 - לא ידוע

8 - אחר

30. בשורה 34 בסעיף "תיאור תרחיש התקיפה" – יש לתאר את תרחיש התקיפה, לרבות שיטת החדירה (וקטור התקיפה), ערוץ התקיפה ופרטים נוספים לגבי התקיפה.

31. בשורה 35 "מאפייני תקיפה חדשים" יש לפרט במידה ונעשה שימוש במאפייני תקיפה חדשים מנקודת ראות הבנק.

32. בשורה 36 בסעיף "מעורבות שרשרת אספקה" – רשימת בחירה עם הערכים: כן/לא. כאשר התשובה בסעיף 36 היא "לא" סעיפים 37 – 39 לא ימולאו. המונח שרשרת אספקה כמשמעותו בהוראת ניהול בנקאי תקין מס' 363.

33. בשורה 39 בסעיף "האם מדובר בספק מהותי?" – רשימת בחירה עם הערכים כן/לא.

34. בשורה 40 בסעיף "סוג הנזק" - יש לבחור מתוך רשימה סגורה את סוג הנזק (ניתן לבחור יותר מערך אחד

1 – שירות

2 – כספי/ פגיעה בנכסים

3 – מידע/ איסוף מודיעין

4 – מוניטין/ אמון הציבור

5 – ציות

6 – משפטי

7 – אחר

35. בשורה 41 בסעיף "תיאור הנזק" – יש לפרט את הנזקים כולל נזק כספי.

36. בשורה 42 בסעיף "אומדן נזק פוטנציאלי" – יש לפרט את כל הנזקים הפוטנציאלים כולל אומדן נזק כספי פוטנציאלי.

37. בשורה 44 "האם ניתן שיפוי מלא ללקוחות?" – רשימת בחירה עם הערכים: כן/לא.

38. בשורה 45 בסעיף "פירוט פעולות שבוצעו" – יש לפרט את הפעולות שננקטו ע"י הישות במסגרת האירוע (כולל workaround) לפי סדר כרונולוגי.

39. בשורה 48 בסעיף "גורמים פנימיים אליהם דווח האירוע" יש לבחור ערך אחד או יותר מתוך רשימת הערכים הבאים:

1- יו"ר דירקטוריון

2- דירקטוריון

3- מנכ"ל

4- CRO

5- CIO

6- מנהל הגנת סייבר

7- מנהל אבטחת מידע

8- מנהל תפעול

9- מנהל המשכיות עסקית

10- דוברות

11- מנהל תשתיות

12- אחראי ביטחון פיזי

13- מחלקה משפטית

14- סמנכ"ל היחידה העסקית הרלוונטית

15- אחר.

40. בשורה 49 בסעיף "גורמים חיצוניים אליהם דווח האירוע" ובשורה 50 בסעיף "גורמים חיצוניים מעורבים בטיפול באירוע" יש לבחור מתוך רשימה בחירה, אחד או יותר מהערכים הבאים:

1 - משטרה

2- Cert לאומי

3- הרשות להגנת הפרטיות (רל"פ)

4- בורסה

5- אחר

דיווח על אירועי כשל טכנולוגי ואירועי סייבר

לוח 01

פרטי התאגיד המדווח		
01	שם הישות המדווחת	
02	מס' הישות המדווחת	
03	תאריך הדיווח	
04	שעת הדיווח	
05	שם פרטי ושם משפחה של ממלא הדיווח	
06	מס' טלפון נייד	
07	מס' טלפון נוסף	
פרטי האירוע		
08	מס' האירוע	
09	שם האירוע	
10	סוג האירוע	
11	מס' סידורי של הדיווח	
12	סטטוס האירוע	
13	תאריך האירוע	
14	שעת האירוע	
15	תאריך זיהוי האירוע	
16	שעת זיהוי האירוע	
17	שם פרטי ושם משפחה של מקבל הדיווח הטלפוני (בפיקוח על הבנקים)	
18	תאריך דיווח ראשוני	
19	שעת דיווח ראשוני	
20	האם האירוע חשוד כאירוע סייבר?	
21	האם האירוע דווח לרגולטורים אחרים?	
22	פירוט רגולטורים אחרים אליהם דווח האירוע	
23	מס' אירוע קודם	
24	האם האירוע פורסם ?	
25	פרסום האירוע - פירוט	
תיאור האירוע		
26	תיאור האירוע	
27	הערכת חומרת האירוע	
28	תפקודים שנפגעו	
29	השפעת האירוע על משתמשים/ תחום/שירות	
30	הגורם המזהה	
31	מקור האירוע	

הרחבת מידע לאירוע סייבר		
32	סוג התוקף	
33	סוג התוקף - פירוט	
34	תיאור תרחיש התקיפה	.
35	מאפייני תקיפה חדשים	
36	מעורבות שרשרת אספקה	
37	פרוט מעורבות שרשרת אספקה	
38	שם הספק	
39	האם מדובר בספק מהותי?	
הערכת הנזק		
40	סוג הנזק	
41	תיאור הנזק	
42	אומדן נזק פוטנציאלי	
43	מספר לקוחות וחשבונות שנפגעו	
44	האם ניתן שיפוי מלא ללקוחות?	
ניהול האירוע		
45	פירוט פעולות שבוצעו	
46	פירוט פעולות מתוכננות, כולל לו"ז מתוכנן	
47	האם הופעל נוהל חרום ? (לפרט)	
48	גורמים פנימיים אליהם דווח האירוע	
49	גורמים חיצוניים אליהם דווח האירוע	
50	גורמים חיצוניים מעורבים בטיפול באירוע	
51	הערכת זמן לסיום האירוע	
סיום האירוע		
52	תאריך סיום האירוע	
53	שעת סיום האירוע	