רשות ניירות ערך
Israel Securities Authority
سلطة الأوراق المالية

הוראה לחברות תשלומים בעניין אמצעים טכנולוגיים ואבטחת מידע

הוראה לפי סעיפים 4(א)(2), 5, 23(ב), 27(א)(1)-(2) ו-(4), ו- 43(ב) לחוק הסדרת העיסוק בשירותי תשלום וייזום תשלום, התשפ"ג-2023 ולפי סעיף 39ד(ב) לחוק שירותי תשלום, התשע"ט-2019

דברי הסבר

חוק הסדרת העיסוק בשירותי תשלום וייזום תשלום, התשפ"ג-2023 (להלן: "**החוק**"), אשר נחקק ביום י"ז בסיוון התשפ"ג, 06.06.2023, ויכנס לתוקף ביוני 2024, הסמיך את רשות ניירות ערך (להלן: "**הרשות**") להעניק רישיונות למתן שירותי תשלום לתאגידים העומדים בדרישות הקבועות בחוק (להלן: "**חברת תשלומים**"), ולפקח על חברות תשלומים, לפי החוק.

עוד הסמיך החוק את הרשות לקבוע הוראות לחברות תשלומים בנושאים שונים, ביניהם הוראות בעניין מנגנונים נאותים ומתקדמים לאבטחת מידע, ניהול סיכונים, הגנת סייבר, והמשכיות עסקית, לרבות בעניין חובת מינוי בעלי תפקידים שיהיו ממונים על אבטחת מידע, ניהול הסיכונים והגנת סייבר, ובעניין קביעת תנאי כשירות ודרישות הכשרה בעבורם, לפי סעיף 23(ב) לחוק. כמו כן, אחד התנאים למתן רישיון שירותי תשלום, לפי סעיף 4(א)(2) לחוק, הוא שלמבקש יש אמצעים טכנולוגיים מתאימים לשם מתן שירות התשלום ומיומנות בהפעלתם, באופן שיבטיח את אמינות המערכות שבאמצעותן יינתנו השירותים ואת קיום ההוראות לפי החוק ולפי חוק שירותי תשלום, התשע"ט-2019 (להלן: "**חוק שירותי תשלום**").

מטרת הוראה זו להסדיר את הדרישות שיחולו על חברות תשלומים, בקשר עם פעילותן כחברות תשלומים, בעניין אמצעים טכנולוגיים, ניהול סיכוני טכנולוגיית מידע, אבטחת מידע, הגנת סייבר והמשכיות עסקית.

ההוראה מתבססת על דרישות החוק, וכן על האסדרה האירופאית בנושא ניהול סיכוני טכנולוגיות מידע ואבטחת מידע שחלה על נותני שירותי תשלום בהתאמות הנדרשות[1]. זאת, בהמשך להתבססות החוק על עקרונות האסדרה של שתי הדירקטיבות האירופאיות המסדירות את תחום שירותי התשלום והייזום הבסיסי באירופה – ה-PSD2[2] וה-EMD[3].

פעילות שירותי תשלום מתאפיינת בשימוש נרחב באמצעים אלקטרוניים ונעשית כיום ברובה באופן מקוון – לדוגמה, באמצעות שימוש בקווים אינטרנטיים, ניידים ואלחוטיים, ורשתות. זאת ועוד, שירותי תשלום מלווים, לעיתים קרובות, בהתקשרויות עם גופים שונים מהמגזר הפיננסי, כמו גם

[1] בפרט ראו: EBA Guidelines on ICT and security risk management under the Directive 2015/2366/EU (PSD2) (EBA/GL/2019/04) ו- EBA Guidelines on Authorisations of Payment Institutions under PSD2 (EBA-GL-2017-09).

[2] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market.

[3] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions.

עם צדדים שלישיים. לאור זאת, הפעילות האמורה חשופה לסיכוני טכנולוגיית מידע ואבטחת מידע (להלן: "**סיכוני טכנולוגיית מידע**"), כולל להתקפות סייבר. לפיכך, ההוראה מחייבת את חברות התשלומים לנהל את הסיכונים האמורים ולנקוט באמצעים נאותים לצמצומם ככל הניתן.

ההוראה קובעת מודל הכולל שלושה מעגלי בקרה שמטרתם לוודא הגשמת תכליות הוראה זו. מעגל הבקרה הראשון כולל את בעלי התפקידים בחברה העוסקים בתחום טכנולוגיית המידע אשר אמונים על המערכות, התהליכים ופעילויות אבטחת המידע (למשל יחידות טכנולוגיית המידע והתפעול); מעגל הבקרה השני כולל את הממונה על אבטחת מידע והגנת סייבר; ומעגל הבקרה השלישי כולל את המבקר. לצד המעגלים לעיל חלה אחריות כוללת בנושא סיכוני טכנולוגיית מידע על דירקטוריון חברת התשלומים אשר נדרש לאשר ולפקח אחר יישומן של דרישות הוראה זו בחברת התשלומים. עוד יודגש כי ההוראה קובעת מהם התהליכים, הנהלים ויתר המסמכים הנדרשים לחברות תשלומים לצורך עמידה בדרישותיה. עם זאת, הדגש הניתן בהוראה הוא על הטמעה, יישום וניטור אחר נאותות היישום של אותם מסמכים, כך שחברת התשלומים אינה יכולה להסתפק בכתיבתם של המסמכים הנדרשים בלבד.

ההוראה המוצעת כוללת את הפרקים הבאים:

- פרק א' מפרט את ההגדרות הרלוונטיות לצורך ההוראה;
- פרק ב' מתמקד בממשל התאגידי ובדרישה לחלוקה ברורה של האחריות אצל חברת התשלומים, לרבות אחריות הדירקטוריון בנושא סיכוני טכנולוגיית מידע;
- פרק ג' עוסק בחובה של חברת תשלומים להכין אסטרטגיית טכנולוגיית מידע, אשר הולמת את האסטרטגיה העסקית הכוללת של חברת התשלומים;
- פרק ד' עוסק בחובת חברת התשלומים לנהל ולהפחית את סיכוני טכנולוגיית המידע באמצעות ממונה אבטחת מידע עצמאי ואובייקטיבי. כמו כן, חברת תשלומים נדרשת לתחזק מיפוי עדכני של התהליכים העסקיים, תהליכים תומכים ונכסי מידע ולסווג אותם במונחים של חיוניות, בהתבסס על סודיות, אמינות וזמינות של מידע. בהמשך לכך, חברת תשלומים נדרשת להעריך את הסיכונים התפעוליים הקשורים לסיכוני טכנולוגיית מידע שמשפיעים עליה, וכן להחליט אילו אמצעים נדרשים כדי לצמצם את הסיכונים שזוהו. במסגרת ההוראה המוצעת תידרש חברת התשלומים לוודא את האפקטיביות של האמצעים לצמצום סיכונים בהם היא נוקטת, כפי שהוגדרו במסגרת ניהול הסיכונים שלה, זאת בפרט כאשר היא נעזרת בספקי מיקור חוץ. אמצעים להפחתת סיכונים בקשר לספקי מיקור חוץ כאמור, ייקבעו במסגרת הסכמים והסדרי רמת שירות (Service Level Agreements), ואולם על חברת התשלומים לפקח, לנטר ולוודא את עמידתם של אותם ספקי מיקור חוץ בהסכמים והסדרי רמת השירות;
- פרק ה' קובע את הדרישות בקשר עם אבטחת מידע כשהמידע מוחזק (held) במערכות טכנולוגיית מידע (ICT systems), לרבות דרישות ליישום אמצעי אבטחת מידע אפקטיביים; הכנה ויישום של מדיניות אבטחת מידע; הטמעה ובדיקת אמצעי אבטחת במידע; והכנת תכנית הדרכות לעובדי חברת התשלומים וספקי מיקור חוץ;

- פרק ו' מתייחס לעקרונות כלליים לגבי ניהול פעולות טכנולוגיית מידע, כולל דרישות לשפר, ככל האפשר, את היעילות של פעולות טכנולוגיית המידע; יישום נהלי תיעוד (logging) וניטור (monitoring) בעניין פעולות טכנולוגיית מידע חיוניות; תחזוקה ועדכון של רשימת נכסי טכנולוגיית מידע; ניטור וניהול מחזור החיים של נכסי טכנולוגיית מידע (the life cycle of ICT assets); ויישום של נהלים בעניין גיבוי ושחזור מידע ומערכות טכנולוגיית מידע וכן בעניין ניהול תקלות ואירועי טכנולוגיית מידע;
- פרק ז' עוסק בדרישות בקשר עם ניהול שינויים בתחום טכנולוגיית מידע, כולל רכישה ופיתוח של מערכות מידע. חברת תשלומים נדרשת לוודא שנערכים לגבי כל שינוי מערכות טכנולוגיית מידע – הערכה ובדיקה, אישור ויישום באופן מבוקר, מתוך מטרה לוודא ששינויים בטכנולוגיית מידע מנוהלים ומפוקחים ושהפיתוח של יישומים מנוטר בזהירות משלב הבדיקות לשלב הייצור;
- פרק ח' עוסק בדרישות בנוגע לניהול המשכיות עסקית ולגיבוש של תכנית תגובה והתאוששות, כולל בחינתה ועדכונה בהתבסס על תוצאות הבחינה. חברת תשלומים נדרשת לוודא שיש לה אמצעי תקשורת יעילים בעת משבר כך שכלל הגורמים הרלוונטיים יוכלו להיות מעודכנים באופן ובזמן ראוי;
- פרק ט' קובע את הדרישות בנוגע לניהול יחסי חברת התשלומים והלקוחות (PSUs – payment service users), כולל דרישות שמטרתן, בין היתר, לזהות הונאות או שימוש לרעה בחשבונות הלקוחות, כדוגמת דרישה לתת ללקוחות המעוניינים בכך התראות לגבי מתן הוראות לביצוע עסקאות או ניסיונות כושלים לתת הוראות לביצוע עסקאות תשלום, וכן דרישה לספק ללקוחות תמיכה בנוגע לשאלות הקשורות לאבטחת מידע והגנת הפרטיות;
- פרק י' עוסק בדרישות שחברות תשלומים יעמדו בהוראות חוק הגנת הפרטיות, התשמ"א-1981 (להלן: "**חוק הגנת הפרטיות**") והתקנות מכוחו, וכן שתקשורת של חברת תשלומים המכילה מידע רגיש מול כל גורם, תעשה בפרוטוקול סטנדרטי ובתעבורה מוצפנת על פי הטכנולוגיות העדכניות הקיימות בשוק. עוד נקבעו בפרק זה, דרישות בעניין תהליך ניטור והגבלת גישה למידע רגיש;
- פרק י"א עוסק בבחינה תקופתית של ההוראה המוצעת לפי חוק עקרונות האסדרה, התשפ"ב-2021, ובמועד תחילתה של ההוראה ביום תחילת החוק.

ביישום ההוראה חברת תשלומים תיקח בחשבון ותשקול לאמץ תקנים בינלאומיים קיימים ושיטות עבודה מומלצים ומובילים (best practice standards) בתחום טכנולוגיית מידע ואבטחת מידע למגזר הפיננסי.

כמו כן, חברת תשלומים תיישם את החובות הקבועות בהוראה זו באופן המתחשב בגודלה, המבנה הארגוני הפנימי שלה, וכן במאפייני השירותים והמוצרים שחברת התשלומים נותנת או מתכוונת לתת, היקפם, מורכבותם ומידת הסיכון בהם.

להלן נוסח ההוראה:

פרק א': הגדרות

1. בהוראה זו –

"**אירוע כשל**" – אסון, השבתה או הפרעה מתמשכת למשאבים חיוניים, כדוגמת מערכות מידע, ובכלל זה שירותי ענן, מערכות תקשורת וכל מערכת המספקת גישה, עיבוד, או אחסון מידע חיוני או רגיש, וכן נזק משמעותי הנגרם לכוח אדם חיוני, מבנים או חומרה, וכפועל יוצא מכך גם לתהליכים העסקיים של חברת התשלומים;

"**אירוע תפעולי או אירוע אבטחת מידע**" (Operational or Security Incident) – אירוע בודד או סדרה של אירועים קשורים, שלא תוכננו על-ידי חברת התשלומים, ושיש להם או עלולה להיות להם השפעה על השלמות, הזמינות, הסודיות או האמינות (Authenticity) של המידע או השירותים;

"**אסטרטגיית טכנולוגיית מידע**" – כמשמעותה בפרק ג' להוראה;

"**הוראת מיקור חוץ**" – הוראה לחברות תשלומים בעניין מיקור חוץ;

"**זמן התאוששות**" ((Recovery Time Objective (RTO) – פרק הזמן המירבי אשר במסגרתו נדרש להשיב לפעילות תקינה מערכת או תהליך שנעשה בהם שימוש כחלק מהפעילות העסקית של חברת תשלומים, בעקבות אירוע כשל;

"**חוק הגנת הפרטיות**" – חוק הגנת הפרטיות, התשמ"א-1981;

"**טכנולוגיית מידע**" (ICT) – טכנולוגיית מידע ותקשורת (Information and Communication Technology);

"**יעד התאוששות**" (Recovery Point Objective (RPO) – הנקודה בזמן, אליה יאוחזר המידע, בקרות אירוע כשל. בפרט, כמות המידע שחברת התשלומים מוכנה לאבד בעקבות אירוע כשל, במונחי שעות עבודה;

"**מבקר**" – כמשמעותו בפרק ב' סימן ג' להוראה.

"**מדיניות אבטחת מידע**" – כמשמעותה בפרק ה' סימן א' להוראה.

"**מידע רגיש**" – כהגדרתו בסעיף 7 לחוק הגנת הפרטיות, התשמ"א-1981;

"**מסגרת ניהול סיכוני טכנולוגיית מידע**" (ICT and security risk management framework) – כמשמעותה בפרק ד' סימן ב' להוראה;

"**מערכות טכנולוגיית מידע**" (ICT systems) – טכנולוגיות מידע ותקשורת (ICT Set-Up) שהוגדרו כחלק ממנגנון או רשת חיבוריות התומכת בפעילות של חברת התשלומים;

"**נכס מידע**" (ICT asset) – מידע, תוכנה או חומרה המשמשים לפעילותו העסקית של חברת תשלומים;

"**סיכוני טכנולוגיית מידע**" (ICT and security risk) – סיכוני טכנולוגיית מידע ואבטחת מידע, ובכלל זה סיכון לאובדן מידע, לרבות במקרים בהם המידע שוכפל אצל אחר, הוצפן בידי אחר, או נמחק על-ידי אחר, וזאת עקב הפרת חובת סודיות, כשל בשלמות מערכות או מידע, חוסר התאמה או חוסר זמינות של מערכות ומידע, או חוסר יכולת לערוך שינויים או התאמות בטכנולוגיית מידע (IT) בתוך זמן סביר ובעלויות סבירות תוך התאמה לנסיבות ולדרישות

העסקיות המשתנות; וכן סיכוני אבטחת מידע הנובעים מתהליכים או אבטחת מידע פיזית לא מספקים או כושלים, או מאירועים חיצוניים לרבות תקיפות סייבר;

"**ספק מיקור חוץ**" או "**ספק**" – כהגדרת "ספק מיקור חוץ" בהוראת מיקור חוץ;

"**צד שלישי**" – אדם בעל יחסים עסקיים או הסכמיים עם חברת התשלומים שמטרתם לספק מוצר או שירות;

"**שירותי טכנולוגיית מידע**" (ICT services) – שירותים המסופקים על-ידי מערכות טכנולוגיות מידע למשתמש אחד או יותר, פנימי או חיצוני לחברת התשלומים, ובכלל זה הזנת נתונים, אחסון נתונים, שירותי עיבוד ודיווח, שירותי ניטור ושירותי תמיכה עסקית;

"**תיאבון לסיכון**" (Risk Appetite) או "**רמת סיכון**" – רמת סיכון מצרפית, לרבות התייחסות לסוגים של סיכונים, שחברת תשלומים מעוניינת לספוג במסגרת מערך הסיכונים שלה (Risk Capacity) בהתאם למודל העסקי שלה, כדי להשיג את יעדי אסטרטגיית טכנולוגיית המידע שלה, בכפוף לציות מלא להוראות הדין החלות עליה;

"**תכנית בקרה**" – כמשמעותה בסעיף 6 להוראה;

"**תכנית ביקורת**" – כמשמעותה בסעיף 7(ב) להוראה;

"**תכנית המשכיות עסקית**" (Business Continuity Plan, BCP) – כמשמעותה בפרק ח' סימן ג' להוראה;

"**תקנות הגנת הפרטיות**" – תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

פרק ב': ממשל תאגידי

<u>סימן א': הדירקטוריון</u>

2. דירקטוריון החברה אחראי לפקח על נאותות הממשל התאגידי של חברת התשלומים, ובכלל זה:
   א. לגבש ולאשר אסטרטגיית טכנולוגיית מידע ולפקח אחר קיומה ויישומה, וזאת כחלק מהאסטרטגיה העסקית הכוללת של חברת התשלומים.
   ב. לאשר תכניות ומסמכי מדיניות בקשר לסיכוני טכנולוגיית מידע ולוודא את יישומם באופן יעיל, לרבות הטמעת שינויים משמעותיים בהם ככל שנדרש, כמפורט להלן:
      (1) מסגרת ניהול סיכוני טכנולוגיות מידע;
      (2) מדיניות אבטחת מידע, ונהלים ותהליכים בקשר עם ניהול פעילות טכנולוגיית מידע לפי סעיף 56 להוראה;
      (3) תכנית המשכיות עסקית;
      (4) תכנית בקרה;
      (5) תכנית ביקורת;
   ג. להגדיר בעלי תפקידים ולקבוע חלוקת אחריות בקשר לגורמים העוסקים בתחומים של טכנולוגיית מידע, ניהול המשכיות עסקית ובקרה, לרבות מינוי ממונה אבטחת מידע ואישור התקשרות עם מבקר.

ד. להבטיח כי בעלי התפקידים הרלוונטיים אצל חברת התשלומים, הם בעלי כישורים מספקים על מנת לתמוך באופן שוטף בצרכים התפעוליים של טכנולוגיית המידע ובתהליכי ניהול סיכוני טכנולוגיות מידע, וכן על מנת ליישם את אסטרטגיית טכנולוגיית המידע של חברת התשלומים. בהקשר זה, הדירקטוריון יוודא כי התקציב, המשאבים וכוח האדם המוקדשים להגשמת האמור בסעיף זה – מספקים, בשים לב בין היתר למאפייני חברת התשלומים, צרכיה, גודלה, מורכבות פעילותה והסיכונים הכרוכים בה.

ה. לוודא כי העובדים, לרבות בעלי תפקידים רלוונטיים לתחומים כמפורט בסעיף קטן ד', אצל חברת התשלומים, עוברים הדרכות מספקות, לפחות אחת לשנה, בקשר לסיכוני טכנולוגיית מידע, ולרבות כמפורט בפרק ה', סימן ז' להוראה.

ו. להבטיח כי הדירקטוריון מקבל דיווחים ועורך דיונים לגבי אירועים מהותיים, כפי שיוגדרו על-ידי הדירקטוריון, וזאת, בין היתר, לעניין השפעת האירועים המהותיים, המענה והבקרות הנוספות שהוגדרו כתוצאה מאירועים כאמור, כמפורט בסעיף 67(ג) להוראה.

ז. להבטיח כי הוא מקבל דיווחים ועורך דיון, בנוגע לתוצאות הבחינה של תכנית ההמשכיות העסקית, ניתוח החולשות אשר נמצאו בבחינה ואופן הטיפול בהן לפי סעיף 92 להוראה, הכל לפחות אחת לשנה.

<u>סימן ב' : ממונה על אבטחת מידע והגנת סייבר</u>

3. חברת תשלומים תמנה ממונה על אבטחת מידע והגנת סייבר ("**ממונה אבטחת מידע**") בעל הכשרה וניסיון מתאימים אשר יהיה אחראי למכלול הנושאים הקשורים לניהול סיכוני אבטחת המידע והגנתו, כמפורט בהוראה זו.

4. ממונה אבטחת מידע יהיה בעל ידע וניסיון של שלוש שנים לפחות בניהול רכיבי אבטחה, שיש לו הסמכה אחת או יותר מההסמכות הבאות:

א. CISSP;

ב. CISO;

ג. CISA;

ד. CISM;

ה. בודקי ספקים שעמדו בהצלחה בבחינות הסיום לקורס בודקי תאימות סייבר לשרשרת אספקה ארגונית, מגופים המוכרים על-ידי מערך הסייבר הלאומי;

ו. הסמכה או הכשרה אחרת, בכפוף לאישור הרשות או עובד הרשות שהיא הסמיכו לכך.

5. ממונה אבטחת מידע יהיה:

א. עצמאי, אובייקטיבי, לא יכהן גם כמנהל טכנולוגיית המידע בחברת התשלומים וכן לא ייקח חלק בביצוע ביקורת בחברת התשלומים;

ב. ימונה על-ידי המנהל הכללי, ויפוטר באישור הדירקטוריון;

ג. בעל סמכויות, אחריות ומשאבים לפיקוח, ניטור ובקרה אחר עמידת חברת התשלומים בדרישות החוק, ההוראות מכוחו ובדרישות חוק הגנת הפרטיות ותקנותיו וכן אחר עמידת חברת התשלומים במסגרת ניהול סיכוני טכנולוגיית המידע שהוגדרה, ובכלל זה יפעל להבטיח כי סיכוני טכנולוגיית המידע יזוהו, יימדדו, יוערכו, ינוהלו, ינוטרו וידווחו לגורמים הרלוונטיים.

6. ממונה אבטחת מידע יכין תכנית בקרה שנתית לבחינת עמידת חברת התשלומים בהוראות הדין ובמסגרת ניהול סיכוני טכנולוגיית מידע, כאמור לעיל בסעיף 5(ג), יהיה אחראי על יישומה ויודיע על ממצאיו להנהלת החברה ולדירקטוריון לפחות אחת לשנה.

<u>סימן ג': ביקורת</u>

7. חברת תשלומים תתקשר עם מבקר שיערוך ביקורת עצמאית לגבי פעילות חברת התשלומים, לפי הוראות אלה:

א. לעניין פסקה זו, "מבקר" – מי שמתקיימים בו כל אלה:

(1) בעל ידע, מומחיות וניסיון מספקים בתחומי סיכוני טכנולוגיות מידע, בכלל זה:

(א) בעל ניסיון של שלוש שנים לפחות בביצוע ביקורות טכנולוגיות כאמור בפסקה זו;

(ב) בעל תואר אקדמי הנוגע לעניין, ממוסד להשכלה גבוהה בישראל שהמועצה להשכלה גבוהה מכירה בו;

(ג) בעל הסמכה בביקורת מערכות מידע או באבטחת מערכות מידע שהיא אחת מההסמכות האלה או דומה לה: CRISC; CISA; או רואה חשבון מוסמך בישראל בעל התמחות במערכות מידע;

(2) המבקר או התאגיד שבו הוא עובד או שותף, אינם מצויים בניגוד עניינים או תלות בקשר עם ביצוע הביקורת, למעט קבלת שכר מחברת התשלומים בעד הכנת הביקורת;

(3) בעל היכולת והתשומות המספקות לביצוע תפקידו כמפורט בהוראה זו.

ב. המבקר יערוך ביקורת לפי תכנית ביקורת שנתית (להלן: "**תכנית ביקורת**"), במסגרתה יערוך בחינה עצמאית ובלתי תלויה ויספק הערכה אובייקטיבית לגבי מידת הציות של כלל הגורמים והפעילויות של חברת התשלומים, לרבות בעניין ממשל תאגידי, מערכות ותהליכים הנוגעים להיבטי טכנולוגיית מידע ואבטחת מידע בחברת התשלומים וזאת, אל מול מסמכי מדיניות ונהלים הפנימיים של חברת התשלומים והוראות הדין הרלוונטיות.

ג. תכנית הביקורת וביצועה, לרבות תדירות וסדר עדיפות הנושאים המבוקרים על פיה, תיערך בהתבסס על הערכת סיכוני טכנולוגיות מידע של חברת התשלומים.

ד. תכנית הביקורת תאושר על-ידי דירקטוריון החברה, לרבות שינויים משמעותיים בה.

ה. המבקר יודיע על ממצאי הביקורות שערך לפי תכנית הביקורת, וכן על סטאטוס יישום המלצותיו ותיקון ממצאים מהותיים על-ידי חברת התשלומים, להנהלת החברה ולדירקטוריון, לפחות אחת לשנה.

8. חברת תשלומים תגבש ותישם תהליך מעקב רשמי אחר ממצאי הביקורות ויישום המלצותיהן, לרבות גיבוש הוראות לאימות ותיקון בזמן של ממצאי הביקורת המהותיים.

פרק ג': אסטרטגיית טכנולוגיית מידע

9. אסטרטגיית טכנולוגיית המידע של חברת התשלומים, תתיישב עם האסטרטגיה העסקית הכוללת שלו, ותתייחס בין היתר לנושאים הבאים:
   א. האופן בו טכנולוגיית המידע, לרבות הארכיטקטורה של טכנולוגיית המידע, של חברת התשלומים צריכה להתפתח על מנת לתמוך ולקחת חלק באופן יעיל באסטרטגיה העסקית הכוללת של חברת התשלומים, לרבות ההתפתחות של המבנה הארגוני, שינויים במערכות טכנולוגיית מידע והסתמכות מהותית על צדדים שלישיים.
   ב. יעדי אבטחת מידע ברורים, המתמקדים במערכות טכנולוגיית מידע ובשירותי טכנולוגיית מידע, כוח אדם ותהליכים.
10. חברת תשלומים תגבש תכניות פעולה הכוללות אמצעים שתנקוט ליישום והשגת מטרות אסטרטגיית טכנולוגיית המידע (להלן: "**תכניות הפעולה**"), וכן תוודא כי כלל הגורמים הרלוונטיים, בין אם פנימיים ובין אם חיצוניים, כדוגמת גורמים עימם חברת התשלומים התקשרה בחוזה וספקי מיקור חוץ, מכירים את התכניות כאמור ונוהגים לפיהן.
11. חברת תשלומים תבחן (review) את תכניות הפעולה באופן תקופתי, לפחות פעם בשלוש שנים, על מנת להבטיח את הרלוונטיות והנאותות שלהן, וכן תגבש תהליכים למדידה וניטור אחר היעילות שבה אסטרטגיית טכנולוגיית המידע שלה מיושמת.

פרק ד': ניהול סיכוני טכנולוגיות מידע

<u>סימן א': ארגון ויעדים – כללי</u>

12. חברת תשלומים תזהה את סיכוני טכנולוגיית המידע שלה ותנהל אותם.
13. בעלי תפקידים בתחום טכנולוגיות מידע, כפי שהוגדרו ונקבעו על-ידי הדירקטוריון חברת התשלומים לפי סעיף 2(ג) לעיל, אשר אמונים על המערכות, התהליכים ופעילויות אבטחת המידע, יוודאו קיומם של תהליכים ובקרות נאותים שמטרתם להבטיח כי כלל הסיכונים מזוהים, מנותחים, נמדדים, מנוטרים, מנוהלים, ומדווחים לגורמים הרלוונטיים, וכי אינם חורגים מגדרי תיאבון הסיכון של חברת התשלומים, וכן כי המערכות והשירותים המסופקים על-ידם עומדים בדרישות מדיניות ונהלים פנימיים של חברת התשלומים והוראות הדין הרלוונטיות.

<u>סימן ב': ארגון ויעדים – מסגרת ניהול סיכוני טכנולוגיית מידע</u>

14. חברת תשלומים תמנה בעלי תפקידים, ותגדיר תחומי אחריות ועקרונות דיווח אשר יבטיחו את אפקטיביות מסגרת ניהול סיכוני טכנולוגיות מידע. מסגרת זו תוטמע באופן מלא בתהליך ניהול הסיכונים הכולל של חברת התשלומים, ותהיה תואמת לתהליך כאמור.
15. מסגרת ניהול סיכוני טכנולוגיות המידע תכלול פירוט כדלהלן:
   א. מהו תיאבון הסיכון בהיבטי טכנולוגיית מידע ואבטחת מידע, בהתאם לתיאבון הסיכון הכולל של חברת התשלומים.

ב. זיהוי, סיווג חיוניות והערכת סיכוני טכנולוגיית מידע אליהם חשופה חברת התשלומים, כמפורט בסימנים ג'-ה' לפרק זה.

ג. הגדרת צעדים לצמצום סיכוני טכנולוגיית מידע, לרבות בקרות רלוונטיות, כמפורט בסעיפים בסימן ו' לפרק זה.

ד. מנגנון ניטור אחר היעילות של הצעדים כאמור בסעיף קטן (ג), וניטור אחר היקף הדיווחים על אודות אירועי אבטחת מידע ואירועים אחרים אשר השפיעו על מערכות ותהליכי טכנולוגיית המידע אצל חברת התשלומים.

ה. פעולות לתיקון וייעול הצעדים כאמור בסעיף קטן (ג), ככל שנדרש.

ו. דיווח לדירקטוריון על אודות סיכוני טכנולוגיית מידע רלוונטיים שזוהו על-ידי חברת התשלומים, תוצאות תהליכי הערכת הסיכונים ופעולות לצמצומם, לרבות תהליכי הבקרה הקיימים בהקשר זה.

ז. זיהוי והערכה האם מתקיימים סיכוני טכנולוגיית מידע חדשים כתוצאה משינויים משמעותיים במערכות טכנולוגיית המידע ותהליכיה, משינויים בנהלים ובתהליכים קשורים, או כתוצאה מאירועים תפעוליים או אירועי אבטחת מידע.

16. חברת תשלומים תוודא כי מסגרת ניהול סיכוני טכנולוגיות מידע, תהיה מתועדת ומעודכנת באופן שוטף, וזאת בהתבסס על תובנות העולות מיישום המסגרת וניטורה.

17. מסגרת ניהול סיכוני טכנולוגיית מידע תיבחן ותאושר, לכל הפחות אחת לשנה, על-ידי הדירקטוריון.

<u>סימן ג': זיהוי תהליכים עסקיים, תהליכים תומכים ונכסי מידע</u>

18. חברת תשלומים תזהה, תגבש ותתחזק מיפוי עדכני של התהליכים העסקיים והתהליכים התומכים אצלה, שעשויים להיות מושפעים מסיכוני טכנולוגיית מידע, במטרה לזהות את החשיבות של כל אחד מהתהליכים האמורים ואת התלות ההדדית שלהם.

19. חברת תשלומים תזהה, תגבש ותתחזק מיפוי עדכני של נכסי המידע התומכים בתהליכים העסקיים ובתהליכים התומכים, כגון: מערכות מידע ותקשורת, צוותים רלוונטיים, ספקים וקבלנים, צדדים שלישיים ותלות במערכות ותהליכים פנימיים או חיצוניים אחרים.

<u>סימן ד': סיווג חיוניות של תהליכים עסקיים, תהליכים תומכים ונכסי מידע</u>

20. בהתבסס על זיהוי התהליכים העסקיים, התהליכים התומכים ונכסי המידע, כאמור בסימן ג' לפרק זה, חברת תשלומים תסווג את התהליכים העסקיים, התהליכים התומכים ונכסי המידע בהתאם למידת החיוניות שלהם לפעילותה; סיווג חיוניות נכסי המידע, תתבסס, בין היתר, על המידה שבה הנכסים תומכים בפעילויות ובתהליכים העסקיים החיוניים שלה. כמו כן, לצורך סיווג חיוניות התהליכים העסקיים, התהליכים התומכים ונכסי המידע כאמור, חברת תשלומים תשקול, בין היתר, את דרישות הסודיות, אמינות והזמינות הרלוונטיות, לרבות לצורך עמידה בהסכם שנקבע עם הלקוחות.

<u>סימן ה': הערכה וניטור סיכונים</u>

21. חברת תשלומים תזהה ותעריך את סיכוני טכנולוגיית המידע אשר משפיעים על התהליכים העסקיים, התהליכים התומכים ונכסי המידע, בהתאם לחיוניותם.
22. הערכת הסיכונים כאמור תבוצע ותתועד בתדירות שנתית, או באופן תדיר יותר ככל שנדרש. הערכת הסיכונים תבוצע גם לאחר כל שינוי ועדכון משמעותי בתשתיות, בתהליכים ובנהלים המשפיעים על התהליכים העסקיים, התהליכים התומכים ונכסי המידע.
23. חברת תשלומים תנטר באופן שוטף אחר האיומים והחולשות הרלוונטיים לתהליכיה העסקיים, התהליכים התומכים ונכסי המידע, ותבחן באופן שוטף את תרחישי הסיכון המשפיעים על תהליכים אלו.

<u>סימן ו': צמצום סיכונים</u>

24. בהתבסס על תהליכי הערכת הסיכונים שיבצע כאמור בסימן ה' לפרק זה, חברת תשלומים תקבע אילו אמצעים נדרשים לשם צמצום סיכוני טכנולוגיות מידע לרמה מקובלת, וכן תבחן אם נדרשים שינויים לתהליכים העסקיים, לבקרות ולמערכות טכנולוגיית מידע ושירותי טכנולוגיית מידע כתוצאה מהערכות הסיכונים כאמור. ככל ששינויים כאמור נדרשים, חברת התשלומים תבחן מהו משך הזמן הנדרש להטמעתם ואת הצורך בנקיטת צעדי ביניים לצמצום סיכוני טכנולוגיות מידע כך שלא יחרגו מגדרי תיאבון הסיכון שהוגדר על ידה.
25. חברת תשלומים תגדיר ותישם אמצעים הנדרשים לשם צמצום סיכוני טכנולוגיית מידע אשר זוהו על-ידה, וכן לשם הגנה על נכסי מידע, בהתאם לסיווג החיוניות שערכה חברת התשלומים לפי סימן ד' לפרק זה.

<u>סימן ז': שימוש בספקי מיקור חוץ</u>

26. מבלי לגרוע מהוראת מיקור חוץ ומכלליות האמור בהוראה זו, גם בעת שימוש בספקי מיקור חוץ המספקים לחברת התשלומים שירות הכרוך בביצוע תהליכים תפעוליים של שירותי תשלום או שירותי טכנולוגיית מידע ומערכות טכנולוגיית מידע, שקשורים בפעילות חברת התשלומים מכוח רישיונה – חברת התשלומים תוודא את יעילותם של האמצעים לצמצום סיכונים כפי שנקבעו במסגרת ניהול הסיכונים שלה, ובכלל זה האמצעים וההוראות שנקבעו בהוראה זו, בין היתר, בעניין אבטחת מידע פיזית.
27. על מנת להבטיח את המשכיות פעילותם של מערכות טכנולוגיית מידע ושירותי טכנולוגיית מידע, חברת תשלומים תוודא כי החוזים והסכמי רמת השירות (Service Level Agreements), הן במהלך העסקים הרגיל והן בעת התרחשות אירועים, מול ספקי מיקור החוץ כאמור בסעיף 26 להוראה זו, כוללים את הנושאים הבאים:
    א. יעדים וצעדים נאותים ופרופורציונאליים לניהול סיכוני אבטחת מידע, לרבות דרישות מינימום בעניין הגנת סייבר, מפרטי מחזורי החיים של המידע (data life cycle) והנתונים של חברת התשלומים, דרישות הנוגעות להצפנת מידע, אבטחת רשתות ותהליכי ניטור אבטחת מידע, והמיקום של מרכזי הנתונים (Data Centers), וכן תוודא שקיימת הלימה

בין החוזים והסכמי רמת השירות מול הספקים כאמור, לבין יעדי שירות של חברת התשלומים מול לקוחותיה ויעדי התאוששות שלה.

ב. נהלים לטיפול באירועים תפעוליים ואירועי אבטחת מידע, לרבות בהתייחס להיבטי הסלמה (escalation) ודיווח.

28. חברת תשלומים תנטר אחר רמת העמידה של ספקי מיקור החוץ, כאמור בסעיף 26 להוראה זו, ביעדי אבטחת המידע והביצועים של חברת התשלומים, כפי שנקבעו בחוזים והסכמי רמת השירות שערכה מולם, ותוודא כי הם עומדים ביעדים כאמור.

פרק ה': אבטחת מידע

<u>סימן א': מדיניות אבטחת מידע</u>

29. חברת תשלומים תגבש ותתעד מסמך מדיניות אבטחת מידע, במסגרתו תגדיר את העקרונות והכללים המרכזיים לשמירה על סודיות, אמינות וזמינות המידע והנתונים שלה ושל לקוחותיה.
30. מדיניות אבטחת המידע תבטיח את הסודיות, האמינות והזמינות של נכסי המידע הלוגיים (לרבות לפי סימן ב' להלן) והפיזיים (לרבות לפי סימן ג' להלן) החיוניים של חברת התשלומים, של המקורות ושל המידע הרגיש של חברת התשלומים, בעת אחסונו, בעת העברתו ובעת שימוש בו.
31. מדיניות אבטחת המידע תעמוד בהלימה ליעדי אבטחת המידע אשר יוגדרו על-ידי חברת התשלומים ותתבסס, בין היתר, על תוצאות תהליכי הערכת הסיכונים הרלוונטיים.
32. מדיניות אבטחת המידע תכלול, בין היתר, את תיאור התפקידים ותחומי האחריות המרכזיים בניהול סיכוני אבטחת מידע בחברת התשלומים, וכן את קביעת הדרישות רלוונטיות בעבור צוותי העובדים, ספקים, תהליכים וטכנולוגיה לעניין אבטחת מידע, וזאת מתוך הכרה כי לעובדים, לרבות בעלי התפקידים של חברת התשלומים, בכל הרמות, וכן לגורמים עימם התקשרה חברת התשלומים, ישנה אחריות לשמירת אבטחת המידע של חברת התשלומים.
33. מדיניות אבטחת המידע תאושר על-ידי הדירקטוריון, לפחות אחת לשלוש שנים.
34. כלל עובדי חברת התשלומים וספקי מיקור חוץ כאמור בסעיף 26 להוראה זו, יעודכנו לגבי מדיניות אבטחת המידע שלו.
35. בהתבסס על מדיניות אבטחת המידע, חברת התשלומים נדרשת לגבש וליישם אמצעים לצמצום סיכוני טכנולוגיות מידע אליהם היא חשופה. אמצעים אלו יכללו, לכל הפחות, את הבאים, כמפורט בהוראה:
    א. ארגון וממשל תאגידי;
    ב. אבטחת מידע לוגית;
    ג. אבטחת מידע פיזית;
    ד. אבטחת מידע פעולות טכנולוגיית המידע;
    ה. ניטור אחר אבטחת מידע;
    ו. ביקורת (Review), הערכה ובחינות (Testing) של היבטי אבטחת מידע;
    ז. מודעות והדרכות בהיבטי אבטחת מידע.

<u>סימן ב': אבטחה לוגית</u>

36. חברת תשלומים תגדיר, תתעד ותישם נהלי בקרת גישה (ניהול זהויות וגישה; להלן: "**נהלי בקרת הגישה**"), שיוטמעו, ייאכפו, ינוטרו באופן שוטף, וכן יתוקפו לפחות פעם בשנה.

37. נהלי בקרת הגישה יכללו גם בקרות לזיהוי פעולות חריגות, ובין היתר ידרשו הטמעתם של העקרונות הבאים (הביטוי "משתמש" על הטיותיו להלן מתייחס גם למשתמשים בעלי גישה טכנית):

א. **עקרון הצורך לדעת (Need to Know), עקרון מתן רמת גישה מינימלית (Least Privilege) לצורך ביצוע התפקיד ועקרון הפרדת התפקידים (Segregation of Duties)**:

1) חברת תשלומים תנהל את הרשאות הגישה לנכסי מידע והמערכות התומכות בנכסים אלה על-בסיס עקרון הצורך לדעת. הרשאות אלה יכילו גם מענה לגישה מרחוק.

2) חברת תשלומים תעניק למשתמש רק את הרשאות הגישה ההכרחיות והנדרשות למילוי תפקידו (על-בסיס עקרון מתן רמת גישה מינימלית), כך שתימנע גישה לא מוצדקת למידע רב, או ימנע עירוב הרשאות גישה (to prevent the allocation of combinations of access rights) שניתן להשתמש בהן לעקיפת מערכות הבקרה (עקרון הפרדת התפקידים).

ב. **זיהוי ואחריות משתמש**: חברת תשלומים תאסור את השימוש בחשבונות משתמשים גנריים או משותפים, ותבטיח שניתן יהיה לזהות את המשתמש לעניין כל פעולה המתבצעת במערכות טכנולוגיית המידע.

ג. **הרשאות גישה מיוחדות (Privileged Access Rights)**:

1) חברת תשלומים תטמיע מנגנוני בקרה מוגברים, ותנטר אחר הרשאות גישה מיוחדות (Privileged System Access), באמצעות השתת מגבלות מחמירות ופיקוח צמוד על חשבונות משתמשים בעלי הרשאות מערכת גבוהות (Elevated System Access Entitlements) (כדוגמת הרשאות חשבון מנהל – Administrator Accounts). לכל משתמש בעל הרשאות מיוחדות (Privileged system access) נדרש שיהיה גם משתמש בעל הרשאות גישה רגילות לשם עבודה בשגרה.

2) חברת תשלומים תיתן גישה מרחוק עם הרשאות ניהול (Administrative access) למערכות טכנולוגיית מידע חיוניות (Critical), רק על-בסיס עקרון הצורך לדעת ולשם ביצוע תפקידה, ותוך **שימוש באמצעי זיהוי חזקים** (Strong authentication solutions – Multi-Factor Authentication).

ד. **מעקב ותיעוד (Logging) פעילויות משתמש**: חברת תשלומים תנטר ותתעד (Log) כל פעולה שנעשית על-ידי משתמשים בעלי הרשאות מיוחדות (Privileged users). יומן המעקב (Access logs) יהיה מאובטח באופן שימנע עריכה או מחיקה לא מורשית, ויישמר לכל הפחות למשך שנתיים, מבלי לגרוע מהוראות כל דין, ובכלל זה הוראות חוק הגנת הפרטיות, והתקנות והצווים לפיו. בעל רישיון ישתמש במידע האמור כדי להקל את הזיהוי והחקירה של פעילויות חריגות שזוהו.

ה. **ניהול הרשאות גישה**: הרשאות גישה יינתנו, יבוטלו או ישונו בתוך פרק הזמן הקצר ביותר האפשרי, בהתאם להליך אישור (Workflow) קבוע שייכתב בנהלי בקרת הגישה, אשר כולל את בעל מאגר המידע שאליו מבוקשת הרשאת גישה (Information asset owner). במקרה של סיום העסקת עובד או התקשרות עם צד שלישי שהוא בעל הרשאת גישה, יש לבטל את הרשאת הגישה שניתנה לו באופן מידי.

ו. **חידוש הרשאות**: חברת תשלומים תבחן את הרשאות הגישה הקיימות באופן תדיר ככל שנדרש, ולפחות אחת לשנה, כדי להבטיח שלמשתמשים אין הרשאות יתר ולוודא ביטול הרשאות ממשתמשים שלא נדרשות להם הרשאות גישה.

ז. **אמצעי אימות**: חברת תשלומים נדרשת לאכוף את השימוש באמצעי אימות חזקים כדי להבטיח באופן יעיל יישום מדיניות של אבטחת מידע ונהלי בקרת הגישה למערכות. אמצעי אימות יותאמו לרמת החיוניות (Criticality) של מערכות טכנולוגיית מידע, המידע או התהליך שאליהם ניגשים. אמצעים אלו יכללו, אמצעי זיהוי חזקים (Multi-Factor Authentication).

<u>סימן ג': אבטחה פיזית</u>

38. חברת תשלומים תגדיר, תתעד ותישם נהלי אבטחת מידע פיזיים שיגנו על מתקניה, מרכזי הנתונים (Data Centers) ואזורי עיבוד המידע מפני כניסה לא מורשית וסיכונים סביבתיים (Environmental hazards).

39. חברת תשלומים תאפשר גישה פיזית למערכות טכנולוגיית מידע (ICT systems) רק לגורמים מורשים. אישור גישה יינתן בהתאם לתפקיד ולאחריות המקצועית של אותו גורם, ויוגבל לגורמים בעלי הכשרה ופיקוח מתאימים.

40. חברת תשלומים תבחן את הרשאות הגישה הפיזית הקיימות באופן תדיר ככל שנדרש, ולפחות אחת לשנה, כדי להבטיח את ביטול הרשאות הגישה של גורמים שלא נדרשים להן.

41. אמצעי הגנה מספקים מפני סיכונים סביבתיים (כגון: הצפה, שרפה, הפסקות חשמל) ייקבעו על-ידי חברת התשלומים בהתאם לחשיבות המתחם, ומרכזיות הפעילות או מרכזיות מערכות טכנולוגיית המידע (ICT systems) שממוקמות במתחם.

<u>סימן ד': אבטחת פעולות טכנולוגיית מידע (ICT Operations Security)</u>

42. חברת תשלומים תטמיע ותישם נהלים למניעה, ככל הניתן, של אירועי כשל, לרבות אירועי אבטחת מידע, במערכות טכנולוגיית מידע ובשירותי טכנולוגיית מידע, ותפעל כדי לצמצם את השפעתם של אירועים מסוג זה, ככל שקורים, על אספקת שירותי טכנולוגיית מידע. על נהלים אלה לכלול את האמצעים הבאים:

א. זיהוי נקודות חולשה אפשריות, הערכתן והענקת מענה להן באמצעות עדכון תדיר של התוכנה והחומרה, לרבות לגבי תוכנה שמספקת חברת התשלומים למשתמשים פנימיים וחיצוניים, על-ידי הפצה של עדכוני אבטחת מידע מהותיים או דרך הטמעה של בקרות מפצות (Compensating Controls);

ב. הטמעת קווי בסיס של כל רכיבי הרשת (Network Components) בתצורה מאובטחת (Secure Configuration Baselines);

ג. הטמעת פילוח רשת (Network Segmentation), מערכות למניעת אובדן מידע, וכן הצפנת תעבורת רשת (Network Traffic), בהתאם לסיווג המידע;

ד. הטמעת הגנה על יחידות קצה (Endpoints), כגון שרתים, עמדות עבודה ומכשירים ניידים (Mobile Devices); חברת תשלומים נדרשת לבחון את עמידתן של יחידות הקצה כאמור בנהלי אבטחת המידע של חברת התשלומים, וזאת לפני הענקת גישה לרשת של חברת התשלומים;

ה. ווידוא קיומם של מנגנונים שמטרתם להבטיח את שלמות ואמינות (Integrity) התוכנה, החומרה והמידע;

ו. הצפנת המידע בעת אחסונו ובעת העברתו (בהלימה לסיווג המידע).

43. חברת תשלומים תבחן באופן שוטף אם יש בשינויים בסביבת הפעילות כדי להשפיע על נהלי אבטחת מידע הקיימים, או דורשים אימוץ של נהלי אבטחת מידע נוספים כדי למזער את הסיכונים הנשקפים משינויים כאמור. שינויים אלה יהוו חלק מהליך ניהול השינויים של חברת התשלומים, שיבטיח בחינה, תיעוד, אישור והוצאה אל הפועל של אותם שינויים.

<u>סימן ה': ניטור אבטחת מידע</u>

44. חברת תשלומים תגבש ותטמיע נהלים לזיהוי פעולות חריגות שעלולות להשפיע על אבטחת המידע, ולתת מענה הולם לפעולות שכאלה. כחלק מהניטור המתמשך, חברת תשלומים נדרשת להטמיע יכולות זיהוי ודיווח הולמות לגבי אירועי חדירה פיזית או לוגית, כמו גם אירועי הפרה של סודיות, שלמות וזמינות של נכסי מידע. תהליכי הניטור והזיהוי יתייחסו לנושאים הבאים:

א. פעילות של גורמים פנימיים וחיצוניים רלוונטיים, לרבות בעלי תפקידים עסקיים או בעלי תפקידים בתחום טכנולוגיית מידע;

ב. פעולות (Transactions) לזיהוי שימוש לרעה בהרשאות בידי צד שלישי או כל ישות אחרת ושימוש לרעה בהרשאה בידי גורם פנימי;

ג. איומים פנימיים וחיצוניים פוטנציאליים.

45. חברת תשלומים תטמיע תהליכים ותגבש מבנה ארגוני מתאימים, שיאפשרו לה לזהות ולנטר באופן קבוע איומי אבטחת מידע שעלולים להיות בעלי השפעה מהותית על יכולתה של חברת התשלומים לספק שירותים. מבלי לגרוע מכלליות האמור, חברת תשלומים:

א. תיזום ניטור אחר פיתוחים טכנולוגיים כדי להבטיח מודעות לסיכוני אבטחת מידע.

ב. תטמיע אמצעי גילוי, בין היתר, כדי לגלות דליפות מידע אפשריות, קוד זדוני ואיומי אבטחת מידע אחרים, וכן חולשות ידועות בחומרה ובתוכנה, וכן תבחן באופן תדיר התאמה של עדכוני אבטחת מידע מתאימים.

46. חברת התשלומים תישם את הליך ניטור אבטחת המידע באופן שיסייע לה להבין את מאפייני אירועי אבטחת המידע והתפעול, לזהות מגמות ולתמוך בהליכי התחקור הפנימיים של חברת התשלומים.

סימן ו': ביקורת (Review), הערכה ובחינה (Testing) של אבטחת מידע

47. חברת תשלומים תערוך מגוון ביקורות, הערכות ובדיקות של אבטחת מידע, כדי להבטיח זיהוי יעיל של חולשות במערכות טכנולוגיית מידע ובשירותי טכנולוגיית מידע, ובכלל זה: בחינות ניתוח פערים (Gap Analysis) ביחס לסטנדרטים של אבטחת מידע; בחינות עמידה בהוראות הדין והנהלים; ביקורות (Audits) של מערכות המידע; בחינות אבטחת מידע פיזית; וכן, תשקול לאמץ נהלים מקובלים לבחינות קוד מקור, הערכות חולשות (Vulnerability Assessments), ובדיקות חדירות (Penetration Tests).
48. חברת תשלומים תגבש ותטמיע **מסגרת לבדיקת אבטחת מידע** שתתקף את האיתנות והיעילות של אמצעי אבטחת המידע של חברת התשלומים, לרבות לגבי העניינים שלהלן:
    א. האיומים והחולשות שזוהו במסגרת תהליכי ניטור והערכה של סיכוני טכנולוגיות מידע.
    ב. אמצעי אבטחת מידע שרלוונטיים לרכיבים שיפורטו להלן, ככל שהם קיימים אצל חברת התשלומים: (1) מסופי תשלום ומכשירים שמשמשים לאספקת שירותי תשלום; (2) מסופי תשלום במכשירים המשמשים לאימות זהות לקוחות (משתמשי שירותי התשלום; PSU - payment service users); (3) מכשירים ותוכנות בהם משתמשת חברת התשלומים, אשר מפיקים עבור משתמש שירותי התשלום קוד אימות.
49. חברת תשלומים תוודא שהמסגרת לבדיקת אבטחת המידע כוללת בדיקות שיתקיימו לגביהן התנאים כדלהלן:
    א. הבדיקות יבוצעו על-ידי בודקים אובייקטיביים שלא מועסקים על-ידי חברת התשלומים, שהם בעלי ידע, מיומנות ומומחיות בבדיקת אמצעי אבטחת מידע ואשר לא מעורבים בפיתוח של אמצעי אבטחת המידע;
    ב. הבדיקות יכללו סריקות חולשות ובדיקות חדירות (כולל בדיקות ממוקדות-איום (threat-led), לפחות אחת ל-18 חודשים או ככל שיידרש, באופן התואם את רמת הסיכון שנקבעה לתהליכים העסקיים ולמערכות חברת התשלומים.
50. חברת תשלומים תבדוק את כלל אמצעי אבטחת המידע שלה באופן שוטף. מבלי לגרוע מכלליות האמור, חברת תשלומים תבצע בדיקות למערכות הבאות, כמפורט להלן:
    א. מערכות טכנולוגיית מידע חיוניות (critical) – בדיקות אמצעי אבטחת מידע תיערכנה לפחות אחת לשנה, ותהיינה חלק מהערכת סיכוני אבטחת המידע הכוללת שחברת התשלומים עורכת בנוגע לשירותי התשלום שהיא מעניקה.
    ב. מערכות טכנולוגיית מידע שאינן חיוניות – בדיקות אמצעי אבטחת מידע תיערכנה בתדירות ההולמת את רמת הסיכון המאפיינת את התהליכים העסקיים ואת המערכות כאמור, ולפחות אחת לשלוש שנים.
51. חברת תשלומים תוודא שבדיקות אמצעי אבטחת מידע מבוצעות בכל מקרה של שינוי בתשתיות, בתהליכים, או כתוצאה מאירוע תפעולי או אירוע אבטחת מידע, או בעקבות הטמעה של יישומים חדשים או יישומים שעברו עדכון או שינוי מהותי, והכל – ככל שהם עלולים לשנות את רמת אבטחת המידע הקיימת או דורשים אימוץ של אמצעי אבטחה נוספים, וזאת כדי לתת

מענה לסיכונים הנשקפים כתוצאה מכך. שינויים כאמור, ייעשו בהתאם לתהליך ניהול שינויים שתקבע חברת התשלומים.

52. חברת תשלומים תנטר באופן שוטף אחר תוצאות בדיקות אבטחת מידע ותעריכן, וכן תעדכן את אמצעי אבטחת המידע בהתאם אליהן בתוך זמן סביר. לעניין מערכות טכנולוגיית מידע חיוניות (critical) – חברת תשלומים תעדכן את אמצעי אבטחת המידע כאמור בסעיף זה ללא דיחוי.
53. בהתבסס על איומי אבטחת מידע שנמצאו והשינויים שבוצעו כאמור בסעיף 52, חברת תשלומים תטמיע בהליכי הבדיקה תרחישים של איומים צפויים ורלוונטיים, וכן של תקיפות אפשריות או צפויות.

<u>סימן ז': הדרכות ומודעות לאבטחת מידע</u>

54. חברת תשלומים תגבש תכנית הדרכות תקופתיות בתחום אבטחת מידע, אשר תכלול תכנים העוסקים בריענון כשירות ובהעלאת מודעות לנהלי אבטחת מידע.
מטרת תכנית ההדרכות היא להבטיח שכלל המועסקים והגורמים הרלוונטיים שהתקשרו עם חברת התשלומים כשירים למלא את תפקידיהם באופן שהולם את מדיניות אבטחת המידע והנהלים של חברת התשלומים, לצמצם סיכונים לטעויות אנוש, גניבות, הונאות, שימוש לרעה או אובדן של מידע, וכן להתמודד עם סיכוני אבטחת מידע.
55. חברת תשלומים תוודא שכלל המועסקים והגורמים הרלוונטיים שהתקשרו עמה, משתתפים בהדרכה בתחום אבטחת מידע כאמור בסעיף 54, ושיעילות ההדרכה האמורה נבחנת, הכל לפחות פעם אחת בשנה.

פרק ו': ניהול פעילות טכנולוגיית המידע (ICT Operations Management)

<u>סימן א': כללי</u>

56. חברת תשלומים תנהל את פעילות טכנולוגיית המידע (ICT Operations) שלה בהתבסס על תהליכים ונהלים כתובים ומוטמעים, לרבות מסמך מדיניות אבטחת מידע, שאושרו על-ידי הדירקטוריון. במסגרת המסמכים כאמור, חברת תשלומים תגדיר כיצד היא פועלת, מנטרת ושולטת במערכות טכנולוגיית מידע ובשירותי טכנולוגיית מידע, ובכלל זה תתעד את פעילות טכנולוגיית המידע החיוניות (Critical ICT Operations).
57. חברת תשלומים תוודא שפעילות טכנולוגיית המידע שלה מותאמות לדרישות העסקיות שלה, וכן תתחזק ותשפר, ככל שיידרש, את יעילות פעילות טכנולוגיית המידע שלו, ובין היתר, תבחן כיצד לצמצם למינימום האפשרי שגיאות שעולות מביצוע ידני של משימות.
58. חברת תשלומים תגבש ותטמיע נהלים לתיעוד (Logging) וניטור בעניין פעולות טכנולוגיית מידע חיוניות, שיאפשרו זיהוי, ניתוח ותיקון של שגיאות.
59. חברת תשלומים תערוך רשימת נכסי טכנולוגיית מידע כגון מערכות טכנולוגיית מידע, מכשירי רשת (network devices), מסדי נתונים (data bases) וכדומה, אשר תעודכן באופן שוטף. רשימה כאמור תכלול את התצורה (configuration) של נכסי טכנולוגיית מידע, הקישורים

(links) והתלות ההדדית בין נכסי טכנולוגיית מידע שונים, וזאת על מנת לאפשר תצורה ותהליך ניהול שינויים נאותים.

60. רשימת נכסי טכנולוגיית מידע תהיה מפורטת דיה על מנת לאפשר זיהוי מידי של נכס טכנולוגיית מידע, המיקום שלו, הסיווג האבטחתי שלו ובעליו. כמו כן, רשימת נכסי טכנולוגיית מידע תכלול התייחסות לקשרי תלות-הדדית בין נכסים, ככל שאלו קיימים, באופן שיתמוך במענה לאירועים תפעולים ואירועי אבטחת מידע, לרבות מתקפות סייבר.
61. חברת תשלומים תנטר ותנהל את מחזור החיים של נכסי טכנולוגיית מידע (the life cycle of ICT assets), באופן שיבטיח שנכסים כאמור מתיישבים באופן שוטף עם הדרישות העסקיות ועם ניהול הסיכונים של חברת התשלומים, ותומכים בהם.
62. חברת תשלומים תבדוק אם נכסי טכנולוגיית המידע שלה נתמכים על-ידי ספקים ומפתחים חיצוניים או פנימיים, ואם מיושמים לגביהם שדרוגים או תיקונים בהתבסס על תהליך מתועד.
63. חברת תשלומים תעריך את הסיכונים שנובעים משימוש בנכסי טכנולוגיית מידע מיושנים או שאינם נתמכים טכנולוגית, ותצמצמם.
64. חברת תשלומים תטמיע תכנית ביצועי אבטחת מידע ומשאבי טכנולוגיית מידע ותהליכי ניטור, כדי למנוע או לזהות בעיות ביצועים מהותיות של מערכות טכנולוגיית מידע וכן כדי לתת מענה לבעיות אלה ולמחסור במשאבי טכנולוגיית מידע באופן מיידי.
65. חברת תשלומים תגדיר ותטמיע נהלי גיבוי ושחזור של מידע ושל מערכות טכנולוגיית מידע, כדי להבטיח שהם יכולים להתאושש (recovered) ממקרה של אירוע תפעולי או אירוע אבטחת מידע, ככל שיידרש. היקף ותדירות הגיבוי והשחזור ייקבעו בהתאמה לדרישות העסקיות, לחיוניות המידע ומערכות טכנולוגיית מידע, ובהתאם להערכת סיכונים של חברת התשלומים. חברת תשלומים תבחן את נהלי הגיבוי והשחזור כאמור באופן תקופתי ולפחות אחת לשנתיים.
66. חברת תשלומים תוודא שגיבוי המידע ומערכות טכנולוגיית מידע מאוחסנים בצורה מאובטחת ומרוחקת מספיק מהאתר הראשי (Primary Site) כדי שלא ייחשפו לאותם הסיכונים של האתר הראשי.

<u>סימן ב': ניהול תקלות ואירועי טכנולוגיית מידע</u>

67. חברת תשלומים תגבש ותישם נוהל ניהול תקלות ואירועי טכנולוגיית מידע, במסגרתו ייקבעו תהליכים שיאפשרו ניטור ותיעוד (Log) של אירועים תפעוליים או אירועי אבטחת מידע בתחום טכנולוגיית מידע, לרבות בקשר למניעת הונאה (Fraud) בשל אירועים כאמור, וכן כדי לאפשר לחברת התשלומים להמשיך או לחדש את אספקת השירותים והתהליכים העסקיים החיוניים שהופרעו עקב אירועים כאמור, בהקדם האפשרי. מבלי לפגוע בכלליות האמור, הנוהל יכלול, בין היתר, כדלהלן:
    א. קריטריונים ותנאי סף שיוגדרו לזיהוי אירוע כאירוע תפעולי או אירוע אבטחת מידע, כמו גם קריטריונים בדבר סימני אזהרה מקדימים (early warning indicators) שישמשו התראה לזיהוי מוקדם של אירועים כאמור.

ב. תהליכים ומבנה ארגוני ראויים, שיבטיחו ניטור, התמודדות ומעקב עקביים ומשולבים אחר אירועים תפעוליים או אירועי אבטחת מידע, וכן כדי לוודא ששורש הבעיה (root causes) מזוהה ומטופל כדי למנוע את הישנות האירועים. תהליך ניהול אירועים ובעיות כאמור, יכלול, בין היתר, כדלהלן:

1) תהליכים לזיהוי, מעקב, תיעוד (Log), חלוקה לקטגוריות של אירועים תפעוליים או אירועי אבטחת מידע, בהתאם לסדר עדיפויות שייקבע על בסיס חיוניות עסקית;

2) תפקידים ותחומי אחריות בנוגע לתרחישי אירוע שונים, כגון: שגיאות, תקלות, ותקיפות סייבר;

3) תהליכים לזיהוי, ניתוח ופתרון של שורש הבעיה שגרמה לאירוע אחד או יותר. בכלל זה, ניתוח אירועים תפעוליים או אירועי אבטחת מידע שעלולים להשפיע על חברת התשלומים, שזוהו או אירעו אצל חברת התשלומים או אצל גורמים חיצוניים, הפקת לקחים מהניתוח האמור, ועדכון את אמצעי אבטחת המידע שלה בהתאם.

ג. תכניות תקשורת פנימית יעילות, לרבות לעניין דיווח והסלמה (Notification and Escalation Procedures), אשר יתייחסו, בין היתר, לתלונות לקוחות הקשורות לאבטחת מידע, וזאת במטרה להבטיח כדלהלן:

1) דיווח על אירועים בעלי השפעה מהותית בקשר למערכות טכנולוגיית מידע ושירותי טכנולוגיית מידע, לגורמי הנהלה בכירים רלוונטיים, ובכלל זה לגורמי הנהלה בכירים בתחום טכנולוגיית מידע;

2) עדכון הדירקטוריון לגבי אירועים בעלי השפעה מהותית בקשר למערכות טכנולוגיית מידע ושירותי טכנולוגיית מידע, ובכלל זה לעניין השפעתם, המענה והבקרות הנוספות שהוגדרו כתוצאה מהם.

ד. תכניות מענה לאירוע תפעולי או אירוע אבטחת מידע כדי למזער את ההשפעות הנובעות ממנו, ולהבטיח שמתן השירות יחודש באופן מאובטח בהקדם האפשרי.

ה. תכניות תקשורת חוץ-ארגוניות בקשר לפונקציות ותהליכים עסקיים חיוניים, על מנת להבטיח כדלהלן:

1) שיתוף פעולה עם גורמים רלוונטיים (stakeholders) חיצוניים לחברת התשלומים, במטרה לתת מענה ולהתאושש מאירועים תפעוליים ואירועי אבטחת מידע באופן יעיל;

2) עדכון גורמים חיצוניים (למשל, לקוחות, גורמי שוק נוספים, הרשות), לגבי אירועים תפעוליים או אירועי אבטחת מידע בתחום טכנולוגיית מידע ככל שיידרש, וזאת על-ידי בעלי תפקידים מוגדרים אצל חברת התשלומים שייקבעו בנוהל לעניין זה, תוך עמידה בזמנים ובהתאם להוראות דין אחרות הרלוונטיות לעניין זה.

פרק ז': ניהול שינויים בתחום טכנולוגיית מידע

<u>סימן א': רכישה ופיתוח מערכות טכנולוגיית מידע</u>

68. חברת תשלומים תגבש ותטמיע תהליכי רכש, פיתוח ותחזוקה של מערכות טכנולוגיית מידע, בהתאם לרמת הסיכון שהוגדרה לגביהן.
69. חברת תשלומים תוודא לפני כל רכש או פיתוח של מערכת טכנולוגיית מידע, כי הדרישות הפונקציונליות והלא-פונקציונליות של המערכת, לרבות דרישות הנוגעות לאבטחת מידע, הוגדרו בבירור ואושרו בידי נושא משרה בכירה רלוונטי בתחום טכנולוגיית מידע ואבטחת מידע בחברת התשלומים.
70. חברת תשלומים תבטיח שננקטים אמצעים למזעור הסיכון בדבר שינוי לא מכוון או מניפולציה מכוונת במערכות טכנולוגיית מידע, במהלך פיתוח והטמעה בסביבת הייצור.
71. חברת תשלומים תגבש ותטמיע נוהל לבחינה ואישור של מערכות טכנולוגיית מידע טרם השימוש הראשון בהן. הנוהל יתחשב בחיוניות של התהליכים העסקיים, התהליכים התומכים ונכסי המידע. עוד במסגרת הבחינה תוודא חברת התשלומים שמערכות טכנולוגיית המידע פועלות כמצופה, וזאת תוך שימוש בסביבת בדיקות שמדמה באופן מספק את סביבת הייצור.
72. חברת תשלומים תבחן את מערכות טכנולוגיית המידע, שירותי טכנולוגיית המידע ואמצעי אבטחת המידע, כדי לזהות חולשות, הפרות ושגיאות אבטחת מידע אפשריות, באופנים ובתדירות שהיא תקבע בנוהל.
73. חברת תשלומים תטמיע מספר סביבות טכנולוגיית מידע (ICT environments) כדי להבטיח הפרדה מספקת של סמכויות של עובדי החברה או צדדים שלישיים, וכדי למזער השפעה של שינויים לא מורשים על מערכות הייצור.
74. מבלי לגרוע מכלליות האמור, חברת תשלומים תוודא הפרדה של סביבות הייצור מסביבות הפיתוח, הבדיקות וכל סביבה אחרת שאינה סביבת ייצור.
75. חברת תשלומים תוודא את השלמות והסודיות של מידע מסביבת הייצור בסביבות שאינן סביבות ייצור.
76. חברת תשלומים תוודא שהגישה למידע מסביבת הייצור תהיה מוגבלת למשתמשים המורשים לכך בלבד.
77. חברת תשלומים תטמיע אמצעים להגנה על שלמות קוד המקור של מערכות טכנולוגיית מידע שפותחו אצל חברת התשלומים.
78. חברת תשלומים תתעד את הפיתוח, ההטמעה, התפעול והתצורה (configuration) של מערכות טכנולוגיית מידע באופן מפורט, כדי לצמצם תלות לא נדרשת במומחים לנושא. התיעוד של מערכות טכנולוגיית מידע יכלול, מקום שרלוונטי, תיעוד אודות המשתמשים (User Documentation), תיעוד מערכת טכני (Technical System Documentation) ונהלי תפעול (Operating Procedures).
79. תהליכי רכש ופיתוח של מערכות טכנולוגיית מידע של חברת תשלומים, יחולו גם לעניין מערכות טכנולוגיית מידע שמפותחות או מנוהלות על-ידי משתמשי קצה עסקיים (Business Function's End Users) שלא מקרב חברת התשלומים, למשל, יישומי מחשב של משתמשי

הקצה (end user computing applications), בהתאם לרמת הסיכון. חברת התשלומים תתחזק תיעוד של רשימת היישומים שתומכים בפעילות או תהליכים עסקיים חיוניים.

פרק ח': ניהול המשכיות עסקית

<u>סימן א': תהליך ניהול המשכיות עסקית – כללי</u>

80. חברת תשלומים תגבש תהליך ניהול המשכיות עסקית (להלן: "**תהליך ניהול המשכיות עסקית**"; (business continuity management (BCM) נאות, במטרה למקסם את יכולתה לספק שירותים על בסיס מתמשך, ולצמצם השלכות תפעוליות, פיננסיות, משפטיות, או כאלו הקשורות למוניטין, וכן השלכות מהותיות אחרות הכרוכות באירוע כשל.

<u>סימן ב': ניתוח השפעות עסקיות</u>

81. כחלק מתהליך ניהול המשכיות עסקית נאות, חברת תשלומים תערוך ניתוח השפעות עסקיות (להלן: "**ניתוח השפעות עסקיות**"; Business Impact Analysis (BIA)) על-ידי בחינת חשיפתה לאירועי כשל, וכן על-ידי הערכה כמותית ואיכותנית של מידת ההשפעה של אירועי כשל, לרבות בהיבטי סודיות, אמינות וזמינות. ניתוח ההשפעות העסקיות ייעשה תוך שימוש בנתונים פנימיים וחיצוניים, וניתוח תרחישים שונים, בהתחשב במידת החיוניות של התהליכים העסקיים, המערכות התומכות ונכסי המידע אשר זוהו וסווגו על-ידי חברת התשלומים, וכן בהתחשב בתלות ההדדית שלהם, לפי פרק ד', סימנים ג' ו-ד' להוראה.

82. חברת תשלומים תוודא כי מערכות טכנולוגיית מידע ושירותי טכנולוגיית מידע מתוכננים (designed) ומותאמים לניתוח ההשפעות העסקיות. כך למשל, חברת תשלומים תדאג כי מערכות ושירותים כאמור מתוכננים ומותאמים ליתירות (redundancy) רכיבים חיוניים מסוימים כדי למנוע שיבושים הנגרמים מאירועי כשל המשפיעים על רכיבים אלה.

<u>סימן ג': תכנית המשכיות עסקית</u>

83. בהתבסס על ניתוח ההשפעות העסקיות (BIA), חברת תשלומים תגבש תכנית המשכיות עסקית בכתב, לפי הוראה זו, אשר תאושר על-ידי הדירקטוריון.

84. תכנית המשכיות עסקית תיושם על-ידי חברת התשלומים, ותכלול, בין היתר, כדלהלן:

א. בחינה של מגוון אירועי כשל, ובכלל זה תרחישים חמורים אך מתקבלים על הדעת, אשר אליהם חברת התשלומים עלולה להיות חשופה, וסיכונים שעלולים להשפיע לרעה על מערכות טכנולוגיית מידע ושירותי טכנולוגיית מידע, לרבות תרחישי מתקפות סייבר, והערכה של ההשפעה האפשרית של אירועים אלה.

ב. פירוט הצעדים שבהם תנקוט חברת התשלומים כדי להגיב באופן הולם לאירועי כשל אפשריים, להתאושש מהם ולחדש את פעילותם התקינה של התהליכים העסקיים החיוניים, התהליכים התומכים, נכסי המידע, בתוך מסגרת זמן התאוששות (RTO) ויעד ההתאוששות (RPO) שתקבע חברת תשלומים (להלן: "**הצעדים לתגובה והתאוששות**"),

על מנת למנוע השפעות שליליות על פעילות חברת התשלומים והמערכת הפיננסית, ובכלל זה השפעות על מערכות התשלומים ולקוחות חברת התשלומים (משתמשי הקצה) וכן על מנת לוודא את ביצוען של עסקאות תשלום שטרם בוצעו (pending payment transactions) ואת השלמת המחויבות החוזית שקיימת עם לקוחות וצדדים שלישיים. במסגרת זו חברת התשלומים תבצע גם כדלהלן:

(1) תפרט את פרטי אתר הגיבוי, גישה לתשתיות מערכות מידע (IT), תוכנות ומידע חיוני או רגיש, כדי להתאושש מאירועי כשל;

(2) תפרט כיצד הצעדים לתגובה והתאוששות מבטיחים את ההמשכיות של מערכות טכנולוגיית מידע, שירותי טכנולוגיית מידע, התהליכים העסקיים והתהליכים התומכים, כמו גם של אבטחת המידע;

(3) תפרט גם את הצעדים לתגובה והתאוששות בהם תנקוט על מנת לצמצם כשלים של צדדים שלישיים בעלי חשיבות מרכזית להמשכיות שירותי טכנולוגיית מידע של חברת התשלומים.

ג. בקביעת הצעדים לתגובה והתאוששות כאמור בסעיף קטן (ב), חברת תשלומים תיקח בחשבון גם פתרונות חלופיים למקרים בהם ההתאוששות לא תהיה אפשרית בטווח הזמן הקצר, בין היתר, לאור היבטי עלויות, סיכונים, לוגיסטיקה או נסיבות לא צפויות אחרות.

ד. פירוט התנאים אשר בהתקיימם תופעל תכנית ההמשכיות העסקית.

85. בקרות אירוע כשל שגורם להפעלה של תכנית המשכיות עסקית, חברת תשלומים תתעדף פעולות המשכיות עסקית בהתחשב ברמת הסיכון והערכות סיכונים שבוצעו במסגרת ניהול סיכוני טכנולוגיית מידע שערכה חברת התשלומים.

86. חברת תשלומים תערוך את תכנית ההמשכיות העסקית בתיאום עם הגורמים הרלוונטיים, פנימיים או חיצוניים.

87. חברת תשלומים תתעד את תכנית ההמשכיות העסקית ותוודא כי היא נגישה לעובדי החברה הרלוונטיים, לרבות צדדים שלישיים רלוונטיים, בכלל ובפרט במקרה חירום.

<u>סימן ד': בחינה תקופתית של תכנית המשכיות עסקית</u>

88. חברת תשלומים תבחן את תכנית ההמשכיות העסקית שלה באופן תקופתי. בפרט, חברת תשלומים תוודא כי תכנית ההמשכיות העסקית שלה, בכל הנוגע לתהליכים עסקיים, תהליכים תומכים ונכסי מידע חיוניים (לרבות אלו המסופקים על-ידי צדדים שלישיים), נבחנת לפחות אחת לשנה, כפי שמפורט להלן בסעיף 90.

89. חברת תשלומים תוודא עדכניות תכנית ההמשכיות העסקית, לכל הפחות אחת לשנה, בהתבסס על תוצאות תהליכי הבחינה שיבוצעו לפי סימן זה, מידע עדכני שהתקבל לגבי איומים ולקחים שנלמדו מאירועי כשל קודמים. כל שינוי ביעדי התאוששות או בזמני התאוששות של החברה ושינויים בתהליכים העסקיים, התהליכים התומכים ונכסי המידע צריך להילקח בחשבון לצורכי עדכון תכנית ההמשכיות העסקית.

90. בחינת תכנית ההמשכיות העסקית על-ידי חברת תשלומים תיערך במטרה להבטיח כי חברת התשלומים מסוגלת להמשיך ולקיים את פעילותה העסקית בצורה מוצלחת, וזאת עד להקמה מחדש של התהליכים העסקיים החיוניים במקרה של אירוע כשל. מבלי לגרוע מכלליות האמור, נדרש כי הבחינה כאמור תקיים את התנאים כדלהלן:

א. תכלול בחינת התרחישים אשר נלקחו בחשבון בעת גיבוש תכנית ההמשכיות העסקית (וכן בחינה של שירותים המסופקים על-ידי ספקים צדדים שלישיים). הבחינה צריכה לכלול העברה של תהליכי העסקים החיוניים, התהליכים התומכים ונכסי המידע לסביבת אתר הגיבוי, והפעלת שירותים אלו לפרק זמן מספק בסביבה זו באופן תקין, ולאחר מכן החזרתם לפעילות רגילה.

ב. תתוכנן באופן המאתגר את ההנחות שבבסיס תכנית ההמשכיות העסקית, לרבות לעניין הממשל התאגידי ותקשורת בעת אירוע כשל.

ג. תכלול בחינת יכולתם של צוותי העבודה, הספקים, מערכות ושירותי המידע והתקשורת להגיב כראוי לתרחישים הנבדקים.

91. חברת תשלומים תתעד את תוצאות בחינת תכנית ההמשכיות העסקית, תנתח את החולשות אם נמצאו במהלך הבחינה ותטפל בהן.

92. חברת תשלומים תדווח לדירקטוריון את תוצאות בחינת תכנית ההמשכיות העסקית, ניתוח החולשות ואופן הטיפול בהן, כאמור בסעיף 91, לפחות אחת לשנה.

<u>סימן ה': תקשורת בעת אירוע כשל</u>

93. חברת תשלומים תוודא כי עומדים לרשותה כלי תקשורת יעילים, באופן אשר יבטיח כי כלל הגורמים הרלוונטיים, פנימיים וחיצוניים כאחד, לרבות המאסדרים השונים ככל שנדרש, וספקים רלוונטיים (למשל, ספקי מיקור חוץ, גורמים בתוך הקבוצה וכדומה), יהיו מעודכנים כנדרש ובזמן הראוי, לרבות לפי הוראות דין או הסכם, בעת אירוע כשל, ובמהלך יישום תכנית המשכיות עסקית.

פרק ט': ניהול יחסי חברת תשלומים ולקוחות (PSUs)

94. התחברות לקוח לאזור האישי שלו במערכת של חברת התשלומים תתאפשר לאחר שחברת התשלומים זיהתה את הלקוח באמצעי זיהוי חזקים (Multi-Factor Authentication).

95. חברת תשלומים תעניק ללקוחות סיוע והכוונה ללקוחות להגברת מודעותם לגבי סיכוני אבטחת מידע והגנת הפרטיות הקשורים לשירותי התשלום, לפחות במסגרת מערכת חברת התשלומים, וכן תאפשר ללקוחות לפנות אליה בקשר עם שאלות או בקשות לתמיכה בנושאים האמורים ובאמצעי קשר שיפורט שם.

96. כאשר ישנו הסכם בין חברת תשלומים ולקוח בדבר מגבלות סכום (Spending Limits) בעסקאות תשלום המבוצעות באמצעות אמצעי תשלום (Payment Instrument) מסוים, חברת התשלומים תספק ללקוח את האפשרות להתאים (adjust) את המגבלות האמורות עד למגבלת המקסימום שהוסכם לגביה.

97. חברת תשלומים תספק ללקוחות המעוניינים בכך את האפשרות לקבל התראות לגבי מתן הוראות לביצוע עסקאות תשלום או ניסיונות כושלים לתת הוראות לביצוע עסקאות תשלום, באופן שיאפשר להם לזהות הונאות או שימוש לרעה בחשבונותיהם.

פרק י': הגנת הפרטיות ואבטחת מידע

98. חברת תשלומים תעמוד בכל עת ולגבי כל פעילויותיו מכוח הרישיון, בהוראות הקבועות בחוק הגנת הפרטיות, התקנות והצווים לפיו, ולעניין הוראות אלו, חברת תשלומים המנהלת מאגר מידע אשר חלה עליו רמת האבטחה הבסיסית, כהגדרתה בתקנות הגנת הפרטיות, תעמוד בכל עת בדרישות החלות על מאגר מידע אשר חלה עליו רמת אבטחה בינונית לכל הפחות.

99. על אף האמור בתקנה 10(ד) לתקנות הגנת הפרטיות, נתוני התיעוד של מנגנון הבקרה לפי תקנה 10(א) לתקנות הגנת הפרטיות, יישמרו למשך שבע שנים לפחות ממועד יצירתם.

100. תקשורת של חברת תשלומים המכילה מידע רגיש מול כל גורם, תיעשה בפרוטוקול סטנדרטי ובתעבורה מוצפנת על פי הטכנולוגיות העדכניות הקיימות בשוק.

101. <u>תהליך ניטור, מעקב והגבלת גישה למידע רגיש</u>

חברת תשלומים תגבש ותישם נוהל מרוכז שיסדיר תהליך שיאפשר ניטור, מעקב והגבלת גישה למידע רגיש, ובכלל זה:

א. תיאור של זרימת המידע שסווג כרגיש, בהקשר של המודל העסקי של המבקש.
ב. הנהלים שקיימים למתן הרשאת גישה למידע רגיש.
ג. תיאור של כלי הניטור.
ד. מדיניות הרשאת גישה, הכוללת פירוט הגישה לכל רכיבי התשתיות והמערכות הרלוונטיות, כולל מאגרי מידע ותשתיות גיבוי.
ה. השימוש הפנימי או החיצוני הצפוי במידע שנאסף.
ו. אמצעי אבטחת מידע טכניים ומערכות מידע (IT systems) שהוטמעו, לרבות הצפנה (Encryption and/or tokenisation).
ז. זהות כלל הגורמים שיש להם גישה למידע הרגיש.
ח. הסבר על אודות דרך גילוי הפרות וטיפול בהן.

פרק י"א: בחינה תקופתית ותחילה

102. בחינה ראשונה של הוראה זו לפי סעיף 36 לחוק עקרונות האסדרה, התשפ"ב–2021, תתבצע לכל המאוחר, בתום 10 שנים מיום תחילתה.

103. תחילתה של הוראה זו ביום תחילתו של חוק הסדרת העיסוק בשירותי תשלום כאמור בסעיף 80(א) רישא לחוק.