רשות ניירות ערך
Israel Securities Authority
سلطة الأوراق المالية

י״ז אדר א תשפ״ד
26 פברואר 2024

הצעת הוראה לבעלי רישיון או אישור שירותי תשלום או ייזום בסיסי בעניין אמצעים טכנולוגיים ואבטחת מידע

נוסח להערות ציבור

הערות ותגובות תתקבלנה עד ליום 31 למרץ 2024

אנשי קשר: עו״ד ספיר מלול, עו״ד אור שטרנברג

טל׳: 02-6556456, פקס: 02-6513646

דוא״ל: OrS@isa.gov.il, sapirm@isa.gov.il, seclaw@isa.gov.il

נבקש להפנות את תשומת ליבכם לנוהל שפרסמה הרשות בעניין ייזום אסדרה, ראו כאן; בהתאם לנוהל זה ההערות המרכזיות מאת הציבור יובאו במסמך המרכז את נוסח האסדרה שגובש, תוך ציון שמות המגיבים מקרב הציבור. ראו גם סעיף 7 לאותו הנוהל, בדבר בקשות מיוחדות להימנע מפרסום שמי כאמור.

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 רישיון או אישור למתן שירותי תשלום או למתן שירות ייזום בסיסי, לתאגידים העומדים בדרישות הקבועות בחוק, ולפקח על בעלי רישיון או אישור (להלן: ״**בעלי רישיון**״), לפי החוק.

עוד הסמיך החוק את הרשות לקבוע הוראות לבעלי רישיון בנושאים שונים, ביניהם הוראות בעניין מנגנונים נאותים ומתקדמים לאבטחת מידע, לניהול סיכונים ולהגנת סייבר, ולעניין חברת תשלומים – גם להמשכיות עסקית, לרבות בעניין חובת מינוי בעלי תפקידים שיהיו ממונים על אבטחת מידע, ניהול הסיכונים והגנת סייבר, ובעניין קביעת תנאי כשירות ודרישות הכשרה בעבורם. כמו כן, אחד התנאים למתן רישיון שירותי תשלום או שירות ייזום בסיסי או למתן אישור שירות ייזום בסיסי, הוא שלמבקש יש אמצעים טכנולוגיים מתאימים לשם מתן שירות התשלום או שירות הייזום הבסיסי, לפי העניין, ומיומנות בהפעלתם, באופן שיבטיח את אמינות המערכות שבאמצעותן יינתנו השירותים ואת קיום ההוראות לפי החוק ולפי חוק שירותי תשלום, התשע״ט-2019.

לפיכך, מוצעת הוראה זו שמטרתה להסדיר את הדרישות שיחולו על בעלי רישיון בעניין אמצעים טכנולוגיים, ניהול סיכוני טכנולוגיית מידע, אבטחת מידע, הגנת סייבר והמשכיות עסקית.

ההוראה המוצעת מתבססת על דרישות החוק, וכן על האסדרה האירופאית בנושא ניהול סיכוני טכנולוגיות מידע ואבטחת מידע שחלה על נותני שירותי תשלום או ייזום בסיסי 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 וייזום בסיסי מתאפיינת בשימוש נרחב באמצעים אלקטרוניים ונעשית כיום ברובה באופן מקוון – לדוגמה, באמצעות שימוש בקווים אינטרנטיים, ניידים ואלחוטיים, ורשתות. זאת ועוד, שירותי תשלום ושירות ייזום בסיסי מלווים, לעיתים קרובות, בהתקשרויות עם גופים שונים מהמגזר הפיננסי, כמו גם עם צדדים שלישיים. לאור זאת, הפעילות האמורה חשופה לסיכוני טכנולוגיית מידע ואבטחת מידע (להלן: "**סיכוני טכנולוגיית מידע**"), כולל להתקפות סייבר. לפיכך, הוראה מוצעת זו מחייבת את בעלי הרישיון לנהל את הסיכונים האמורים ולנקוט באמצעים נאותים לצמצומם ככל הניתן.

ההוראה המוצעת קובעת מודל בו קיימים שלושה מעגלי בקרה שמטרתם לוודא יישום מטרות הוראה זו לרבות צמצום סיכוני טכנולוגיית המידע אצל בעל הרישיון. 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 בעל הרישיון אשר נדרש לאשר ולפקח אחר יישומן של דרישות הוראה זו בבעל הרישיון. עוד יודגש כי ההוראה קובעת מהם התהליכים, הנהלים ויתר המסמכים הנדרשים לבעל הרישיון לצורך עמידה בדרישותיה. עם זאת, הדגש הניתן בהוראה הוא על הטמעה, יישום וניטור אחר נאותות היישום של אותם מסמכים, כך שבעל הרישיון אינו יכול 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 בעל הרישיון, לרבות אחריות הדירקטוריון בנושא סיכוני טכנולוגיית מידע;
- פרק ג' עוסק בחובה של בעל הרישיון להכין אסטרטגיית טכנולוגיית מידע, אשר הולמת את האסטרטגיה העסקית הכוללת של בעל הרישיון;

---

[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.

- פרק ד׳ עוסק בחובת בעל הרישיון לנהל ולהפחית את סיכוני טכנולוגיית המידע באמצעות ממונה אבטחת מידע, עצמאי ואובייקטיבי, שיהיה מופרד כראוי מתהליכי תפעול טכנולוגיית המידע ושאינו המבקר. כמו כן, בעל רישיון נדרש לתחזק מיפוי עדכני של התהליכים העסקיים, תהליכים תומכים ונכסי מידע ולסווג אותם במונחים של חיוניות, בהתבסס על סודיות, אמינות וזמינות של מידע. בהמשך לכך, בעל רישיון נדרש להעריך את הסיכונים התפעוליים הקשורים לסיכוני טכנולוגיית מידע שמשפיעים עליו, וכן להחליט אילו אמצעים נדרשים כדי לצמצם את הסיכונים שזוהו. במסגרת ההוראה המוצעת יידרש בעל הרישיון לוודא את האפקטיביות של האמצעים לצמצום סיכונים בהם הוא נוקט, כפי שהוגדרו במסגרת ניהול הסיכונים שלו, זאת בפרט כאשר הוא נעזר בצדדים שלישיים. אמצעים להפחתת סיכונים בקשר לצדדים שלישיים כאמור ייקבעו במסגרת הסכמים והסדרי רמת שירות (Service Level Agreements), ואולם על בעל הרישיון לפקח, לנטר ולוודא את עמידתם של אותם צדדים שלישיים בהסכמים והסדרי רמת השירות;
- פרק ה׳ קובע את הדרישות בקשר עם אבטחת מידע כשהמידע מוחזק (held) במערכות טכנולוגיית המידע (ICT systems), לרבות דרישות ליישום אמצעי אבטחת מידע אפקטיביים; הכנה ויישום של מדיניות אבטחת מידע; הטמעה ובדיקת אמצעי אבטחת במידע; והכנת תכנית הדרכות לכל עובדי בעל הרישיון וצדדים שלישיים;
- 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; 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. בעל רישיון נדרש 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 בחינתן ועדכונן בהתבסס על תוצאות הבחינה. בעל רישיון נדרש לוודא שיש לו אמצעי תקשורת יעילים בעת משבר כך שכלל הגורמים הרלוונטיים יוכלו להיות מעודכנים באופן ובזמן ראוי;
- פרק ט׳ קובע את הדרישות בנוגע לניהול יחסי בעל הרישיון והלקוחות (PSUs – payment service users), כולל דרישות לאפשר ללקוח להשבית פונקציות תשלום ספציפיות (ככל שהדבר מתאפשר במסגרת השירות המוצע), וכן דרישות לתת ללקוחות המעוניינים בכך התראות לגבי ייזום עסקאות או ניסיונות כושלים ליזום עסקאות תשלום, ולספק ללקוחות תמיכה בנוגע לשאלות הקשורות לאבטחת מידע והגנת הפרטיות;

- פרק י' עוסק בדרישות שבעלי רישיון יעמדו בהוראות חוק הגנת הפרטיות והתקנות מכוחו, וכן שתקשורת של בעל רישיון המכילה מידע רגיש מול כל גורם, תעשה בפרוטוקול סטנדרטי ובתעבורה מוצפנת על פי הטכנולוגיות העדכניות הקיימות בשוק. עוד נקבעו שם דרישות בעניין תהליך ניטור והגבלת גישה למידע רגיש, וכן דרישות בעניין איסוף מידע סטטיסטי.

ביישום הוראה מוצעת זו, בעל רישיון ייקח בחשבון וישקול לאמץ תקנים בינלאומיים קיימים ושיטות עבודה מומלצים ומובילים (best practice standards) בתחום טכנולוגיית מידע ואבטחת מידע למגזר הפיננסי.

כמו כן, בעל רישיון יקיים הוראה זו באופן מלא ובהתחשב בגודלו, המבנה הארגוני הפנימי שלו, ואת אופי, היקף, מורכבות ומידת הסיכון המאפיינים את השירותים והמוצרים שבעל הרישיון נותן או מתכוון לתת.

<u>פטור מפרסום דוח הערכת רגולציה (RIA)</u>

בחודש נובמבר 2021 חוקק חוק עקרונות האסדרה, התשפ"ב–2021 (להלן: "**חוק עקרונות האסדרה**"). משכך, החל מחודש ינואר 2023, חלה על הרשות חובה לערוך דוח הערכת רגולציה (RIA) בהתאם לחוק זה. עם זאת, בחוק עקרונות האסדרה מנויים מספר חריגים, אשר בהתקיימם חל פטור מעריכת דוח כאמור.

לעמדת הרשות, נכון לפטור את טיוטת ההוראות מחובת RIA, זאת בהתבסס על החריג הקבוע בסעיף 34(ג)(4) לחוק עקרונות האסדרה הקובע פטור מפרסום דוח במקרה בו "האסדרה מבוססת, בהתאמות הנדרשות, על כללים מקובלים במדינות עם שווקים משמעותיים, המנחים את התאגיד הציבורי בתחום פעילותו". בדברי ההסבר לסעיף זה נכתב כי "אסדרה נוספת שהחובה לא תחול לגביה היא אסדרה שקידומה נועד להתאים את האסדרה הנוהגת באותו עניין ובאותה שעה, בישראל, לאסדרה בין־לאומית מקובלת או לאמנות בין־לאומיות. לדוגמה, אסדרה שמטרתה להתאים את האסדרה בתחום הבנקאות לעקרונות הליבה שנקבעו על-ידי ועדת בזל, או להתאים את האסדרה בתחום הביטוח למדיניות ארגון המפקחים הבינלאומי על הביטוח" (עמ' 1160).

כפי שתואר בהרחבה, ההוראות המוצעות, מבוססות על דרישות האסדרה האירופאית בנושא ניהול טכנולוגיית מידע, אבטחת מידע הגנת סייבר והמשכיות עסקית, בפרט הנחיות ה- European Banking Authority (EBA) בנושא ניהול סיכוני טכנולוגיית מידע ואבטחת מידע והנחיות EBA בנושא הגשת בקשת רישיון לעניין טכנולוגיית מידע ואבטחת מידע[4], אשר אומצו באנגליה על ידי ה- Financial Conduct Authority (FCA) (רשות ניירת ערך של בריטניה, אשר קלטה לדין המקומי הוראות רבות מתוך הדירקטיבה)[5]. עם זאת, יצוין כי נעשו כמה התאמות מינוריות יחסית למצב

[4] EBA Guidelines on ICT and security risk management under the Directive 2015/2366/EU (PSD2) (EBA/GL/2019/04); EBA Guidelines on Authorisations of Payment Institutions under PSD2 (EBA-GL-2017-09)

[5] פרק 18 ל- Our Approach: The FCA's role under the Payment – Payment Services and Electronic Money Services Regulations 2017 and the Electronic Money Regulations 2011.

בישראל, בעיקר בהיבטי הגנת הפרטיות מאחר שדיני הגנת הפרטיות בישראל ובאירופה אינם זהים. לאור האמור, מוצע לקבוע כי אסדרה זו חוסה תחת הפטור מכוח סעיף 34(ג)(4) לחוק עקרונות האסדרה.

להלן נוסח ההוראה המוצעת.

רשות ניירות ערך
Israel Securities Authority
سلطة الأوراق المالية

טיוטת הוראה לבעלי רישיון או אישור שירותי תשלום או ייזום בסיסי

בעניין אמצעים טכנולוגיים ואבטחת מידע

הוראה לפי סעיפים 4(א)(2), 5, 14(ג), 15(ב), 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

<u>פרק א' – הגדרות</u>

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 בעל הרישיון;

"**אירוע תפעולי או אירוע אבטחת מידע**" (Operational or Security Incident) – אירוע בודד או סדרה של אירועים קשורים, שלא תוכננו על-ידי בעל הרישיון, 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;

"**בעל רישיון**" – בעל רישיון או אישור מאת הרשות למתן שירותי תשלום או ייזום בסיסי, לפי העניין, אלא אם נאמר במפורש אחרת;

"**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 בעל רישיון, 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 שבעל הרישיון מוכן 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 בעל הרישיון;

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

"**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;

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

"**שירותי טכנולוגיית מידע**" (ICT services) – שירותים המסופקים על-ידי מערכות טכנולוגיות מידע למשתמש אחד או יותר, פנימי או חיצוני לבעל הרישיון, 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, שבעל רישיון מעוניין לספוג במסגרת מערך הסיכונים שלו (Risk Capacity) שלו בהתאם למודל העסקי שלו, כדי להשיג את יעדי אסטרטגיית טכנולוגיית המידע שלו, בכפוף לציות מלא להוראות הדין החלות עליו;

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

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

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

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

<u>פרק ב': ממשל תאגידי</u>

<u>סימן א': הדירקטוריון</u>

2. דירקטוריון החברה אחראי לפקח על נאותות הממשל התאגידי של בעל הרישיון, ובכלל זה:
   א. לגבש ולאשר אסטרטגיית טכנולוגיית מידע ולפקח אחר קיומה ויישומה, וזאת כחלק מהאסטרטגיה העסקית הכוללת של בעל הרישיון.
   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 בעל הרישיון, 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 בעל הרישיון. בהקשר זה, הדירקטוריון יוודא כי התקציב, המשאבים וכוח האדם המוקדשים להגשמת האמור בסעיף זה – מספקים, בשים לב בין היתר למאפייני בעל הרישיון, צרכיו, גודלו, מורכבות פעילותו והסיכונים הכרוכים בה.

ה. לוודא כי העובדים, לרבות בעלי תפקידים רלוונטיים לתחומים כמפורט בסעיף קטן ד, אצל בעל הרישיון, 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 93 להוראה, הכל לפחות אחת לשנה.

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

3. בעל רישיון ימנה 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 ניסיון וידע בניהול רכיבי אבטחה שיש לו הסמכה כדוגמת 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.

5. ממונה אבטחת מידע יהיה:

א. עצמאי, אובייקטיבי, מופרד מפעילות טכנולוגיית המידע בבעל הרישיון וכן לא ייקח חלק בביצוע ביקורת בבעל הרישיון;

ב. ימונה או יפוטר על ידי הדירקטוריון;

ג. בעל סמכויות, אחריות ומשאבים לפיקוח, ניטור ובקרה אחר עמידת בעל הרישיון בדרישות החוק, ההוראות מכוחו ובדרישות חוק הגנת הפרטיות ותקנותיו וכן אחר עמידת בעל הרישיון 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 בעל הרישיון 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. בעל הרישיון יתקשר עם מבקר שיערוך ביקורת עצמאית לגבי פעילות בעל הרישיון, לפי הוראות אלה:

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

(1) יחיד תושב ישראל;

(2) 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;

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

(4) 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 בעל הרישיון, לרבות בעניין ממשל תאגידי, מערכות ותהליכים הנוגעים להיבטי טכנולוגיית מידע ואבטחת מידע בבעל הרישיון וזאת, אל מול מסמכי מדיניות ונהלים הפנימיים של בעל הרישיון והוראות הדין הרלוונטיות.

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

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 בעל הרישיון, להנהלת החברה ולדירקטוריון, לפחות אחת לשנה.

8. בעל הרישיון יגבש ויישם תהליך מעקב רשמי אחר ממצאי הביקורות ויישום המלצותיהן, לרבות גיבוש הוראות לאימות ותיקון בזמן של ממצאי הביקורת המהותיים.

<u>**פרק ג': אסטרטגיית טכנולוגיית מידע**</u>

9. אסטרטגיית טכנולוגיית המידע של בעל הרישיון, תתיישב עם האסטרטגיה העסקית הכוללת שלו, ותתייחס בין היתר לנושאים הבאים:

א. האופן בו טכנולוגיית המידע, לרבות הארכיטקטורה של טכנולוגיית המידע, של בעל הרישיון צריכה להתפתח על מנת לתמוך ולקחת חלק באופן יעיל באסטרטגיה העסקית הכוללת של בעל הרישיון, 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. בעל הרישיון יגבש תכניות פעולה הכוללות אמצעים שינקוט ליישום והשגת מטרות אסטרטגיית טכנולוגיית המידע (להלן: "**תכניות הפעולה**"), וכן יוודא כי כלל הגורמים הרלוונטיים, בין אם פנימיים ובין אם חיצוניים, כדוגמת גורמים עימם בעל הרישיון התקשר בחוזה וספקים צדדים שלישיים, מכירים את התכניות כאמור ונוהגים לפיהן.

11. בעל הרישיון יבחן (Review) את תכניות הפעולה באופן תקופתי, לפחות פעם בשלוש שנים, על מנת להבטיח את הרלוונטיות והנאותות שלהן, וכן יגבש תהליכים למדידה וניטור אחר היעילות שבה אסטרטגיית טכנולוגיית המידע שלו מיושמת.

<u>**פרק ד': ניהול סיכוני טכנולוגיות מידע**</u>

<u>סימן א': ארגון ויעדים – כללי</u>

12. בעל רישיון יזהה את סיכוני טכנולוגיית המידע שלו וינהל אותם.

13. בעלי תפקידים בתחום טכנולוגיות מידע, כפי שהוגדרו ונקבעו על-ידי הדירקטוריון בעל הרישיון לפי סעיף 3(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 בעל הרישיון, וכן כי המערכות והשירותים המסופקים על-ידם עומדים בדרישות מדיניות ונהלים פנימיים של בעל הרישיון והוראות הדין הרלוונטיות.

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

14. בעל רישיון ימנה בעלי תפקידים, ויגדיר תחומי אחריות ועקרונות דיווח אשר יבטיחו את אפקטיביות מסגרת ניהול סיכוני טכנולוגיות מידע. מסגרת זו תוטמע באופן מלא בתהליך ניהול הסיכונים הכולל של בעל הרישיון, 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 בעל הרישיון.
ב. זיהוי, סיווג חיוניות והערכת סיכוני טכנולוגיית מידע אליהם חשוף בעל הרישיון, 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 בעל הרישיון.
ה. פעולות לתיקון וייעול הצעדים כאמור בסעיף קטן (ג), ככל שנדרש.
ו. דיווח לדירקטוריון על אודות סיכוני טכנולוגיית מידע רלוונטיים שזוהו על-ידי בעל הרישיון, 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. בעל הרישיון יוודא 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. בעל רישיון יזהה, יגבש ויתחזק מיפוי עדכני של התהליכים העסקיים והתהליכים התומכים אצלו, שעשויים להיות מושפעים מסיכוני טכנולוגיית מידע, במטרה לזהות את החשיבות של כל אחד מהתהליכים האמורים ואת התלות ההדדית שלהם.
19. בעל רישיון יזהה, יגבש ויתחזק 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, בעל הרישיון יסווג את התהליכים העסקיים, התהליכים התומכים ונכסי המידע

בהתאם למידת החיוניות שלהם לפעילותו ; סיווג חיוניות נכסי המידע, תתבסס, בין היתר, על המידה שבה הנכסים תומכים בפעילויות ובתהליכים העסקיים החיוניים שלו. כמו כן, לצורך סיווג חיוניות התהליכים העסקיים, התהליכים התומכים ונכסי המידע כאמור, בעל הרישיון ישקול, בין היתר, את דרישות הסודיות, אמינות והזמינות הרלוונטיות, לרבות לצורך עמידה בהסכם שנקבע עם הלקוחות.

<u>סימן ה' : הערכה וניטור סיכונים</u>

21. בעל הרישיון יזהה ויעריך 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. בעל הרישיון ינטר באופן שוטף אחר האיומים והחולשות הרלוונטיים לתהליכיו העסקיים, התהליכים התומכים ונכסי המידע, ויבחן 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, בעל הרישיון יקבע אילו אמצעים נדרשים לשם צמצום סיכוני טכנולוגיות מידע לרמה מקובלת, וכן יבחן אם נדרשים שינויים לתהליכים העסקיים, לבקרות ולמערכות טכנולוגיית מידע ושירותי טכנולוגיית מידע כתוצאה מהערכות הסיכונים כאמור. ככל ששינויים כאמור נדרשים, בעל הרישיון יבחן מהו משך הזמן הנדרש להטמעתם ואת הצורך בנקיטת צעדי ביניים לצמצום סיכוני טכנולוגיות מידע כך שלא יחרגו מגדרי תיאבון הסיכון שהוגדר על ידו.
25. בעל הרישיון יגדיר ויישם אמצעים הנדרשים לשם צמצום סיכוני טכנולוגיית מידע אשר זוהו על-ידו, וכן לשם הגנה על נכסי מידע, בהתאם לסיווג החיוניות שערך בעל הרישיון לפי סימן ד' לפרק זה.

<u>סימן ז' : שימוש בספקים צדדים שלישיים</u>

26. מבלי לגרוע מהוראות הרשות בנושא מיקור חוץ ומכלליות האמור בהוראה זו, בעת שימוש בספקים צדדים שלישיים (לרבות, בתוך קבוצה אליה משתייך בעל הרישיון), לשם ביצוע תהליכים תפעוליים של שירותי התשלום או כחלק משירותי טכנולוגיית מידע ומערכות טכנולוגיית מידע, בעל הרישיון יוודא את היעילות של האמצעים לצמצום סיכונים כפי שנקבעו במסגרת ניהול הסיכונים שלו, 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, בעל הרישיון יוודא כי החוזים והסכמי רמת השירות (Service Level Agreements), הן

במהלך העסקים הרגיל והן בעת התרחשות אירועים, מול הספקים השונים, כוללים את הנושאים הבאים:

א. יעדים וצעדים נאותים ופרופורציונאליים לניהול סיכוני אבטחת מידע, לרבות דרישות מינימום בעניין הגנת סייבר, מפרטי מחזורי החיים של המידע והנתונים של בעל הרישיון, דרישות הנוגעות להצפנת מידע, אבטחת רשתות ותהליכי ניטור אבטחת מידע, והמיקום של מרכזי הנתונים (Data Centers), וכן יוודא שקיימת הלימה בין החוזים והסכמי רמת השירות מול הספקים כאמור, לבין יעדי שירות של בעל הרישיון מול לקוחותיו ויעדי התאוששות שלו.

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

28. בעל הרישיון ינטר אחר רמת העמידה של ספקיו ביעדים בעניין אבטחת מידע והביצועים של בעל הרישיון, כפי שנקבעו בחוזים והסכמי רמת השירות שערך מול הספקים, ויוודא כי הם עומדים ביעדים כאמור.

פרק ה': אבטחת מידע

סימן א': **מדיניות אבטחת מידע**

29. בעל רישיון יגבש ויתעד מסמך מדיניות אבטחת מידע, במסגרתו יגדיר את העקרונות והכללים המרכזיים לשמירה על סודיות, אמינות וזמינות המידע והנתונים שלו ושל לקוחותיו.
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 בעל הרישיון, של המקורות ושל המידע הרגיש של בעל הרישיון, בעת אחסונו, בעת העברתו ובעת שימוש בו.
31. מדיניות אבטחת המידע תעמוד בהלימה ליעדי אבטחת המידע אשר יוגדרו על-ידי בעל הרישיון 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 בבעל הרישיון, וכן את קביעת הדרישות רלוונטיות בעבור צוותי העובדים, ספקים, תהליכים וטכנולוגיה לעניין אבטחת מידע, וזאת מתוך הכרה כי לעובדים, לרבות בעלי התפקידים של בעל הרישיון, בכל הרמות, וכן לגורמים עימם התקשר בעל הרישיון, ישנה אחריות לשמירת אבטחת המידע של בעל הרישיון.
33. מדיניות אבטחת המידע תאושר על-ידי הדירקטוריון, לפחות אחת לשלוש שנים.
34. כלל העובדים והספקים של בעל הרישיון יעודכנו לגבי מדיניות אבטחת המידע שלו.
35. בהתבסס על מדיניות אבטחת המידע, בעל הרישיון נדרש לגבש וליישם אמצעים לצמצום סיכוני טכנולוגיות מידע אליהם הוא חשוף. 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. בעל רישיון יגדיר, יתעד ויישם 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) בעל רישיון ינהל את הרשאות הגישה לנכסי מידע והמערכות התומכות בנכסים אלה על-בסיס עקרון הצורך לדעת. הרשאות אלה יכילו גם מענה לגישה מרחוק.

2) בעל הרישיון יעניק 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**: בעל רישיון יאסור את השימוש בחשבונות משתמשים גנריים או משותפים, ויבטיח שניתן יהיה לזהות את המשתמש לעניין כל פעולה המתבצעת במערכות טכנולוגיית המידע.

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

1) בעל רישיון יטמיע מנגנוני בקרה מוגברים, וינטר 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) בעל רישיון ייתן גישה מרחוק עם הרשאות ניהול (Administrative access) למערכות טכנולוגיית מידע חיוניות (Critical), רק על-בסיס עקרון הצורך לדעת ולשם ביצוע תפקידו, ותוך **שימוש באמצעי זיהוי חזקים** (– Strong authentication solutions Multi-Factor Authentication).

ד. **מעקב ותיעוד (Logging) פעילויות משתמש**: בעל הרישיון ינטר ויתעד (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**: בעל הרישיון יבחן 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**: בעל רישיון נדרש 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. בעל רישיון יגדיר, יתעד ויישם נהלי אבטחת מידע פיזיים שיגנו על מתקניו, מרכזי הנתונים (Data Centers) ואזורי עיבוד המידע מפני כניסה לא מורשית וסיכונים סביבתיים (Environmental hazards).
39. בעל רישיון יאפשר 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. בעל רישיון יבחן 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 בעל הרישיון 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. בעל רישיון יטמיע ויישם נהלים למניעה, ככל הניתן, של אירועי כשל, לרבות אירועי אבטחת מידע, במערכות טכנולוגיית מידע ובשירותי טכנולוגיית מידע, ויפעל 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 שמספק בעל הרישיון 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); בעל רישיון נדרש לבחון את עמידתן של יחידות הקצה כאמור בנהלי אבטחת המידע של בעל הרישיון, וזאת לפני הענקת גישה לרשת של בעל הרישיון;

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. בעל הרישיון יבחן 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 בעל רישיון, שיבטיח בחינה, תיעוד, אישור והוצאה אל הפועל של אותם שינויים.

<u>סימן ה': ניטור אבטחת מידע</u>

44. בעל רישיון יגבש ויטמיע נהלים לזיהוי פעולות חריגות שעלולות להשפיע על אבטחת המידע, ולתת מענה הולם לפעולות שכאלה. כחלק מהניטור המתמשך, בעל רישיון נדרש 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. בעל רישיון יטמיע תהליכים ויגבש מבנה ארגוני מתאימים, שיאפשרו לו לזהות ולנטר באופן קבוע איומי אבטחת מידע שעלולים להיות בעלי השפעה מהותית על יכולתו של בעל הרישיון לספק שירותים. מבלי לגרוע מכלליות האמור, בעל רישיון:

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

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

46. בעל הרישיון יישם את הליך ניטור אבטחת המידע באופן שיסייע לו להבין את מאפייני אירועי אבטחת המידע והתפעול, לזהות מגמות ולתמוך בהליכי התחקור הפנימיים של בעל הרישיון.

<u>סימן ו': ביקורת (Review), הערכה ובחינה (Testing) של אבטחת מידע</u>

47. בעל רישיון יערוך 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, ישקול לאמץ נהלים מקובלים לבחינות קוד מקור, הערכות חולשות (Vulnerability Assessments), ובדיקות חדירות (Penetration Tests).
48. בעל רישיון יגבש ויטמיע **מסגרת לבדיקת אבטחת מידע** שתתקף את האיתנות והיעילות של אמצעי אבטחת המידע של בעל הרישיון, 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 בעל הרישיון: (1) מסופי תשלום ומכשירים שמשמשים לאספקת שירותי תשלום; (2) מסופי תשלום במכשירים המשמשים לאימות זהות משתמשי שירותי התשלום (PSU - payment service users); (3) מכשירים ותוכנות בהם משתמש בעל הרישיון, אשר מפיקים עבור משתמש שירותי התשלום (PSU) קוד אימות.
49. בעל רישיון יוודא שהמסגרת לבדיקת אבטחת המידע כוללת בדיקות שיתקיימו לגביהן התנאים כדלהלן:
    א. הבדיקות יבוצעו על-ידי בודקים אובייקטיביים שלא מועסקים על-ידי בעל הרשיון, 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 בעל הרישיון.
50. בעל רישיון יבדוק את כלל אמצעי אבטחת המידע שלו באופן שוטף. מבלי לגרוע מכלליות האמור, בעל רישיון יבצע 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 שבעל הרישיון עורך בנוגע לשירותי התשלום שהוא מעניק.
    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. בעל רישיון יוודא 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, העלולים 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 שיקבע בעל הרישיון.

52. בעל רישיון ינטר באופן שוטף אחר תוצאות בדיקות אבטחת מידע ויעריכן, וכן יעדכן את אמצעי אבטחת המידע בהתאם אליהן בתוך זמן סביר. לעניין מערכות טכנולוגיית מידע חיוניות (critical) – בעל רישיון יעדכן את אמצעי אבטחת המידע כאמור בסעיף זה ללא דיחוי.
53. בהתבסס על איומי אבטחת מידע שנמצאו והשינויים שבוצעו כאמור בסעיף 52, יש להטמיע בהליכי הבדיקה תרחישים של איומים צפויים ורלוונטיים, וכן של תקיפות אפשריות או צפויות.

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

54. בעל רישיון יגבש 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 בעל הרישיון כשירים למלא את תפקידיהם באופן שהולם את מדיניות אבטחת המידע והנהלים של בעל הרשיון, לצמצם סיכונים לטעויות אנוש, גניבות, הונאות, שימוש לרעה או אובדן של מידע, וכן להתמודד עם סיכוני אבטחת מידע.
55. בעל רישיון יוודא שכלל המועסקים והגורמים הרלוונטיים שהתקשרו עמו, משתתפים בהדרכה בתחום אבטחת מידע כאמור בסעיף 54, ושיעילות ההדרכה האמורה נבחנת, הכל לפחות פעם אחת בשנה.

<u>**פרק ו': ניהול פעילות טכנולוגיית המידע**</u> (ICT Operations Management)

<u>סימן א': כללי</u>

56. בעל רישיון ינהל את פעילות טכנולוגיית המידע (ICT Operations) שלו בהתבסס על תהליכים ונהלים כתובים ומוטמעים, לרבות מסמך מדיניות אבטחת מידע, שאושרו על-ידי הדירקטוריון.
במסגרת המסמכים כאמור, בעל רישיון יגדיר כיצד הוא פועל, מנטר ושולט במערכות טכנולוגיית מידע ובשירותי טכנולוגיית מידע, ובכלל זה יתעד את פעילות טכנולוגיית המידע החיוניות (Critical ICT Operations).
57. בעל רישיון יוודא שפעילות טכנולוגיית המידע שלו מותאמות לדרישות העסקיות שלו, וכן יתחזק וישפר, ככל שיידרש, את יעילות פעילות טכנולוגיית המידע שלו, ובין היתר, יבחן כיצד לצמצם למינימום האפשרי שגיאות שעולות מביצוע ידני של משימות.
58. בעל רישיון יגבש ויטמיע נהלים לתיעוד (Logging) וניטור בעניין פעולות טכנולוגיית מידע חיוניות, שיאפשרו זיהוי, ניתוח ותיקון של שגיאות.
59. בעל רישיון יערוך 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. בעל רישיון ינטר וינהל את מחזור החיים של נכסי טכנולוגיית מידע, באופן שיבטיח שנכסים כאמור מתיישבים באופן שוטף עם הדרישות העסקיות ועם ניהול הסיכונים של בעל הרישיון, ותומכים בהם.
62. בעל רישיון יבדוק אם נכסי טכנולוגיית המידע שלו נתמכים על-ידי ספקים ומפתחים חיצוניים או פנימיים, ואם מיושמים לגביהם שדרוגים או תיקונים בהתבסס על תהליך מתועד.
63. בעל רישיון יעריך את הסיכונים שנובעים משימוש בנכסי טכנולוגיית מידע מיושנים או שאינם נתמכים טכנולוגית, ויצמצם.
64. בעל רישיון יטמיע תכנית ביצועים 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. בעל רישיון יגדיר ויטמיע 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 בעל הרישיון. בעל רישיון יבחן את נהלי הגיבוי והשחזור כאמור באופן תקופתי ולפחות אחת לשנתיים.
66. בעל רישיון יוודא 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. בעל רישיון יגבש ויישם 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 לבעל הרישיון 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 בעל הרישיון, שזוהו או אירעו אצל בעל הרישיון או אצל גורמים חיצוניים, הפקת לקחים מהניתוח האמור, ועדכון את אמצעי אבטחת המידע שלו 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 לבעל הרישיון, 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 בעל הרישיון שייקבעו בנוהל לעניין זה, תוך עמידה בזמנים ובהתאם להוראות דין אחרות הרלוונטיות לעניין זה.

<u>פרק ז': ניהול שינויים בתחום טכנולוגיית מידע</u>

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

68. בעל רישיון יגבש ויטמיע תהליכי רכש, פיתוח ותחזוקה של מערכות טכנולוגיית מידע, בהתאם לרמת הסיכון שהוגדרה לגביהן.
69. בעל רישיון יוודא 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 בבעל הרשיון.
70. בעל רישיון יבטיח שננקטים אמצעים למזעור הסיכון בדבר שינוי לא מכוון או מניפולציה מכוונת במערכות טכנולוגיית מידע, במהלך פיתוח והטמעה בסביבת הייצור.
71. בעל רישיון יגבש ויטמיע נוהל לבחינה ואישור של מערכות טכנולוגיית מידע טרם השימוש הראשון בהן. הנוהל יתחשב בחיוניות של התהליכים העסקיים, התהליכים התומכים ונכסי המידע. עוד במסגרת הבחינה יוודא בעל הרישיון שמערכות טכנולוגיית המידע פועלות כמצופה, וזאת תוך שימוש בסביבת בדיקות שמדמה באופן מספק את סביבת הייצור.
72. בעל רישיון יבחן את מערכות טכנולוגיית המידע, שירותי טכנולוגיית המידע ואמצעי אבטחת המידע, כדי לזהות חולשות, הפרות ושגיאות אבטחת מידע אפשריות, באופנים ובתדירות שהוא יקבע בנוהל.
73. בעל רישיון יטמיע 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, בעל רישיון יוודא הפרדה של סביבות הייצור מסביבות הפיתוח, הבדיקות וכל סביבה אחרת שאינה סביבת ייצור.
75. בעל רישיון יוודא את השלמות והסודיות של מידע מסביבת הייצור בסביבות שאינן סביבות ייצור.
76. בעל רישיון יוודא שהגישה למידע מסביבת הייצור תהיה מוגבלת למשתמשים המורשים לכך בלבד.
77. בעל רישיון יטמיע אמצעים להגנה על שלמות קוד המקור של מערכות טכנולוגיית מידע שפותחו אצל בעל הרישיון.
78. בעל רישיון יתעד 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 בעל רישיון, יחולו גם לעניין מערכות טכנולוגיית מידע שמפותחות או מנוהלות על-ידי משתמשי קצה עסקיים (Business Function's End Users) שלא מקרב בעל הרישיון, למשל, יישומי מחשב של משתמשי הקצה (end user computing applications), בהתאם לרמת הסיכון. בעל הרישיון יתחזק תיעוד של רשימת היישומים שתומכים בפעילות או תהליכים עסקיים חיוניים.

פרק ח': ניהול המשכיות עסקית

סימן א': כללי

80. פרק זה לא יחול על פעילות ייזום בסיסי.

סימן ב': תהליך ניהול המשכיות עסקית – כללי

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

סימן ג': ניתוח השפעות עסקיות

82. כחלק מתהליך ניהול המשכיות עסקית נאות, בעל רישיון יערוך ניתוח השפעות עסקיות (להלן: ניתוח השפעות עסקיות; Business Impact Analysis (BIA)) על-ידי בחינת חשיפתו 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 בעל הרישיון, וכן בהתחשב בתלות ההדדית שלהם, לפי פרק ד', סימנים ג' ו-ד' להוראה.

83. בעל רישיון יוודא כי מערכות טכנולוגיית מידע ושירותי טכנולוגיית מידע מתוכננים (designed) ומותאמים לניתוח ההשפעות העסקיות. כך למשל, בעל רישיון ידאג כי מערכות ושירותים כאמור מתוכננים ומותאמים ליתירות (redundancy) רכיבים חיוניים מסוימים כדי למנוע שיבושים הנגרמים מאירועי כשל המשפיעים על רכיבים אלה.

סימן ד': תכנית המשכיות עסקית

84. בהתבסס על ניתוח ההשפעות העסקיות (BIA), בעל רישיון יגבש תכנית המשכיות עסקית בכתב, לפי הוראה זו, אשר תאושר על-ידי הדירקטוריון.

85. תכנית המשכיות עסקית תיושם על-ידי בעל הרישיון, ותכלול, בין היתר, כדלהלן:

א. בחינה של מגוון אירועי כשל, ובכלל זה תרחישים חמורים אך מתקבלים על הדעת, אשר אליהם בעל הרישיון עלול להיות חשוף, 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 ינקוט בעל רישיון 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) שיקבע בעל הרישיון (להלן: "**הצעדים לתגובה והתאוששות**"), על מנת למנוע השפעות שליליות על פעילות בעל הרישיון והמערכת הפיננסית, ובכלל זה השפעות על מערכות התשלומים ולקוחות בעל הרישיון (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 בעל הרישיון יבצע גם כדלהלן:

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

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

(3) יפרט גם את הצעדים לתגובה והתאוששות בהם ינקוט על מנת לצמצם כשלים של צדדים שלישיים בעלי חשיבות מרכזית להמשכיות שירותי טכנולוגיית מידע של בעל הרישיון.

ג. בקביעת הצעדים לתגובה והתאוששות כאמור בסעיף קטן (ב), בעל רישיון ייקח 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.

86. בקרות אירוע כשל שגורם להפעלה של תכנית המשכיות עסקית, בעל רישיון יתעדף פעולות המשכיות עסקית בהתחשב ברמת הסיכון והערכות סיכונים שבוצעו במסגרת ניהול סיכוני טכנולוגיית מידע שערך בעל הרישיון.

87. בעל רישיון יערוך את תכנית ההמשכיות העסקית בתיאום עם הגורמים הרלוונטיים, פנימיים או חיצוניים.

88. בעל רישיון יתעד את תכנית ההמשכיות העסקית ויוודא כי היא נגישה לעובדי החברה הרלוונטיים, לרבות צדדים שלישיים רלוונטיים, בכלל ובפרט במקרה חירום.

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

89. בעל רישיון יבחן את תכנית ההמשכיות העסקית שלו באופן תקופתי. בפרט, בעל רישיון יוודא כי תכנית ההמשכיות העסקית שלו, בכל הנוגע לתהליכים עסקיים, תהליכים תומכים ונכסי מידע חיוניים (לרבות אלו המסופקים על-ידי צדדים שלישיים), נבחנת לפחות אחת לשנה, כפי שמפורט להלן בסעיף 91.

90. בעל הרישיון יוודא 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.

91. בחינת תכנית ההמשכיות העסקית על-ידי בעל הרישיון תיערך במטרה להבטיח כי בעל הרישיון מסוגל להמשיך ולקיים את פעילותו 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.
92. בעל הרישיון יתעד את תוצאות בחינת תכנית ההמשכיות העסקית, ינתח את החולשות אם נמצאו במהלך הבחינה ויטפל בהן.
93. בעל הרישיון ידווח לדירקטוריון את תוצאות בחינת תכנית ההמשכיות העסקית, ניתוח החולשות ואופן הטיפול בהן, כאמור בסעיף 92, לפחות אחת לשנה.

<u>סימן ו': תקשורת בעת אירוע כשל</u>

94. בעל רישיון יוודא כי עומדים לרשותו 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.

<u>פרק ט': ניהול יחסי בעל רישיון ולקוחות (Users)</u>

95. התחברות לקוח למערכת של בעל רישיון תתאפשר לאחר שבעל הרישיון זיהה את הלקוח באמצעי זיהוי חזקים (Multi-Factor Authentication).
96. בעל רישיון יעניק ללקוחות סיוע והכוונה ללקוחות (משתמשי שירות התשלום (PSUs)) להגברת מודעותם לגבי סיכוני אבטחת מידע והגנת הפרטיות הקשורים לשירותי התשלום, לפחות במסגרת מערכת בעל הרישיון, וכן יאפשר ללקוחות לפנות אליו בקשר עם שאלות או בקשות לתמיכה בנושאים האמורים ובאמצעי קשר שיפורט שם.
97. בעל הרישיון יאפשר ללקוחות להשבית (to disable) פונקציות תשלום מסוימות הקשורות לשירותי התשלום שמציע בעל הרישיון ללקוחות, ככל שהדבר מתאפשר במסגרת השירות המוצע.

98. כאשר ישנו הסכם בין בעל רישיון ולקוח בדבר מגבלות סכום (Spending Limits) בעסקאות תשלום המבוצעות באמצעות אמצעי תשלום (Payment Instrument) מסוים, בעל הרישיון יספק ללקוח את האפשרות להתאים (adjust) את המגבלות האמורות עד למגבלת המקסימום שהוסכם לגביה.

99. בעל הרישיון יספק ללקוחות המעוניינים בכך את האפשרות לקבל התראות לגבי ייזום של עסקאות תשלום או ניסיונות כושלים לייזום עסקאות תשלום, באופן שיאפשר להם לזהות הונאות או שימוש לרעה בחשבונותיהם.

<u>פרק י': הגנת הפרטיות ואבטחת מידע</u>

100. בעל רישיון יעמוד בכל עת ולגבי כל פעילויותיו מכוח הרישיון, בהוראות הקבועות בחוק הגנת הפרטיות, התקנות והצווים לפיו, ולעניין הוראות אלו, בעל רישיון או אישור המנהל מאגר מידע אשר חלה עליו רמת האבטחה הבסיסית, כהגדרתה בתקנות הגנת הפרטיות, יעמוד בכל עת בדרישות החלות על מאגר מידע אשר חלה עליו רמת אבטחה בינונית לכל הפחות.

101. 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.

102. בעל רישיון לא ייגש, יעבד או ישמור מידע רגיש, אלא אם הוא נחוץ לצורך מתן שירותי תשלום או שירות ייזום בסיסי, ובכפוף לקבלת הסכמה מפורשת של הלקוח (PSU).

103. תקשורת של בעל רישיון המכילה מידע רגיש מול כל גורם, תיעשה בפרוטוקול סטנדרטי ובתעבורה מוצפנת על פי הטכנולוגיות העדכניות הקיימות בשוק.

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

בעל רישיון יגבש ויישם 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, <u>למעט אם מדובר במבקש המתכוון לתת רק ייזום תשלומים</u>.

ו. אמצעי אבטחת מידע טכניים ומערכות מידע (IT systems) שהוטמעו, לרבות הצפנה (Encryption and/or tokenisation).

ז. זהות האנשים, הגופים והוועדות שיש להם גישה למידע הרגיש.

ח. הסבר על אודות דרך גילוי הפרות וטיפול בהן.