

# ניהול המידע והגנתו

## תוכן

3	פרק א': כללי
3	מבוא
3	תחולה
3	הגדרות
5	פרק ב': פיקוח וניהול
5	דירקטוריון לשכת אשראי
5	הנהלת לשכת אשראי
6	ממונה על אבטחת מידע
7	ביקורת פנימית
7	דיווחים לממונה
10	פרק ג': הגנת המידע
10	מסגרת עבודה (Framework) לניהול הגנת מידע
10	סקר הערכת סיכוני אבטחת מידע ומבחני חדירה
11	איסוף מודיעין
12	בקרה וניטור
13	תהליכי פיתוח, תחזוקה וניהול שינויים
14	אבטחת רשת וגישה מרחוק
15	קישוריות לרשת האינטרנט
15	מניעת דלף מידע ואובדן מידע
16	קבלה והצפנת נתונים
16	אבטחת מערכות ועדכון
17	אבטחת מערכות קצה
17	מניעת קוד עיון
18	שימוש במכשירים ניידים
18	הפרדה בין סביבות ואבטחתן
19	ניהול משתמשים
20	סיסמאות ואמצעי הזדהות
21	ניהול הרשאות ובקרת גישה
22	יישום בקרות
22	תכנית היערכות לניהול אירועי אבטחת מידע
23	מיקור חוץ (Outsourcing)
25	שירותי מחשוב ענן

**26 ..... פרק ד': הגנה פיסית**

26..... אבטחה פיסית.

27..... אבטחת ציוד וניירת

27..... תחקור אירועי אבטחת פיסית

**28 ..... פרק ה': משאבי אנוש והדרכה**

28..... גיוס עובדים

28..... הוראות לעניין יישום נהלי אבטחת מידע

29..... ניווד או סיום העסקה

29..... עובדי חוץ ומבקרים

29..... הדרכה

**31 ..... פרק ו': פעילות בערוצי תקשורת**

31..... בקרות בתהליך הרישום לביצוע פעולות

31..... בקרה על הזדהות לקוחות

31..... ניהול סיסמאות לקוח

32..... מסירת מידע באמצעים דיגיטליים

**33 ..... פרק ז': תיעוד, מחיקה, אחזור וגיבוי המידע, והפסקת פעילות לשכה**

33..... תיעוד

33..... מחיקת מידע

34..... אחזור מידע

34..... גיבוי ואחזור נתונים

34..... סיום או הפסקת פעילות לשכה

## פרק א': כללי

### מבוא

1. ניהול נכסי המידע וההגנה עליהם מהווה רכיב מרכזי בהפעלת שירות נתוני אשראי ושירות מידע על עוסקים. על מנת להבטיח את הפעלתם התקינה והרציפה של שירותים אלו, נדרשים משאבים ניהוליים, כספיים ואחרים לניהול והגנה על המידע הנאסף, הנוצר והנמסר על ידי לשכה.
2. ניהול נכסי המידע כולל פעולות של זיהוי, הערכה, מניעה, והתמודדות עם איומים על שלמות ודיוק המידע, ועל שימוש אסור בו, בטרם התממשותם, במהלך התממשותם ולאחריהם.
3. מתוקף סמכות הממונה לפי סעיף 68 לחוק נתוני אשראי, התשע"ו-2016 (להלן – **החוק**), ולאחר התייעצות בוועדה המייעצת, נקבעה הוראה זו הקובעת עקרונות וכללים לניהול והגנה על נכסי המידע שבידי הלשכה באופן שתשמר פרטיות הקוחות, תובטח שלמות המידע וזמינותו, וימוזער הסיכון לחשיפת או העברת המידע לגורמים שלא הורשו להחשף לו. למען הסר ספק, הוראה זו אינה גורעת מהדרישות הנוספות הקבועות בהוראות הדין השונות, לרבות חוק הגנת הפרטיות, תשמ"א-1981 (להלן – **חוק הגנת הפרטיות**) ותקנותיו, וכללי נתוני אשראי (אבטחת מידע), התשע"ט-2018.
4. על לשכת מידע על עוסקים חלות ההוראות הקבועות בהוראות הדין השונות, לרבות חוק הגנת הפרטיות ותקנותיו.
4. לאור חשיבות פעילות הלשכה והצורך לשמור על פרטיות לקוחות הלשכה, מצופה ממנה לאמץ סטנדרטים גבוהים לניהול הגנת המידע ואבטחתו.

### תחולה

5. הוראה זו חלה על לשכת אשראי (להלן – **הלשכה** או **לשכת אשראי**).
6. ההוראה חלה על פעילות לשכת האשראי במתן שירותים לפי סעיפים 12 ו-13 לחוק, לרבות עיסוקים אשר הותרו לה לפי כללי נתוני אשראי (הוראות שונות), התשע"ח-2017.
7. בוטל.
8. בוטל.
9. הממונה רשאי לפטור לשכת אשראי מסוימת מקיום סעיפים מסוימים בהוראה זו, או לקבוע הוראות מסוימות שונות מאלו המפורטות להלן אשר יחולו על לשכת אשראי מסוימת. זאת, במקרים חריגים לאחר שבחן את בקשתה ונימוקה אשר נמסרו לו בכתב, ורשאי הממונה לקבוע כי הפטור או ההוראות השונות יחולו לתקופה קצובה כפי שתיקבע על ידו.

### הגדרות

10.

כללי אבטחת מידע"	- כללי נתוני אשראי (אבטחת מידע), התשע"ט-2018 ;
"מידע רגיש"	- כהגדרתו בחוק הגנת הפרטיות, תשמ"א-1981, וכל מידע אשר סווג על ידי הלשכה כמידע רגיש לעניין הוראה זו ;

<p>- כלל המערכות התומכות בפעילות העסקית ואשר יש להן חשיבות בהיבטי אבטחת מידע, לרבות ציוד ממוכן, תשתיות וטכנולוגיות התומכות בתפעולן, בין היתר: שרתים, ציוד תקשורת, ציוד הגנת מידע, כלי פיתוח ואמצעי אבטחה;</p>	<p><b>"מערכות מידע"</b></p>
<p>- נכס מידע הוא מאגר נתונים, התקן, או רכיב של סביבה התומך בפעילויות הקשורות במידע (לרבות תשתיות). נכסי מידע כוללים, בדרך כלל, חומרה, תוכנה ומידע;</p>	<p><b>"נכסי מידע"</b></p>
<p>- תיעוד פעולות המתבצעות במערכות מידע. התיעוד מקשר את הפעולה לנתונים כגון: שם מבצע הפעולה, המועד, הפעולה עצמה ועוד לצורך זיהוי האלמנטים שהשתנו;</p>	<p><b>"נתיב בקרה"</b></p>
<p>- קוד המושתל על ידי משתמש זדוני ועשוי לגרום לביצוע פעולות לא רצויות, פגיעה במערכות הלשכה ודלף מידע רגיש לגורמים לא מורשים;</p>	<p><b>"קוד עיון"</b></p>
<p>- קבוצת מחשבים המקושרים זה לזה בעזרת ציוד תקשורת ונגישים למשאבים בתוך הלשכה. במובן של הוראה זו, רשת פנימית הנה רשת המופרדת מרשתות ציבוריות;</p>	<p><b>"רשת פנימית – (LAN) "Local Area Network"</b></p>
<p>- תהליך אימות המורכב לפחות משני גורמי אימות, משתי קטגוריות שונות, המפורטים להלן: (1) פריט הנמצא ברשות המשתמש, לדוגמה: סיסמה חד-פעמית זמנית (OTP-One Time Password) הנוצרת על ידי רכיב חומרה הנמצא בידי המשתמש ומקושר לחשבון שלו, סיסמה חד פעמית זמנית הנוצרת על ידי נותן השירות ומועברת ללקוח על ידי מסרון ולעניין זה לרבות מסרון קולי, או תעודה דיגיטלית הנשמרת בכרטיס חכם או רכיב אחר אשר ברשות המשתמש; (2) פריט הידוע רק למשתמש, לדוגמה: סיסמה קבועה; (3) פריט שהוא המשתמש, לרבות מאפיין ביומטרי, כגון: זיהוי קולי, טביעת אצבע וזיהוי פנים.</p>	<p><b>תהליך "Multi-Factor Authentication (MFA)"</b></p>
<p>- כהגדרתה בסעיף 5 לכללי אבטחת מידע;</p>	<p><b>"תעודה אלקטרונית"</b></p>
<p>- איום אזרחי, או אבטחתי, או כלכלי, או אחר על הלשכה העלול לגרום נזק מלא או חלקי לתפקודה ולהשבתה חלקית או מלאה של תהליכים עסקיים או מתן שרות.</p>	<p><b>"תרחיש איום"</b></p>

## פרק ב': פיקוח וניהול

### דירקטוריון לשכת אשראי

11. הדירקטוריון ידון במסמך המדיניות לניהול המידע והגנתו ויאשר אותו, לפחות אחת לשנה וכן בעת ביצוע שינוי מהותי בתהליכים עסקיים, או בסביבה הטכנולוגית או בחשיפה לסיכונים (להלן: "שינוי מהותי").
12. מסמך המדיניות יכלול, בין היתר, התייחסות לנושאים הבאים:
  - 12.1. מטרות השימוש במידע;
  - 12.2. סוגי המידע השונים הכלולים במאגר המידע;
  - 12.3. הסיכונים העיקריים של פגיעה באבטחת המידע ואופן ההתמודדות עימם;
  - 12.4. תפיסת הגנת המידע- אבטחת המידע והגנת הפרטיות;
  - 12.5. האמצעים שיש לנקוט והמשאבים שיש להקדיש לצורך הגנה על נכסי המידע;
  - 12.6. עקרונות גיבוי ואחזור נתונים במצבים של תקלות והתממשות תרחישי איום;
  - 12.7. מיקור חוץ;
  - 12.8. פיתוח ושינויים במערכות מידע, לרבות שימוש בטכנולוגיות חדשות;
  - 12.9. נושאים שהוגדרו ע"י בעל מאגר המידע במסמך "הגדרות המאגר" כמפורט בסעיף 2(א) בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017;
  - 12.10. אירועי אבטחת מידע מהותיים המחייבים דיווח מיידי לדירקטוריון;
  - 12.11. הגדרת דיווחים נוספים לממונה, מעבר לדיווחים שנקבעו בסעיף 27 להלן.
13. הדירקטוריון ידון לפחות אחת לשנה וכן בעת ביצוע שינוי מהותי, בחשיפות לסיכונים הנובעים מניהול המידע והגנתו, כפי שעולים מסקר הסיכונים ומבחני החדירה, מממצאי דוחות ביקורת בנושא אבטחת מידע והגנת הפרטיות, ומתמונת המצב אודות איומי אבטחת מידע וסייבר כמפורט בסעיפים 44-א-44, וכן ידון בתכנית להפחתת סיכונים, ובתכנית העבודה הרב שנתית שנקבעה על ידי ההנהלה ויאשר אותה.
14. הדירקטוריון ידון לפחות אחת לשנה בתכנית היערכות לניהול אירועי אבטחת מידע בהתאם לסעיפים 121 עד 128, וכן באירועי אבטחת מידע מהותיים שהתרחשו ובהחלטות והפעולות שבוצעו.

### הנהלת לשכת האשראי

15. ההנהלה תקיים מסגרת עבודה מתאימה שתבטיח, בין היתר, יישום אפקטיבי של מדיניות הדירקטוריון.
- 15א. ההנהלה תגבש מסמך מדיניות לניהול המידע והגנתו, תבחן את הצורך לעדכנו לכל הפחות אחת לשנה וכן בכל שינוי מהותי, ותעביר המלצותיה לדירקטוריון.
16. ההנהלה תדון באופן שוטף בנושאים המפורטים להלן, ובהתאם לכך, תגבש תכנית להפחתת הסיכונים, ותבחן את הצורך בעדכון נוהלי העבודה ואמצעי הבקרה ואבטחת המידע:
  - 16.1. תוצאות מסמך סקרי הסיכונים ומבחני החדירה בדגש על הסיכונים המרכזיים;

- 16.2. ממצאי דוחות ביקורת בנושא אבטחת מידע והגנת הפרטיות של המבקר הפנימי ושל הממונה שיועברו אליה ;
- 16.3. תמונת מצב אודות איומי אבטחת מידע וסייבר כמפורט בסעיפים 44א-44ב, לרבות אמצעים שננקטו לצמצום החשיפות.
- 16א. ההנהלה תקבע תכנית עבודה רב-שנתית בתחום ניהול המידע והגנתו, בין היתר, בהתאם לחשיפות לסיכונים הנובעים מניהול המידע והגנתו ולתכנית להפחתתם, וכן בהתאם לתכנית העסקית של הלשכה, תעמיד לה משאבים נאותים, ותעקוב לכל הפחות ברמה רבעונית אחר יישומה.
17. בוטל.
18. לפחות אחת לרבעון, תדון ההנהלה באירועי אבטחת מידע שהתרחשו (לרבות כאלו שלא הובילו לפגיעה חמורה) ההחלטות והפעולות שבוצעו.
19. ההנהלה תיקבע ותקיים מבנה ארגוני הולם לניהול המידע והגנתו ותגדיר את אחריות הגורמים העוסקים בתחום לרבות אחריות דיווחית, וקיום מנגנוני פיקוח ובקרה תוך שמירה על עקרונות של הפרדת תפקידים וסמכויות.
20. ההנהלה תגדיר את סוגי הפעילויות והאירועים לגביהם נדרש דווח, לרבות דיווח בזמן אמת, והגורמים המוסמכים לטיפול באירועים כאמור.
- 20א. ההנהלה תדווח לדירקטוריון, לפחות אחת לשנה, על אופן יישום תכנית העבודה הרב שנתית ותכנית ההיערכות לניהול אירועי אבטחת מידע בהתאם לסעיפים 121 עד 128.

#### ממונה על אבטחת מידע

21. הנהלת לשכת אשראי תמנה ממונה על אבטחת מידע בעל הכשרה וניסיון מתאימים שיפעל בכפיפות ישירה למנכ"ל או לנושא משרה בכירה אחר הכפוף ישירות למנכ"ל, ויהיה אחראי למכלול הנושאים הקשורים לניהול המידע וההגנתו, כמפורט בהוראה זו.
22. הממונה על אבטחת מידע לא ישא באחריות לניהול טכנולוגיות המידע או בכל תפקיד אחר שעלול לפגוע ביכולתו לבצע כראוי את תפקידו או להגבילו. הממונה על אבטחת מידע יכול להיות עובד במשרה חלקית בתנאי שהיקף משרתו יהיה תואם את מידת החשיפה של המערכת לאיומים, או יועץ חיצוני.
23. ההנהלה תקצה לממונה על אבטחת המידע את המשאבים הדרושים לו לשם מילוי תפקידו.
24. הממונה על אבטחת מידע יפעל כדלקמן :
- 24.1. יכין נוהל אבטחת מידע ויביאו לאישור ההנהלה.
- 24.2. יעדכן את נוהל אבטחת המידע, ויביאו לאישור ההנהלה, לכל הפחות אחת לשנה או כאשר זיהה שינויים מהותיים במערכות המאגר ובתהליכי עיבוד מידע או בחשיפות לסיכונים.
- 24.3. יכין תכנית לבקרה שוטפת אחר העמידה בדרישות חוק הגנת הפרטיות ותקנותיו, יבצע אותה ויודיע להנהלת הלשכה על ממצאיו.

- 24.4. יעקוב אחר אופן יישום והטמעת מדיניות ונוהלי אבטחת מידע, המלצות הסקרים וביקורות המבקר הפנימי והממונה והנחיות החוק הרלבנטי.
- 24.5. יגדיר דרישות להגנה על המידע בכל מערכת חדשה שנקתה או פותחה, ובעת שדרוג של מערכות מידע קיימות ויהיה מעורב ביישום תהליכי רכש או פיתוח של מערכות חדשות ובעת שדרוג מערכות קיימות.
- 24.6. במקרים בהם חשיפות בסיכון גבוה לא טופלו במהלך תקופה של שלושה חודשים מביצוע סקר אבטחת המידע, יבחן הממונה על אבטחת המידע את הסיבות לאי הטיפול בחשיפות אלו, ויעביר המלצותיו בנושא לדירקטוריון ולהנהלה.
- 24.7. יתחקר אירועים חריגים ויעביר המלצותיו למנכ"ל תוך פרק זמן סביר שלא יעלה על 30 יום.
- 24.8. יבחן מעת לעת את תהליכי ניטור המידע שהוגדרו, תקינותם ואיכות האירועים שמתקבלים, ולכל הפחות אחת לשנה.
- 24.9. ינחה מקצועית את הארגון בנושאי אבטחת מידע והגנת הפרטיות.
- 24.10. יבחן באופן שוטף, האם אין המידע שנשמר במאגר רב מהנדרש לצורך עמידה במטרות המאגר ודרישות החוק.
- 24.11. יגבש תמונת מצב אודות איומי אבטחת מידע וסייבר, כמפורט בסעיפים 44א-44ב, יפעל להפקת לקחים במקרה של התממשות אירועי אבטחת מידע וסייבר, ליישום מסקנות רלוונטיות ולצמצום החשיפות לאיומים, וכן ידווח להנהלה באופן שוטף על תמונת המצב ועל האמצעים שננקטו לצמצום החשיפות.

#### ביקורת פנימית

25. תכנית הביקורת הפנימית תכלול ביקורת, שתתבצע אחת לשנתיים לפחות לבחינת מסגרת העבודה הכוללת לניהול המידע והגנתו.
26. הביקורת תעשה ע"י גורם בעל הכשרה וניסיון מתאימים לביצוע ביקורת בנושא אבטחת מידע, לרבות ע"י גורם חיצוני בלתי תלוי.

#### דיווחים לממונה

27. הלשכה תעביר לממונה דיווח על אירוע משמעותי בתחום ניהול המידע והגנתו, או על חשד ממשי לאירוע כאמור, במקרים הבאים:
- 27.1. אירוע של פגיעה בשלמות המידע;
- 27.2. אירוע שנעשה בו שימוש במידע בלא הרשאה או בחריגה מהרשאה;
- 27.3. נפגעו או הושבתו מערכות ייצור המכילות מידע רגיש ליותר מ-3 שעות, למעט השבתה יזומה;
- 27.4. יש אינדיקציות לכך שמידע רגיש אודות לקוחות הלשכה נחשף או דלף אל מחוץ לחצרות הלשכה;

- 27.5. התממשות אירועים חריגים, לרבות ניסיונות מהותיים של חדירה ותקיפה, חדירה בפועל למערכות מחשב, קריסה של מערכות מרכזיות, הפעלת תכנית להתמודדות עם אירועים חריגים וכיוצא באלה;
- 27.6. הפסקה של שירותים מהותיים כתוצאה מהשבתה לא מתוכננת של פעילות המערכות הממוכנות למשך יום עסקים אחד או יותר;
- 27.7. אירוע של שימוש ללא הרשאה בתעודה האלקטרונית;
- 27.7א. אירוע אשר הטיפול בו דורש מעורבות משמעותית של מנהל הגנת הסייבר, ואשר הטיפול בו לא הסתיים תוך שעתיים ממועד זיהויו לראשונה;
- 27.7ב. אירוע שהינו בעל מאפייני תקיפה חדשים או רמת מורכבות גבוהה;
- 27.8. כל אירוע משמעותי אחר שהתרחש בעל השפעה מהותית על ניהול המידע והגנתו;
- 27.9. כל אירוע כמפורט לעיל בסעיפים 27.1 עד 27.8 שכמעט והתרחש.
- דיווח על אירוע משמעותי שהתרחש יועבר לממונה טלפונית או בכתב תוך שעתיים ממועד הזיהוי הראשוני של האירוע כמחייב דיווח (להלן – **דיווח ראשוני**). השלמת הדיווח תתבצע בכתב בתוך 8 שעות ממועד הדיווח הראשוני (להלן – **דיווח משלים**). הדיווח הראשוני והדיווח המשלים יכללו את הפרטים הידועים נכון למועד מסירת הדיווח.
- ככל שתהיינה התפתחויות מהותיות במהלך האירוע, על הלשכה לעדכן את הממונה על התפתחויות אלו. כמו כן, יש לעדכן את הממונה על סיום האירוע.
- דיווח על אירוע שכמעט והתרחש יועבר לממונה בכתב תוך 7 ימים ממועד הזיהוי הראשוני של האירוע כמחייב דיווח.
28. הלשכה תדווח לממונה על תוצאות התחקיר שבוצע בעקבות המקרים המפורטים בסעיף 27 לעיל, ועל הלקחים והפעולות שבוצעו בעקבותיהם ככל שנדרש. דיווח ראשון יועבר לממונה תוך 3 ימים ודיווח נוסף תוך 30 ימים מהמועד שהאירוע הסתיים, או תוך 45 יום ממועד הזיהוי הראשוני של האירוע כמחייב דיווח, לפי המוקדם מביניהם.
29. למען הסר ספק, דיווח לממונה בקרות אירוע אבטחת מידע אינו גורע מחובת הדיווח לגורמים שנדרש לדווח להם בהתאם להוראות הדין, לרבות דיווח לרשות להגנת הפרטיות בהתאם לתקנות הגנת הפרטיות (אבטחת מידע). בנוסף, הממונה רשאי להורות ללשכה, להודיע לגורמים נוספים על אירוע האבטחה בהתאם לנסיבות.
30. הלשכה תעביר לממונה, מראש ולא יאוחר מ-30 ימים לפני האירוע או השינוי, דיווחים לגבי הנושאים הבאים:
- 30.1. שינויים מהותיים צפויים במדיניות ניהול טכנולוגיית המידע;
- 30.2. הסבה מהותית של מערכות מחשב או מחשב מחדש של מערכות מרכזיות ודומיהם;
- 30.3. שינוי מהותי בערוצי התקשורת;
- 30.4. יוזמה טכנולוגית חדשה;
- 30.5. כל נושא אחר בעל השפעה מהותית על ניהול המידע והגנתו.





31. הלשכה תעביר לממונה את סקרי אבטחת המידע ואת תוצאות מבחני החדירה לא יאוחר מ- 14 ימים מעת ביצועם, ואת התכנית להפחתת הסיכונים אשר עלו מסקרי אבטחת המידע וממבחני החדירה לא יאוחר מעשרה ימים מהמועד האמור.

## פרק ג': הגנת המידע

### מסגרת עבודה (Framework) לניהול הגנת מידע

32. הלשכה תקבע מסגרת עבודה לניהול הגנת המידע, שתתייחס בין היתר לנושאים הבאים:
- 32.1. מדיניות לניהול המידע והגנתו שתתבסס על תפיסת הגנת המידע לכל הפחות כמפורט בהוראה זו;
  - 32.2. סקר הערכת סיכוני אבטחת מידע ומבחני חדירה כחלק מסקר הערכת סיכונים כאמור בהוראה לגבי ניהול סיכונים;
  - 32.3. מסגרת ארגונית הכוללת סמכויות ותחומי אחריות, קווי דיווח, גופי פיקוח ובקרה, היבטים של משאבי אנוש והדרכות;
  - 32.4. נהלי עבודה שיעברו תהליך עדכון בהתאם לצורך, עם כל שינוי משמעותי בסביבה הטכנולוגית או שינוי במתאר הסיכונים של הלשכה, ולכל הפחות אחת ל – 24 חודשים.
  - 32.5. כללים ותהליך עבודה לזיהוי וסיווג המידע שיכללו:
    - 32.5.1. זיהוי המידע הקיים בלשכה ומיפוי מערכות המידע בהן הוא מאוחסן, פירוט אופן זרימת המידע בין המערכות השונות ומיפוי ערוצי התקשורת של הלשכה עם לקוחותיה (Data Discovery).
    - 32.5.2. סיווג המידע לקטגוריות, כגון: מידע אישי רגיש, מידע אישי אחר, מידע עסקי רגיש, מידע פומבי (Data Classification).

### סקר הערכת סיכוני אבטחת מידע ומבחני חדירה

33. הלשכה תיישם, כחלק מתכנית העבודה הרב-שנתית סקר אבטחת מידע ומבחני חדירה המכסים את מערכות המידע והתהליכים הארגוניים ותיישם תכנית להפחתת סיכונים.
34. הסקר ומבחני החדירה (להלן - **הסקרים**) יבחנו את התאמת כל מערכות המידע והתהליכים העסקיים למדיניות ולנוהלי אבטחת המידע של הלשכה, לרבות ברמת בדיקת קיום ואפקטיביות הבקורות להגנה על המידע בפני סיכונים פנימיים וחיצוניים.
35. הערכת הסיכונים תתייחס למכלול של איומים פוטנציאליים, ביניהם משתמשי המערכת, סביבת המערכת ומיקור חוץ.
36. הערכת הסיכונים תתייחס הן לסביבת הייצור (Operation Technology) והן לסביבות הפיתוח הבדיקות והגיבוי, המכילות מידע רגיש.
37. לצורך זיהוי הסיכונים והערכתם, הלשכה תשתמש, בין היתר, במיפוי תהליכים עסקיים ומערכות הקשורות אליהן, בממצאי ביקורות, באיסוף וניתוח אירועים פנימיים וחיצוניים הנוגעים להגנת המידע שהתרחשו ובניתוח תרחישים לזיהוי אירועים פוטנציאליים של התממשות הסיכון.

38. תכנית העבודה לביצוע הסקרים תיישם את הנושאים הבאים:
- 38.1. כיסוי של כל רמות האבטחה של התהליכים והמערכות, לרבות: הגנות פיסיות וסביבתיות, הגנות תשתיות הכוללות אחסון, מערכות הפעלה, רשתות, בסיסי נתונים, רכיבי תווכה (Middleware) ודומיהם, הגנות אפליקטיביות, הגנות ברמת הלוגיקה העסקית המיושמות במערכת וכן התהליכים הסובבים את המערכת כגון ניהול משתמשים והרשאות, תהליכי גיבוי, ניטור וכדומה.
- 38.2. ביצוע מבחני חדירה תקופתיים הכוללים: מבחן המדמה ניסיון תקיפה מרשתות חיצוניות (כגון רשת האינטרנט, חיבור לספקים או שותפים עסקיים), בדיקות הנדסה חברתית, התחזות ופשינג, ותקיפה מתוך הרשת. ה"פורצים" יפעלו הן כמשתמש קיים והן כפורץ ללא חשבון קיים.
- 38.3. ביצוע סקרים שייתחסו לחשיפות אבטחת מידע במערכות הלשכה. הסקרים יתנו ביטוי לחשיפות הנובעות מחיבור מערכות הלשכה לרשתות חיצוניות ולחשיפות הנובעות מניסיונות תקיפה ברשת הפנימית של הלשכה.
39. תדירות ביצוע הסקרים תיקבע בהתאם למידת החשיפה של המערכת לאיומים, רגישות המידע המנוהל במערכת ושינויים שבוצעו במערכת או בסביבתה.
40. תדירות ביצוע הסקרים למערכות מידע שיש אליהן גישה מרשת ציבורית לא תפחת מאחת ל-12 חודשים. תדירות ביצוע הסקרים עבור מערכות מידע שאין אליהן גישה מרשת ציבורית, תיקבע בהתאם לרגישות המערכת ולא תפחת מאחת ל-18 חודש.
41. על אף האמור לעיל, יש לבצע סקרים טרם הטמעת שינוי משמעותי במערכת מידע, או בסביבתה הטכנולוגית, או טרם יישום של שירות חדש.
42. הסקרים יבוצעו על ידי גורם מקצועי, עצמאי, ובלתי תלוי שאינו מעורב בפיתוח והטמעת מערכות בלשכה או בבעל עניין בה ושהינו בעל נסיון של 3 שנים לפחות בביצוע פעילות דומה (להלן- גורם מבקר).
43. לאחר תיקון הליקויים יתבצעו בדיקות חוזרות ע"י הגורם המבקר על מנת לוודא שאכן בוצעו התיקונים הנדרשים.
44. הלשכה תגדיר תכנית לביצוע הסקרים לגבי ספקי מיקור חוץ שהם בעלי גישה למערכות הלשכה, או מאחסנים או מעבדים נתונים של הלשכה. רמת הכיסוי של הסקרים תותאם לרגישות המידע ולרמת הסיכון, ותכלול בדיקות שמטרתן לוודא את עמידת הספק בדרישות הגנה על המידע ולזהות חשיפות לסיכונים אלו. הסקרים יבוצעו בתדירות המותאמת לרמת הסיכון ולקצב עדכון התהליכים ומערכות הספק, ולכל הפחות אחת ל-24 חודשים. יתאפשר שימוש בסקרים שיוזם ספק מיקור החוץ ובתנאי שהוא עומד בדרישות חוזר זה לביצוע סקרים ושהסקרים בוצעו על ידי גורם בלתי תלוי.

#### איסוף מודיעין

- 44א. הלשכה תעקוב אחר איומי סייבר משמעותיים בישראל ובעולם ותבסס תמונת מצב עדכנית אודות איומי אבטחת מידע וסייבר, מידת חשיפתה מול האיומים, מצב הגנת המידע וזיהוי

חולשות (להלן – **תמונת המצב אודות איומי אבטחת מידע וסייבר**). תמונת המצב אודות איומי אבטחת מידע וסייבר תשמש כבסיס לקבלת החלטות מושכלות, תיעדוף דרכי פעולה, וקיום הגנה אפקטיבית בזמן אמת, וכן תשמש את הלשכה להפקת לקחים, יישום מסקנות רלוונטיות ונקיטת פעולות לצמצום החשיפות לאיומים.

444. הלשכה תאסוף ותנתח מידע רלוונטי ממקורות פנימיים וחיצוניים (לרבות פרסומים שונים של מערך הסייבר הלאומי והרשות להגנת הפרטיות). בין היתר, תתעדכן באופן שוטף במזהים (מזהים - IOC – INDICATORS OF COMPROMISE - כוללים כתובות IP) מהן מתרחשות תקיפות, כתובות מייל זדוניות ועוד, המופצים על ידי מערך הסייבר הלאומי, יצרני מערכות מידע והגנה, ומקורות חיצוניים נוספים. בהתאם לאמור ולהערכת סיכונים, הלשכה תטיב את מערכות ההגנה והניטור.

### בקרה וניטור

45. הלשכה תיישם נתיב בקרה הולם לפעולות המתבצעות במערכות המנהלות מידע רגיש על לקוחות וכן במערכות שרמת החשיפה שלהן לביצוע פעילות בלתי מורשה הינה גבוהה (בהתאם להערכת הסיכונים של הלשכה) כדי לאפשר התחקות אחר פירוט הרישום לצורך ביקורת, זיהוי פעילות של גורם בלתי מורשה, תחקור לאחר מעשה ומניעת התכחשות.

46. נתיב הבקרה יוגן משינוי בלתי מורשה, יתבסס על רישום ממוכן ויכלול את המידע הבא:

46.1. פעולות לרבות ניסיונות חיבור למערכות, שאילתות, עדכוני נתונים, הדפסת דוחות ושליחת מידע המבוצעים במערכות המידע כולל ניסיונות לביצוע פעולות כאמור.

46.2. מידע על מועדי הגישה למערכת, תיעוד המקור לביצוע הפעולות והגורם שביצע או ניסה לבצע, רכיב המערכת אליו בוצעה הגישה, סוג הגישה, היקפה ואם הגישה אושרה או נדחתה.

46.3. במערכות שהמידע המנוהל בהן עשוי להשפיע באופן מהותי על עסקי הלשכה ויציבותה ישמר ערך טרום ביצוע הפעולה ולאחריה.

47. פרק הזמן לשמירת נתיב בקרה יתאים למטרות הנתיב ובכל מקרה לא יפחת מ-24 חודשים.

48. הלשכה תקיים מערך לניטור מערכות מידע (להלן – מערך ה-SIEM), באופן עצמאי או באמצעות קבלת שירות, הכולל קבלת דיווחים בזמן אמת ממערכות המידע השונות אודות חשש לאירועים חריגים הנוגעים לאיומים על המידע בגין פעולות שמקורן מחוץ ללשכה או בתוכה, לרבות ניסיונות לביצוע שינויים במידע, תוך מתן דגש למערכות תשתית ומערכות אפליקטיביות.

48. הלשכה תגדיר מתודולוגיה לסיווג ההתראות המתקבלות ממערך ה-SIEM בהתאם לתהליך ניהול סיכונים מקובל על פי רמות חומרה שונות, וכן תקבע את אופן הטיפול בהתאם לכל רמת חומרה, לרבות פעולות לטיפול, לוחות זמנים ובעלי תפקידים רלוונטיים.

48. הלשכה תטמיע כללים ייעודיים והתראות במערך ה-SIEM, לזיהוי אנומליה או פעילות חריגה עבור מכשירים ניידים.

49. הלשכה תקיים נוהל בדיקה שגרתית של נתוני נתיב הבקרה ודיווחי הניטור, ותערוך דוח של הבעיות שהתגלו וצעדים שננקטו בעקבותיהן.
50. זיהוי והתרעה של פעולות חריגות שמקורן מחוץ ללשכה יכול להתבצע על ידי ספק מיקור החוץ בתנאי שהוא עומד בדרישות הלשכה לביצוע ניטור ומתריע מוקדם ככל האפשר על אירועים חריגים.
- 50א. הלשכה תערוך תהליך טיוב של הכללים שהוגדרו במערכות הבקרה והניטור, עם כל שינוי מהותי במערכות המידע ובשירותים הניתנים על ידי הלשכה, ולכל הפחות אחת לשנה. במסגרת זו, הלשכה תבחן, בין היתר, את התאמת הכללים לשינויים טכנולוגיים, רגולטוריים ועסקיים, לרבות היקפי פעילות משתנים.

### תהליכי פיתוח, תחזוקה וניהול שינויים

51. תהליכי פיתוח בלשכה יתבצעו באופן מאובטח (SSDLC), הן ביחס לפיתוחים חדשים והן ביחס לשינויים מהותיים במערכות המידע, ויכללו, לכל הפחות, את השלבים הבאים:
- 51.1 ייזום ואפיון מערכת, הכולל: (1) הערכת סיכונים חשיפת מידע רלוונטיים, הן ביחס לפיתוח והן ביחס למוצר עצמו; (2) הגדרת דרישות הגנה מתאימות בעת ייזום ואפיון מערכת; (3) קבלת אישורים מהממונה על אבטחת המידע ומגורמים מקצועיים רלוונטיים על אפיון המערכת.
- 51.1א עיצוב מערכת, הכולל: (1) אפיון דרישות למנגנוני הגנה תוך פירוט השימוש המיועד לכל פונקציה ורכיב במערכת; (2) צמצום משטח התקיפה על ידי זיהוי נקודות תורפה והפחתת היכולת לניצול חולשות פוטנציאליות, כגון: סגירת שירותים שאינם נחוצים ויישום הגנה בשכבות.
- 51.2 פיתוח מערכת, הכולל: מימוש והטמעת דרישות האבטחה המופיעות באפיון המערכת. הגנת המידע תוטמע בכל רכיבי המערכת, לרבות: תשתיות, אפליקציה (ככל שרלוונטי), וברמת הלוגיקה העסקית המיושמת במערכת.
- 51.3 בדיקת מערכת, הכוללת: (1) ביצוע הערכת סיכונים נוספת בהלימה לסיווג המידע ורגישותו, לפונקציונלית הקוד, לחלקים שיידרשו לבדיקות תוכנה, לאופן הבדיקות והיקפן; (2) ביצוע מבחני חדירה לרבות סקר אבטחת מידע, טרם הטמעת המערכת, על ידי גורם בלתי תלוי שאינו מעורב בפיתוח והטמעת המערכות; (3) ביצוע בדיקות וניתוח קוד דינמי (Dynamic Analysis) בזמן הרצה בכלים אוטומטיים ייעודיים, בנוסף לבדיקה ידנית. הבדיקות תבוצענה על ידי גורם בעל הכשרה וניסיון או באמצעות כלי טכנולוגי מתאים; (4) הגדרת פונקציות וממשקי API מותרים לתקשורת עם המערכת, ככל שרלוונטי.
- 51.4 קליטת מערכת, הכוללת: (1) הכנת תכנית חזרה לאחור תוך שמירת גרסא קודמת לייחוס; (2) קבלה והתקנה מאובטחת ומאושרת של המערכת על ידי גורמים מוסמכים לכך, תוך וידוא יישום דרישות הגנת המידע.

52. תחזוקה או ניהול שינויים במערכת יבוצעו לפי השלבים הבאים: (1) ביצוע הערכת סיכונים אבטחת מידע והגנת הפרטיות ווידוא כי סיכונים שעלולים להיווצר בעת ביצוע פעולות תחזוקה ושינויים במערכות מידע ובתהליכים, לרבות במערכות מקוונות או בתהליכי הזדהות של לקוחות לשירותים אלקטרוניים, יטופלו באופן מספק, טרם ביצוע השינוי; (2) סקירת שלבי הפיתוח המאובטח, כאמור לעיל, הרלוונטים לפעילות התחזוקה או ניהול השינויים, ואישור כל שינוי שנדרש לפני הפצה.

53. הממונה על אבטחת מידע יקבל דיווח טרם ביצוע פעולות פיתוח, תחזוקה וניהול שינויים במערכות המידע, ויהיה מעורב בתהליך הפיתוח המאובטח מראשיתו ועד סיומו, בהתאם לאופי השינוי, לרגישות הנתונים ולהשפעה אפשרית של השינוי על סיכונים וחשיפות המערכת.

54. בוטל.

#### אבטחת רשת וגישה מרחוק

55. הלשכה תשתמש באמצעי הגנה המתאימים לסיכונים גישה מרחוק לרשת הלשכה, כגון אמצעי סינון תקשורת ותוכן, אמצעי ניטור ותהליכי בקרה.

56. האמצעים יותאמו לסיכונים ייחודיים לשירותי רשת שונים, כגון דואר אלקטרוני, מתחמי כתובות - DNS, שירותי העברת קבצים, שירותי Web ועוד.

57. הלשכה תישם מידור בין החלקים השונים ברשת באמצעות חלוקה לוגית או פיסית שלה והגבלת אפשרות הקישור בין הרשתות השונות. רמת המידור תיקבע בהתאם לרגישות הנתונים המנוהלים במערכות, ולפחות יתבצע מידור בין המתחמים הבאים: רשת משתמשים, שרתי ייצור נתוני אשראי פרטניים, שרתי ייצור אחרים, רשת מנהלנים, רשת חיץ לאינטרנט.

58. הלשכה תיישם מנגנונים למניעת חיבור של אמצעים בלתי-מורשים לרשת הלשכה.

59. רשת הגיבוי תיושם כרשת ייעודית, נפרדת מרשתות אחרות. גישה לרשת הגיבוי תבוצע, לכל הפחות, באותם אמצעי זיהוי המשמשים לגישה לרשת הלשכה.

60. תישמר הפרדה בין מערכות המידע למתן שירות נתוני אשראי לבין מערכות המידע למתן שירות מידע על עוסקים. לצורך כך תקיים הלשכה לפחות את הדרישות הבאות:

60.1 הפרדה לוגית, הכוללת חסימת גישת יישום אחד למסד הנתונים האחר.

60.2 הגנות לוגיות נוספות, כגון שימוש בשמות מסדי נתונים וטבלאות שונות.

60.3 הפרדה לוגית בין האפליקציות, הכוללת מסכי הזדהות שונים ומובחנים זה מזה של עובדי הלשכה.

61. הלשכה תטמיע אמצעי אבטחה כגון ניטור מוגבר על גבי תשתיות תקשורת.

א.61 לפחות אחת לרבעון, תבוצע סריקת חולשות אבטחה במערכות המידע ובתשתיות, תוך הקפדה על עדכניות הכלים האוטומטיים באמצעות מבוצעת הסריקה וטיפול נאות בממצאים בהתאם לרמת הסיכון. סריקה כאמור תוכל להתבצע באמצעות ספק מיקור חוץ.

62. בוטל.

### קישוריות לרשת האינטרנט

63. אפשרות גישה מן הרשת הפנימית כלפי חוץ, תותר רק אל שרתים הנמצאים באזורי החץ. לא תתאפשר גישה ישירה מתחנות ומשרתי הרשת הפנימית לרשת חיצונית כלשהי.
64. קישור מערכות הלשכה לרשת האינטרנט יבוצע תוך יישום אמצעי הפרדה, שמטרתם למנוע הפעלה של קוד עיון, הכנסה בלתי מבוקרת של קבצים לרשת הלשכה או יצירה של ערוצים חשאיים אל מחוץ לארגון.
65. גישת משתמשים לרשת האינטרנט הציבורית תבוצע באמצעות מערכת גלישה וירטואלית.
66. קישוריות רשת הלשכה לאינטרנט תאובטח לפחות ע"י אנטי וירוס, מסנני תוכן, מערכת לאיתור ניסיונות חדירה (IDS) ו firewall.
67. הלשכה תבצע הפרדה מוחלטת של רשתות אלחוטיות מרשת הייצור שלה. לחילופין וככל שלא מדובר ברשת אלחוטית לשירות אורחיה, הלשכה תיישם מנגנונים מספקים לאבטחת רשתות אלחוטיות, לרבות הצפנה, הזדהות חזקה, מניעת התקפות על הרשת ומניעה של התחברות גורמים או ציודים בלתי מורשים לרשת האלחוטית.

### מניעת דלף מידע ואובדן מידע

- 66א. הלשכה תגדיר כללים בעניין מניעת דלף מידע ואובדן מידע, ובהתאם לכך תטמיע כלים טכנולוגיים, תהליכים ובקורות רלוונטיים, ותנקוט בפעולות להעלאת רמת מודעות העובדים; לעניין זה, "דלף מידע" (Data Leakage) - חשיפת מידע לגורמים שאינם מורשים מחוץ לארגון; "אובדן מידע" (Data Loss) - פגיעה בשלמות המידע (Data Integrity), לרבות במצב מנוחה (Data At Rest), בעת שימוש (Data In Use) ובתנועה (Data In Transit).
- 66ב. הלשכה תקבע את אופן העברת או הוצאת נתונים אל מחוץ לחצרות הלשכה, בהתאם לרמת רגישותם, וכן תגדיר ותיישם תהליכי הגנה הכרחיים להעברת או להוצאת נתונים כאמור, כגון: הצפנת תווך התקשורת והנתונים מקצה לקצה, וידוא הגעת נתונים ליעדם, הגבלת גישה לנתונים על בסיס "הצורך לדעת", בהתאם לרמת רגישותם.
- 66ג. הלשכה תזהה את הסיכונים הרלוונטיים לדלף מידע ולאובדן מידע.
- 66ד. הלשכה תוודא יישום בקורות מתאימות למניעת דלף מידע ואובדן מידע, לדוגמה הטמעת התראות או חסימות על ניסיונות להעברת או הוצאת נתונים על ידי גורמים שאינם מורשים, או בניגוד למדיניות ולנהלים שנקבעו על ידי הלשכה.
- 66ה. הלשכה תבצע טיוב של הבקורות באופן שוטף, בהתאם לסוגי המידע ולערוצי התקשורת הרלוונטיים ולשינויים מהותיים בסביבת הפעילות ובחשיפה לסיכונים, תוך בחינת הכללים שהוגדרו ומהימנות הכלים הטכנולוגיים שהוטמעו.
- 66ו. הלשכה תבחן את הכללים בעניין מניעת דלף מידע ואובדן מידע בתדירות של אחת לשנה לכל הפחות, וכן בעת שינויים מהותיים בסביבת הפעילות או בחשיפה לסיכונים, ותעדכןם במידת הצורך.

**קבלה והצפנת נתונים**

68. הלשכה תפנה בבקשות לקבלת נתוני אשראי ממערכת נתוני אשראי לצורך מתן שירותים לפי חוק נתוני אשראי ותקבל נתוני אשראי על הלקוח בתבניות שנקבעו על ידי הממונה במסמך בנושא "אפיון מפורט של השאילתות ונתוני האשראי שיקבלו לשכות האשראי".
69. בוטל.
70. בוטל.
71. בוטל.
72. הלשכה תצפין תעבורה בתוך (Data In-Transit) בכפוף להערכת סיכונים, ולכל הפחות בתקשורת מחוץ לחצרות הלשכה, ובכלל זאת במקרים הבאים:
- 72.1. תקשורת באמצעות האינטרנט;
- 72.2. גישה מרחוק למחשבי הלשכה;
- 72.3. בוטל;
- 72.4. תקשורת ללקוחות קבועים של הלשכה;
- 72.5. מקרים נוספים כפי שיבחנו ויוגדרו ע"י הלשכה כבעלי סיכון גבוה.
- א72. הלשכה תצפין במנוחה (Data At-Rest) נתוני אשראי ומידע אחר הנכלל בסעיפים 1(3)(ז) ו-1(3)(ח) בתוספת הראשונה לתקנות הגנת הפרטיות, הנאסף על ידה במסגרת מתן שירותים ללקוח, לרבות בבסיסי הנתונים ובקלטות גיבוי. הצפנה כאמור בבסיס הנתונים תבוצע עם כניסת המידע לבסיס הנתונים.
73. בוטל.
74. ההצפנה תיושם באמצעות טכניקות הצפנה מוכרות שהוכחו כיעילות, ותתוקף האפקטיביות שלהן באופן תקופתי.
75. הלשכה תגדיר נהלים מתאימים ליצירה, עדכון, חידוש, התקנה וביטול של מפתחות הצפנה ככל שרלוונטי לפעילותה.

**אבטחת מערכות ועדכון**

76. הלשכה תשמור רשימה עדכנית (Inventory) של תשתיות ומערכות מידע לצורך הגנה על המידע. הלשכה תגדיר תהליכים שוטפים לשמירת עדכניות הרשימה.
77. הלשכה תגדיר ותיישם עדכוני תוכנה ועדכוני אבטחת מידע שוטפים ומבוקרים למערכות המידע ולתשתיות באופן תקופתי, תוך התייחסות למקוריות קבצי העדכון, בדיקת עדכונים בטרם יישומם, ושמירה על יציבות מערכות בתהליך העדכון, והגדרת תהליכים לוידוא עדכניות אמצעי האבטחה (כגון: קבלת התרעות על כשל בעדכון קבצי חתימות).
78. הלשכה תבצע עדכון תוכנה מיידי בעת זיהוי חולשות קריטיות וזאת לאחר שנבדק ונמצא כי העדכון אינו צפוי לגרום לכשל במערכתיה.
- א78. הלשכה תגדיר ותיישם מדיניות לביצוע עדכוני אבטחת מידע ולזיהוי, דירוג ותיקון פרוצדורות אבטחה. מדיניות זו תכלול, בין היתר, התייחסות לנושאים הבאים:



- 78א.1. תהליך לאיתור הודעות רלוונטיות ממקור מהימן ;
- 78א.2. תהליך שוטף של בחינת קוד המקור הנכתב בלשכה ואיתור חולשות אבטחה ;
- 78א.3. דירוג חולשות האבטחה שאותרו לפי סדר עדיפות ולוחות הזמנים לתיקון, על סמך ציון מקובל לפגיעות (CVSS - Common Scoring System) והרלוונטיות של הפגיעות ללשכה ;
- 78א.4. בחינת אופן עדכון אבטחת המידע (ידני/אוטומטי/הפצה מדורגת וכד'); ;
- 78א.5. בחינת העדכונים הנדרשים באמצעות רשת בדיקה יעודית או מכונות לא קריטיות וכן בחינת הצורך בהטמעת בקורות מפצות עד לסיום הטמעת העדכון ;
- 78א.6. ביצוע עדכון אבטחת המידע ומעקב אחר הטמעתו כנדרש ;
- 78א.7. גיבוש תכנית גיבוי המאפשרת שחזור בטוח וחזרה למצב לפני העדכון במקרה של השפעות בלתי צפויות כתוצאה מעדכון .
- 78ב. הלשכה תוודא כי התקני קצה וכן תוכנות חדשות יהיו מותקנים במלואם, לרבות עדכוני אבטחה אחרונים, לפני חיבורם לרשת הארגונית.
- 78ג. ככלל, לא יעשה שימוש במערכות מידע שאינן נתמכות על ידי היצרן. במקרים חריגים, על הלשכה לבצע בחינה של הסיכונים ולקבל את אישור ההנהלה לשימוש במערכות אלו תוך מתן מענה אבטחתי הולם.
- 78ד. הלשכה נדרשת לזהות סיכונים הנובעים מחוסר עדכניות או היעדר תמיכה במערכות המידע ותפעל לצמצום הסיכון לרמת סיכון שיורי מקובלת.
79. בוטל.
80. בוטל.

#### אבטחת מערכות קצה

81. הלשכה תיישם אמצעי הגנה על מערכות קצה, תוך התחשבות בסיכונים הפעלת קוד עויין וסיכונים חדירה למערכות, תוך ניצול התקנים המחוברים למערכות קצה.
82. הלשכה תיישם מנגנונים טכנולוגיים אשר יוודאו כי רק אפליקציות שאושרו להתקנה ע"י גורמי אבטחת המידע יוכלו להיות מותקנות על גבי מערכות קצה.
83. הלשכה תשתמש במערכות בקרה, שמטרתן צמצום סיכון של דלף מידע רגיש ממערכות קצה או הגבלת היכולת לשמור מידע רגיש על מערכות קצה.
84. בוטל.

#### מניעת קוד עויין

85. הלשכה תטמיע אמצעי אבטחה למניעת חדירה והתפשטות קוד עויין במערכותיה, שיכללו מספר שכבות אבטחה כגון: סינון תקשורת וקבצים נכנסים, הגנה בזמן אמת על שרתים או תחנות קצה, ומערכות ניטור ומניעה ייעודיות.

86. הלשכה תעדכן בתדירות גבוהה את אמצעי האבטחה האמורים לעיל, ותגדיר תהליכים לוידוא עדכניות אמצעי האבטחה כאמור (כגון: קבלת התרעות על כשל בעדכון קבצי חתימות).
87. ככלל, הלשכה תחסום אפשרות לחיבור התקן זיכרון חיצוני (לרבות USB, DISC ON KEY וכיו"ב) למחשבי הארגון. במקרים בהם יוחלט כי קיימת הצדקה עסקית לשימוש בהתקן זיכרון חיצוני, יש לקיים מנגנוני הגנה ובקרה אפקטיביים שימנעו דלף מידע או החדרת קוד עוין, בשים לב לסיכונים המיוחדים הקשורים לשימוש בהתקן זיכרון חיצוני באותם מחשבים ובכלל זאת:
- 87.1 ניהול "רשימה לבנה" מרכזית של אמצעים מורשים לחיבור;
- 87.2 שימוש בהתקן זיכרון חיצוני שנרכש על ידי הלשכה בלבד, והכולל טכנולוגיית הצפנת מדיה נתיקה;
- 87.3 שימוש בעמדת הלבנת קבצים טרם חיבור התקן זיכרון חיצוני למחשב הלשכה ולאחר כל שימוש בו;
- 87.4 ניטור והתראה על חיבור או ניסיון חיבור של התקן זיכרון חיצוני במחשבי הלשכה.

#### שימוש במכשירים ניידים

- 87א. שימוש במכשירים ניידים (לרבות מחשבים ניידים, טלפונים ניידים, טאבלטים וכיו"ב) יהיה כפוף להנחיות שלהלן:
- 87א.1 הלשכה תגבש מדיניות ארגונית ונהלים לשימוש במכשירים ניידים, אשר יתייחסו, בין היתר, להגדרות אבטחה, עדכניות המערכות, אופן הגישה ליישומים ארגוניים, מחיקת נתונים מרחוק, ותהליכים מובנים לטיפול באובדן מכשיר. על המדיניות הארגונית להיבחן אחת לשנה ובמקרים של שינויים מהותיים.
- 87א.2 במקרה שבו מתאפשרת גישה למידע רגיש כחלק מהשימוש במכשירים ניידים שאינם מוגדרים ברשת הארגונית של הלשכה, לרבות גישה למידע רגיש בתיבות דואר אלקטרוני, הלשכה תטמיע תהליך לניהול מכשירים ניידים. במסגרת תהליך זה, יוגדר כיצד תיושם המדיניות הארגונית, בין היתר באמצעות הקשחות ומנגנוני הגנה ובקרה על מכשירים ניידים שאינם מוגדרים ברשת הארגונית של הלשכה, כגון: מניעת דלף מידע, הצפנת תווך, הצפנת מידע רגיש לרבות מידע צרכני ועסקי במטרה למזער את הסיכון של חשיפת מידע רגיש, שימוש בסיסמא, נעילה אוטומטית לאחר פרק זמן, התקנת עדכוני תוכנה, הורדת אפליקציות רק מחנויות מורשות, בחינה תקופתית של הרשאות גישה שניתנו לאפליקציות הארגוניות.
- 87א.3 לא יתאפשר מתן שירות ללקוחות וטיפול בתלונות ופניות הציבור, באמצעות מכשיר נייד שאינו מוגדר ברשת הארגונית של הלשכה.
- 87א.4 על מכשיר נייד המוגדר ברשת הארגונית של הלשכה יחולו כל דרישות הוראה זו.

#### הפרדה בין סביבות ואבטחתן

88. סביבת היצור תופרד מסביבות אחרות, כגון פיתוח ובדיקות.

89. הסביבה בה ינוהלו נתוני אשראי של לקוחות פרטיים כחלק משרותי הלשכה, תופרד באופן מוחלט מסביבות התומכות בפעילות עסקית אחרת של הלשכה. גישה לנתוני האשראי של לקוחות פרטיים תתבצע תחת בקרה וסינון.
90. רשת המשתמשים תופרד מסביבות אחרות וכל גישה מהסביבה תסונן על ידי מערכת חומת אש (firewall).
91. הפרדת הסביבות תתייחס גם לתשתיות עזר תומכות סביבת התקשוב.
92. הרשאות משתמשים לסביבות ייצור תנוהלנה בנפרד מההרשאות לסביבות האחרות.
93. העברת נתונים מסביבת ייצור לסביבה אחרת תתבצע באישור הממונה על אבטחת המידע, או מי מטעמו.
94. העברת מערכות ונתונים מסביבות פיתוח ובדיקות לסביבת ייצור תיערך בצורה מבוקרת, בהתאם לנהלים, כדי למנוע פגיעה בנתונים בסביבת הייצור.

#### ניהול משתמשים

95. הלשכה תבצע זיהוי אישי חד ערכי של כל גורם בעל גישה למערכות המידע כתנאי מוקדם למתן גישה. במקרים חריגים של ספקים, עובדים, או גורמים אחרים, בהם לא ניתן לקיים האמור לעיל, תיישם הלשכה אמצעים חלופיים מתאימים, המוגבלים למועד ולמשימה ספציפיים.
96. יקבעו כללים וכלים לזיהוי ולמתן הרשאות לגורמים שונים לרכיבי טכנולוגיית המידע. כללים אלו יביאו בחשבון את רמות הסיכון הנגזרות ואת מסגרת האחריות, הסמכות והמגבלות של המשתמשים, תוך שמירה על עקרונות של הפרדת תפקידים וסמכויות, הצורך לדעת ומתן הרשאות מינימליות לביצוע פעולות הקשורות לעבודתם בלבד, על פי סיווג לקבוצות.
97. הלשכה תגדיר נהלים המתייחסים לתהליכים שונים במחזור חיים של ניהול חשבונות משתמש במערכות מידע של הלשכה, החל מיצירת חשבון משתמש ואופן אישורו, ועד לאופן נעילת החשבון (העברתו למצב Disable) או מחיקתו בתום הפעילות, תוך שמירת סימן מזהה.
- 97א. הלשכה תגדיר אופן נעילת חשבון משתמש במקרה של אי שימוש בחשבון במשך תקופה ממושכת, שהינה לכל היותר תקופה של 90 יום, וכן במקרה של מספר ניסיונות חיבור כושלים. כמו כן, תגדיר הלשכה את תהליך האישור של שחרור נעילה כאמור.
98. תינתן התייחסות מיוחדת ליצירת חשבונות משתמשים עבור ספקים חיצוניים, עובדי מיקור חוץ, ועובדים זמניים, לרבות הגדרת אופן אישור חשבונות אלה, הגבלת השימוש בהם והמעקב אחר ביטולם בתום תקופת העסקה או תום פרויקט.
99. חשבון משתמש ישויך לעובד מסוים, ותוגדר אחריותו של העובד על חשבון זה ועל הפעולות המבוצעות במערכות הלשכה באמצעות חשבון זה.
100. ככלל, יעשה שימוש בחשבונות משתמש אישיים. עם זאת, במקרים בהם יש צורך בקיום חשבונות משתמש שאינם אישיים, כגון כאלה המיועדים לשימוש על ידי תהליך ממוכן, יוגדרו תהליכים מיוחדים לשמירה על סודיות אמצעי הזדהות של החשבון, להגבלת השימוש בו ככל הניתן ויוגדר גורם האחראי על חשבון המשתמש.

- 100.א. הלשכה תתעד, תנטר ותבצע בקרה אחר משתמשים באופן שוטף ותחקור אנומליות או חריגות.
- 100.ב. בכל הנוגע לניהול חשבונות משתמשים בעלי הרשאות חזקות (לדוגמה - Privileged User Accounts, Domain Administrative Accounts, Service Accounts, Application Accounts, Accounts with admin permissions, Active Directory/Domain Service Accounts), הלשכה תפעל גם בהתאם להנחיות המפורטות להלן:
- 100.ב.1. תמפה את כלל חשבונות המשתמשים, לרבות משתמשים המנהלים יישומים שנרכשו על ידי הלשכה מגורם צד שלישי ותנהל את חשבונות המשתמשים באופן מרוכז, לדוגמה באמצעות מערכות המיישמות טכנולוגיית Privileged Access Management (PAM);
- 100.ב.2. תוודא כי ערוצי התקשורת (Sessions) יוקלטו וינוטרו;
- 100.ב.3. עבור משתמש שאינו זקוק להרשאות חזקות באופן קבוע, הפעילות בחשבון המשתמש תבוצע לאחר קבלת אישור מראש של הגורם המוסמך בנושא ותהיה מוגבלת בזמן.
101. הלשכה תגדיר תהליכי סקירה תקופתיים ומתועדים שמטרתם לוודא את הצורך בקיום חשבונות המשתמשים. תהליכי הסקירה לכלל החשבונות, יבוצעו לכל הפחות אחת לשנה, ועבור חשבונות משתמשים חזקים, ספקים חיצוניים, עובדי מיקור חוץ ועובדים זמניים יבוצעו בתדירות גבוהה יותר. תהליכי הסקירה יבוצעו בהתאם לסוג ההרשאה שניתנה ומידת מורכבותה.
102. בוטל.
- סיסמאות ואמצעי הזדהות**
103. הלשכה תעשה שימוש בתעודה אלקטרונית, לצורך התקשרות עם מערכות המאגר.
104. הלשכה תמסור לממונה, לפי בקשתו, מידע שהוא למיטב ידיעתה נכון ומלא, הדרוש לו לשם הנפקת התעודה האלקטרונית.
105. לשכה בעלת תעודה אלקטרונית תגיש בקשה לחידוש תוקף התעודה האלקטרונית עד חודש לפני פקיעת התעודה.
106. מבלי לגרוע מהאמור לעיל בנוגע לחובת השימוש בתעודה האלקטרונית כאמור, הלשכה תגדיר אופן הזדהות למערכות מידע, באופן המתאים לרמת רגישות המידע המנוהל במערכת ולסיכונים השונים בתהליך ההזדהות.
107. הלשכה תגדיר נהלים המתייחסים, בין היתר, לנושא כללים לניהול סיסמאות ואמצעי הזדהות, אשר יכללו, בין היתר, התייחסות לאורך הסיסמה, מידת מורכבותה ותדירות החלפתה וכן לשמירה על סודיות הסיסמה והחלפת סיסמה ראשונית על ידי המשתמש. במסגרת נהלים אלו יקבע כי סיסמאות עבור כל סוגי המשתמשים יוחלפו בתדירות של אחת ל-90 יום לפחות.

108. יש לאמת את זהות המשתמש כאשר נמסרת לו סיסמה ראשונית למערכת. המשתמש יחויב לשנותה בהתחברות הראשונה למערכת. תוקף הסיסמה הראשונית ייקבע למינימום אפשרי, בהתאם לאופי השימוש בחשבון ולא יעלה על 14 ימים.
109. סיסמאות או אמצעי הזדהות אחרים לא יישמרו באופן גלוי (Clear Text) או באופן הניתן לשחזור ברשומות, בזיכרון או במאגרי מידע.
110. מורכבות הסיסמה תיקבע בהתאם לתקנים מקובלים, הלשכה תקבע את חוזק אמצעי ההזדהות, כגון הצורך בסיסמה חד-פעמית או מורכבות הסיסמה בהתאם להערכת הסיכונים. הלשכה תגדיר אמצעי בקרה על מערך ההזדהות, כגון נעילת חשבון משתמש לאחר מספר ניסיונות גישה כושלים או אי שימוש ממושך בחשבון, החלפה תקופתית של סיסמה ובקרה על מורכבותה.
111. משתמשים בעלי הרשאות חזקות, מנהלני מערכות וגורמים בעלי הרשאת גישה לנתוני אשראי פרטניים יבצעו הזדהות באמצעות תהליך Multi-Factor Authentication (MFA).

#### ניהול הרשאות ובקרת גישה

112. הלשכה תגדיר תהליכים מתועדים למתן הרשאות גישה למערכות ושירותים, לרבות: אחריות גורמים עסקיים לאישור הרשאות למערכות עסקיות, התאמת הרשאות לצרכי תפקיד, רמת הסיכון מהרשאות, שינוי הרשאות בעת שינוי תפקיד וביטול הרשאות בעת סיום העסקה.
113. מתן הרשאות גישה יתבצע על בסיס הגדרות תפקיד. הרשאות הגישה לכל תפקיד תהיה במידה הנדרשת לביצוע התפקיד בלבד.
- 113א. בפרופילי הרשאות המשתמשים תיושם הפרדת סמכויות, ובכלל זאת לעובד פיתוח לא תהיה גישה לסביבת הייצור, למעט הרשאות צפייה. במקרים חריגים, ניתן לתת הרשאות גישה לגורמים ייעודיים לצורך טיפול בתקלות בסביבת הייצור, בהתקיים התנאים הבאים: (1) הפעילות תבוצע לאחר קבלת אישור פרטני ומתועד לפעילות זו מהגורם המוסמך בנושא, שיכלול את הסיבה למתן ההרשאה; (2) ההרשאות שניתנו תהיינה זמניות ויבוטלו עם סיום הפעילות; (3) ישמר תיעוד לתהליך ומועד מתן ההרשאות הזמניות ולביטולן.
114. הלשכה תנהל רשימה מעודכנת של תפקידים, הרשאות גישה שניתנו להם, ושל העובדים הממלאים תפקידים אלו. הלשכה תנקוט באמצעים כדי לוודא כי הגישה לרשימה נעשית בידי עובד המורשה לכך בלבד.
115. לצורך גישה למערכות מידע שהוערכו כבעלות סיכון גבוה, ובכל מקרה של גישה מרחוק למערך טכנולוגיית המידע של הלשכה על ידי עובדים, ספקים ונותני שירותים, תשתמש הלשכה בטכנולוגיה המשלבת זיהוי ואימות המשתמש תוך שימוש בתהליך Multi-Factor Authentication (MFA), סודיות ושלמות הנתונים ומניעת הכחשה.
116. לא תותר העתקת נתוני אשראי ממחשב של הלשכה להתקן זיכרון חיצוני.
117. גישה מרחוק אסורה, למעט אם הוסדר מנגנון שיופעל לפי הערכת הסיכונים לנושאים הבאים:

- 117.1 קבלת אישור גישה מרחוק לכל אירוע, מתן אישור בעת ביצוע הגישה במחשב אליו ניגשים ;
- 117.2 הפעלת מנגנון ניתוק התקשורת, גישה מרחוק, לאחר פרק זמן שיקבע ;
- 117.3 יופעל רישום, LOG, של הפעילות הנעשית באירוע "גישה מרחוק" ;
- 117.4 ייושמו כלים המאפשרים זיהוי חד-ערכי של משתמשים אשר ביצעו שינויים במידע או בתוכנה או אשר ניגשו למידע רגיש, תוך פירוט הפעילות שבוצעה וזמן הביצוע, לפי הגדרות מנהל הגנת המידע ;
- 117.5 כלי לזיהוי ולרישום גישה לרשת מגורמים מרוחקים, ניסיונות חדירה, ניסיונות לדלף מידע רגיש החוצה וגישה לקבצים רגישים. כלי זה יעקוב אחר הפעילות ברמת הרשת ;
- 117.6 תיעוד ברמת האפליקציה של גישה למידע רגיש ע"י משתמש. התיעוד יבדיל בין סוגי הגישה לנתונים : יצירה, קריאה/צפייה, כתיבה ;
- 117.7 תיעוד ברמת האפליקציה של ניסיונות לעקוף את מנגנוני ההזדהות ;
- 117.8 כלים לאכיפה של הקשחת השרתים ותיעוד ניסיונות לחריגה ממדיניות ההקשחה ;
- 117.9 כלים להגנת מסדי נתונים מניסיונות חדירה, גניבת נתונים, שיבוש, הזרקת קוד, מחיקה והשתלה של נתונים שלא ע"י האפליקציות הייעודיות ;
- 117.10 הפעלת מנגנון הקלטת תעבורה מלאה (Full Packet Capture) או כל מנגנון אחר שיתעד את הפעולות שבוצעו בעת התחברות מרחוק.

118. בוטל.

119. בוטל.

### יישום בקרות

120. הלשכה תגדיר בקרות מתאימות להתמודדות עם סיכוני הגנת המידע בהתאם להערכת הסיכון. הבקרות יתייחסו לכל הפחות, להגנה על המידע באזורים ותהליכים אלו :
- 120.1 בציוד קצה.
- 120.2 בתהליך העברת המידע בין אתרים או בין ארגונים.
- 120.3 בשרתים, מסדי נתונים ובגיבויים.
- 120.4 בתהליכי הזדהות והרשאות.

### תכנית היערכות לניהול אירועי אבטחת מידע

121. הלשכה תגדיר תכנית היערכות לניהול אירועי אבטחת מידע (להלן – **תכנית היערכות**), בהתאם להערכת סיכונים ולניתוח תרחישי איום (כגון: גישה לא מורשית לנכסי המידע בלשכה, דלף מידע ואובדן מידע, התחזות, נוזקות, הונאה, מניעת שירות וכדומה) אשר תתייחס לשלבי האירוע הבאים :
- 121.1 גילוי - גילוי וזיהוי השלב בו נמצא האירוע תוך פירוט שלבי פעולה (בידוד, חקירה, איסוף ראיות, הסקת מסקנות וכדומה).

- 121.2 הערכת מצב - בירור וניתוח האירוע ובחינת דרכי פעולה להתמודדות, לרבות הפסקת פעילות באופן זמני באירועים בחומרה גבוהה.
- 121.3 הכלה - השגת שליטה על האירוע .
- 121.4 בלימה - עצירת החמרה של האירוע.
- 121.5 התאוששות - הכרעת האירוע תוך מזעור הנזק שנגרם.
- 121.6 חזרה לשגרה - חזרה לפעילות מלאה של הלשכה לאחר תיקון כל נזק שנגרם.
122. הלשכה תעדכן את תכנית ההיערכות בכל עת שנעשה שינוי טכנולוגי או ארגוני משמעותי או חל אירוע אבטחה משמעותי ולפחות אחת לשנה.
123. בנוסף, תכנית ההיערכות תתן ביטוי לנושאים הבאים לפחות :
- 123.1 דרכי תגובה ופעולה, בהתייחס לתרחישי איום שונים, והגורמים האחראים על הפעלתן.
- 123.2 דרכי התקשרות והעברת מסרים עם גורמים פנימיים וחיצוניים, ובכללם לקוחות, בהתאם לתרחישים שונים.
- 123.3 מתכונת ותדירות הדיווח על האירועים, גורם מדווח, נמען הדיווח וזמן התגובה הסביר לדיווח.
124. תכנית ההיערכות תעודכן על בסיס שנתי, בהתאם להערכת סיכונים מעודכנת, ותכלול התייחסות גם לעובדים חדשים ולמיקור חוץ.
125. הלשכה תקבע מנגנון דיווח על אירועי אבטחת מידע שיהיה נגיש לעובדים.
126. הלשכה תקים צוות תגובה להתמודדות עם אירועי אבטחת מידע.
127. הלשכה תקים, לכל הפחות, אחת לשנה תרגול של כלל המערכים הרלוונטיים שמטרתו להכין אותו להפעלת התכניות שהוזכרו לעיל ולשיפורן בהתאם ללקחי התרגול. התרגול יכלול, בין היתר :
- 127.1 תרגול עיוני אסטרטגי בהשתתפות ההנהלה, שמטרתו להגביר מודעות לאיומי סייבר ולגבש החלטות ניהוליות ברמה האסטרטגית.
- 127.2 תרגול מעשי, שמטרתו לבחון את התמודדות כלל המערכים הרלוונטיים בלשכה עם אירוע אבטחת מידע משמעותי.
128. אחת לרבעון ידווח לדירקטוריון ולהנהלה אודות כלל ניסיונות התקיפה ואירועי אבטחת המידע שהתרחשו (לרבות כאלה שלא הובילו לפגיעה חמורה), ההחלטות והפעולות שבוצעו.

### מיקור חוץ (Outsourcing)

129. הלשכה תיישם את ההוראות הבאות הנוגעות להתקשרות והגנה על המידע בעת השימוש במיקור חוץ :
- 129.1 התקשרות לצורך מיקור חוץ תיעשה בהסכם כתוב.
- 129.2 בכל התקשרות לקבלת שירותי מיקור חוץ יש לבחון את סיכוני אבטחת מידע הכרוכים בהתקשרות.

- 129.3 כל התקשרות עם ספק חיצוני לביצוע פעילות הקשורה בחשיפה לנתונים אודות אנשים פרטיים טעונה אישור הממונה. הספק יצטרך לעמוד בכל דרישות מסמך זה הרלוונטיות לפעילות הספק ולמידע הנוגע לפעילות, בין אם הפעילות נעשית באתר הלשכה ובין אם באתר אחר.
- 129.4 אין לבצע מיקור חוץ לשירותי דרוג אשראי והפקת דוח אשראי.
- 129.5 הלשכה תגדיר נוהל לדרישות הגנת מידע בהתייחס לסיכוני מיקור חוץ ולאבטחת שרשרת האספקה. נוהל זה ייושם בעת התקשרות עם גורם מיקור חוץ חדש.
- 129.6 בהסכם התקשרות לקבלת שירותי מיקור חוץ יש להתייחס, בין היתר, לנושאים הבאים:
- 129.6.1 הגדרת תחומי אחריות של כל אחד מהצדדים להסכם לרבות קבלני משנה.
- 129.6.2 הגדרת רמת שרות (SLA).
- 129.6.3 חובת סודיות, אבטחת מידע וגיבוי.
- 129.6.4 הסדרים להפסקת הסכם וליישוב מחלוקות.
- 129.6.5 יכולת הלשכה לבצע ביקורות על פעילות נותן השירות.
- 129.6.6 אפשרות שהלשכה תתפעל ותתחזק את פעילות מיקור החוץ במקרים בהם נותן השירות חדל ממתן השירות, כגון ע"י החזקת תוכנות מקור והרשאות אצל נאמן.
- 129.6.7 איסור על נותן השירות להעביר לצד שלישי מידע שקיבל במסגרת ההתקשרות, או להשתמש במידע שאליו נחשף אגב ביצוע ההתקשרות, לכל מטרה אחרת שלא קשורה לביצוע ההתקשרות.
- 129.6.8 בעת הצורך בהעברת נתונים, יבוצע תהליך של גישה מבוקרת לנתונים פרטניים ולא שכפול כלל בסיס הנתונים.
130. אספקה של שירותי תחזוקה מרחוק (מידע, תוכנה או ציוד תקשורת) על ידי גורמי מיקור חוץ, תבצע בתנאים הבאים:
- 130.1 נותן שירות מיקור חוץ יקבל אישור פוזיטיבי להתחברות, לפני תחילת עבודתו. הממונה על אבטחת המידע יקבע מי בעל הסמכות לאשר התחברות מסוג זה.
- 130.2 גישה מרחוק תתאפשר באמצעות משתמש ייעודי לכל נותן שירות מיקור חוץ ובתיאום מראש עם הלשכה לאופן ההתקשרות ותדירותה.
- 130.3 גישה מרחוק תתאפשר לזמן מוגבל על פי סוג הפעילות אותה יבצע נותן שירות מיקור החוץ.
- 130.4 הלשכה תיישם הזדהות באמצעות תהליך MFA לצורך כל גישה מרחוק של נותן שירות מיקור חוץ.
- 130.5 הלשכה תיישם הצפנה מקצה לקצה לכל אורך נתיב ההתקשרות מרחוק שהינה הצפנת תווך התקשורת/הנתונים מהתחנה/השרת.
- 130.6 הלשכה תנטר כל פעילות שבוצעה בגישה מרחוק.



130.7 חשיפת נותן שירות מיקור חוץ למידע אודות לקוחות תצומצם עד למינימום הכרחי, ובמידת האפשר תחסם במלואה.

130א. אין בהוראות לגבי מיקור חוץ הקבועות בהוראה זו בכדי לגרוע מאחריות הלשכה לכל פעולה הנעשית על ידי נותני השירות במיקור חוץ.

#### שירותי מחשוב ענן

131. הלשכה רשאית להעביר לסביבת ענן ציבורי רק מערכות שאינן מנהלות מידע רגיש.
132. שימוש בשירותי מחשוב ענן יהיה כפוף להנחיות לעניין מיקור חוץ.
133. בטרם הפעלת מערכות מבוססות ענן, על הלשכה לבצע הערכת סיכונים ייעודית ולדון בסיכונים אפשריים, משימוש בשירותים כאמור.
134. גישה לנתונים בענן תבוצע דרך כתובות הלשכה בלבד.
135. הלשכה תעשה שימוש בטכנולוגיות כגון הצפנה, מיסוך נתונים או טוקניזציה בעת שימוש במערכות בסביבת ענן.
136. הלשכה תכלול בהסכם ההתקשרות עם ספק מחשוב הענן אפשרות חד צדדית להפסקת השימוש בשירותי ספק מחשוב הענן תוך מחיקת המידע ממערכותיו והתחייבותו שלא ניתן לאחזר מידע זה במערכותיו.
137. הלשכה תיידע את הממונה 3 חודשים מראש לגבי כוונתה להעביר מערכות לסביבת ענן ציבורי ותקבל את אישורו לכך.
138. בוטל.

## פרק ד': הגנה פיסית

### אבטחה פיסית

139. הלשכה תיישם את ההוראות הבאות בנוגע לבקורות אבטחה פיסיות שיתייחסו למכלול הסיכונים הפיסיים והסביבתיים באזורים המאובטחים כאמור להלן:
- 139.1. הלשכה תחלק את האתר וסביבת העבודה לאזורים מאובטחים לפי רמת רגישות המידע אליו ניתן לגשת.
- 139.2. הלשכה תיישם מעגלים של בקורות ותיעוד גישה פיסית שרמתם תותאם לרמת רגישות המידע. מעגלים אלו יכללו בקורות מונעות (כגון דלתות נעולות, שערים אלקטרוניים, ומערכות למניעת שריפות) ובקורות מגלות (כגון מערכת מצלמות ומערכות אזעקה).
- 139.3. מערכות המידע יחוברו למערכות אל פסק, מקורות הזנה ושימוש בגנרטור בעת הצורך או פתרונות אחרים על מנת למנוע הפסקת פעולות המערכות במקרה של ניתוק חשמל.
- 139.4. הלשכה תאפשר גישה לאזורי העבודה בהתאם לצורך, ותמנע בהקדם האפשרי את הגישה לאזורים אלה כאשר אין עוד צורך בגישה זו, לרבות בעת שינוי תפקיד או סיום ההעסקה.
- 139.5. היה והלשכה תעניק שירותי קבלת קהל במשרדה, תתקיים הפרדה בין האזור בו ניתנים שירותים אלו, לבין אזורי העבודה השוטפים בלשכה. לא יתאפשר לגורם, שאינו מורשה, להסתובב במשרדי הלשכה ללא פיקוח.
- 139.6. אזורים המכילים מידע רגיש ימודרו בפני גישה של אנשים שאינם בעלי הרשאה למידע.
140. מידע רגיש יאובטח באמצעות שילוב מושכל של האמצעים הבאים:
- 140.1. אתר חוות שרתים, חדר מחשב מרכזי, ארונות תקשורת ימצאו במבנה קשיח ויזכו באמצעי הגנה פיסיים ההולמים לרמת הסיכון.
- 140.2. בקרת גישה באמצעות אזעקה המחוברת למוקד חיצוני ומופעלת כאשר האתר אינו מאויש.
- 140.3. מחוץ לשעות הפעילות יבוצעו סיורים יזומים לבדיקת תקינות המערכות, לשמירת נוהלי אבטחה ולפעילות מניעה.
- 140.4. ספקים חיצוניים ומבקרים באתרי הלשכה יבדקו, יזוהו ויירשמו בכניסתם וביציאתם.
- 140.5. באחריות האחראי לאבטחת מידע לקבוע נהלים להגנה ושמירה על מחשבים ואמצעי אחסון ניידים המכילים מידע רגיש.
- 140.6. באחריות האחראי לאבטחת מידע לקבוע נהלים לליווי מבקרים מזדמנים וספקים כולל מחויבותם לשמירת הסודיות.
- 140.7. הלשכה תעזר בחוות דעת של מומחה לאבטחת מידע פיסי.

**אבטחת ציוד וניירת**

141. אופן הוצאת ציוד המכיל מידע רגיש מאחד ממעגלי האזורים המאובטחים תיעשה בהתאם להערכת סיכונים.
142. הלשכה תבצע השמדה של ציוד רגיש (פיסי או דיגיטלי) שאין בו שימוש ותגדיר את אופן הטיפול והשמירה עד להשמדתם.
143. ציוד המועבר להשמדה או תחזוקה אל גורם מחוץ ללשכה לא יכיל מידע רגיש.
144. יקבע נוהל להשמדת מסמכים (נייר, תצלום, מדיה מגנטית) שיאושר ע"י הממונה על אבטחת המידע. כל המסמכים שתם השימוש בהם, יושמדו בתחומי הלשכה. מדיה מגנטית תפורמט ולאחר מכן תיגרס באופן מפורק.

**תחקור אירועי אבטחת פיסית**

145. בעת אירוע אבטחה פיסית נדרש:
- 145.1 לחקור ולתעד את האירוע.
- 145.2 לערב גורמי חקירה חיצוניים ככול שנדרש.
- 145.3 לערב את הממונה על אבטחת המידע וגורמים נוספים בלשכה, בהתאם לאופי האירוע.
- 145.4 להכין דוח אירוע ולהפיצו להנהלה.
- 145.5 לבצע הליך הפקת לקחים ולהפיץ את הידע לגורמים רלוונטיים.

## פרק ה': משאבי אנוש והדרכה

### גיוס עובדים

146. על הנהלת הלשכה, הקולטת עובדים חדשים לוודא יישום הליכי בקרה הנוגעים לעובדים החדשים הנקלטים. מטרת ההליכים לוודא כי העובדים מתאימים לקבלת גישה לסוג המידע הנדרש בשים לב לרגישות המידע, היקף הרשאות הגישה והתפקיד שמיועד לעובד.
147. עבור משרות שיוגדרו כרגישות על ידי הממונה על אבטחת המידע (כגון כאלה המאפשרות גישה למידע רגיש או שיש להן הרשאות העלולות לסכן את הלשכה), יבוצעו בדיקות לבחינת אמינות המועמדים.
148. הממונה על אבטחת המידע בשיתוף גורם משאבי אנוש ובתיאום עם גורמים רלוונטיים בלשכה יתוו ויגדירו את יישומם של:
- 148.1 תהליכים ואמצעים לוודא מהימנות עובדים, בהתאם לצורך.
  - 148.2 טיפול בחריגים.
  - 148.3 אופן ביצוע פיקוח והבקרה על עובדים.
149. חוזה הנחתם עם עובדים חדשים יכלול התייחסות לאחריות העובד בכל הנוגע להיבטי סיכונים אבטחת מידע והגנת הפרטיות, וילווה בהצהרת סודיות, והכל בהתאם למידת רגישות המידע לו הם יקבלו גישה.
150. חוזה של הלשכה עם חברות להשמת כוח אדם או עם חברות המספקות שירותי מיקור חוץ, יכלול אף הוא התייחסות לסעיפים לעיל.
151. הממונה על אבטחת המידע יקבע בתיאום עם הגורמים הרלוונטיים בלשכה את רמות סיווגי האבטחה הנדרשים מעובדי הלשכה לרבות במערכות החיוניות (קריטיות), תוך התייחסות לקריטריונים ספציפיים הנוגעים לרגישות המידע אליו יחשפו.
152. יתבצע תיעוד הכולל פירוט הליכי הגיוס.

### הוראות לעניין יישום נהלי אבטחת מידע

153. הלשכה תקבע כללים למנהלים ולעובדים בנוגע לאחריותם ליישום נהלי אבטחת מידע בתחומי סמכותם, לפעילות הולמת של המנהלים והעובדים בהיבטי האבטחה וכן לטיפול בנושאי אבטחת מידע חריגים בשיתוף עם אחראי אבטחת מידע.
154. האחריות לאבטחת המידע, בין אם הנה מוטלת על עובדי הלשכה ובין אם על מנהליו, מתייחסת לכל ההבטים הרלבנטיים, כולל בין היתר, אבטחה פיזית, אבטחת הרשומות והאבטחה הלוגית.
155. על מנת לוודא כי כל עובד יודע ומועד לחובותיו בנושא אבטחת המידע תפיק הלשכה חוברת ייעודית לנושא זה בה ייכללו כל חובות האבטחה המוטלות על העובד. החוברת תינתן לכל עובד חדש במסגרת הליך קליטתו ולעובד קיים אם טרם קיבל. אחריות לעדכון החוברת מוטלת על הממונה על אבטחת המידע או גורם אחר שיוסמך על ידו.
156. הלשכה תקבע נוהל דיווח מיידי לממונה על אבטחת המידע או גורם אחר המוסמך על ידו, על כל פעילות העלולה להשפיע על אבטחת המידע.

### ניוד או סיום העסקה

157. לעובדים (לרבות עובדים במיקור חוץ ועובדי קבלן) העוברים תפקיד או מסיימים את העסקתם ייחסמו הרשאות הגישה למידע שאינם צריכים עוד לביצוע תפקידם ובסיום העסקה לא יישארו נכסי מידע של הלשכה בידי העובד.
158. הלשכה תגדיר בקרות הגנה נוספות המתייחסות לתקופת הזמן שבין החלטה על מעבר תפקיד או סיום העסקה של עובד ובין ביטול הרשאות הגישה שלו, כגון מעקב מוגבר של הממונה על אבטחת המידע אחר בקשות של העובד להרשאות או פעולות חריגות שמבוצעות על ידו, והכל בכפוף להוראות החוק וכו'.
159. בעת מעבר של עובד לתפקיד חדש או שינוי הגדרת התפקיד תישם הלשכה הליכי בקרה שיבטיחו כי העובד מתאים לקבל גישה לסוג המידע עבורו נידרשת ההרשאה, ובשים לב לרגישות המידע, היקף הרשאות הגישה והתפקיד אליו מיועד העובד.
160. יש להסדיר באופן הולם את החובה של העובד על שמירת חסיון המידע לו היה חשוף גם לאחר סיום עבודתו בלשכה.

### עובדי חוץ ומבקרים

161. הממונה על אבטחת המידע או גורם אחר המוסמך על ידו, יתוו תהליכים לניהול אבטחת המידע בגין פעילות של עובדי חוץ ומבקרים (להלן- חיצוניים), לרבות:
- 161.1 קריטריונים להגדרת סיווג רגישות החיצוניים.
  - 161.2 דרישות אבטחה בכפוף לסיווג רגישות החיצוניים.
  - 161.3 שיטות וכלים לאכיפת הדרישות.
  - 161.4 תהליכים ואמצעים לפיקוח ובקרה ולטיפול בחריגים.
162. יבוצע זיהוי ורישום של עובדי חוץ, עובדי ספקים ומבקרים.

### הדרכה

163. הלשכה תגדיר תכנית להעלאת רמת מודעות של עובדים לסיכונים אבטחת מידע והגנת הפרטיות (להלן - תכנית להעלאת רמת המודעות).
164. התכנית להעלאת רמת המודעות תשולב במערך הדרכה של הלשכה ותכלול התייחסות לאוכלוסיות העובדים השונות, לרבות עובדי מיקור חוץ.
165. התכנית להעלאת רמת המודעות תגדיר הדרכות תקופתיות לעובדים לפי סוג התפקיד ובמהלך התפקיד ותתייחס גם להדרכה הנדרשת בעת קבלת עובדים או בעת מעבר לתפקיד חדש. ההדרכות תתייחסנה, בין היתר, לחוק הגנת הפרטיות התשמ"א – 1981 וכן למסמכי המדיניות והנהלים הרלבנטיים בלשכה, ותותאם לאיומים ולסיכונים רלוונטיים.
166. התכנית להעלאת רמת המודעות תסייע להטמעת נהלי אבטחת המידע והגנת הפרטיות בתהליכי העבודה של הלשכה.

167. תוגדר תכנית הדרכה בתחום האבטחה לרבות תכנית הדרכה ממוקדת לעובדים להם נגישות למערכות חיוניות. אחת לשנה יבוצעו פעולות לשימור והעלאת מחויבות ומודעות כללית לתחום אבטחת המידע לעובדים.
168. עובד חדש, או עובד ששונה לגביו הקפי ההרשאה, יתוודך בטרם כניסתו לתפקיד או ביצוע השינוי על ידי הממונה על אבטחת המידע או גורם אחר המוסמך על ידו, וכן בזמן מעבר מתפקיד לתפקיד, אם קיימת משמעות אבטחתית למעבר. ההדרכה תתייחס, בין היתר, לחובות העובד בגין חוק הגנת הפרטיות ותקנותיו ונוהלי הלשכה בנושאי אבטחת מידע. הממונה על אבטחת המידע או גורם אחר המוסמך על ידו ידאג להחתים את העובדים על מסמך המעיד שקראו והבינו את נהלי השמירה וסדרי האבטחה הפיסית ואבטחת סיכוני הגנת המידע.

## פרק ו': פעילות בערוצי תקשורת

### בקורות בתהליך הרישום לביצוע פעולות

169. הלשכה תוודא זהות לקוח (ארגוני או פרטי) בטרם השלמת רישומו לקבלת שירותים מקוונים. הרישום יכול להיות רישום תקופתי או חד פעמי, בהתאם לצורכי הלקוח.
170. הלשכה תגדיר את אופן הזדהות הלקוחות לערוצי שירות שונים. אופן ההזדהות יתאים לאופי ערוץ השירות, לרמת הרגישות של המידע והפעולות המבוצעות באמצעות הערוץ, ולסיכונים השונים לתהליך ההזדהות, כגון התחזות, האזנה לתוך התקשורת וכדומה. בערוצים מבוססי אינטרנט יעשה שימוש באמצעי הזדהות חזקים או אמצעי הזדהות שאינם קבועים, כגון סיסמאות חד פעמיות הנשלחות בהודעת SMS.
171. הלשכה תגדיר נהלים המתייחסים למסירת אמצעי הזדהות, כגון משלוח סיסמה ראשונית באמצעות דואר לכתובת לקוח, מסרון לנייד הלקוח או באמצעות ערוץ אחר המאפשר מסירת אמצעי ההזדהות ללקוח, וצמצום הסיכון לגניבת או העתקת אמצעי זה בדרך אל הלקוח.
172. הלשכה תוודא כי לעובדיה אין גישה לאמצעי הזדהות של לקוחות, העלולה לאפשר ניצול לרעה של חשבון לקוח, למעט עובדים מורשים.
173. הלשכה תבצע ניטור ייעודי לזיהוי התקפות עליה, כגון: ניסיונות התחזות, התקפות שונות על מנגנוני אימות זהות לקוח (אותנטיקציה), התקפות "הנדסה חברתית", התקפות על מנגנוני שחזור סיסמה וכדומה. כמו כן, הלשכה תיישם אמצעים למניעת התקפות על ערוצי תקשורת כגון, ניחוש שמות משתמשים (user harvesting) ניחוש סיסמאות (Brute Force), מניעת שירות באמצעות נעילת חשבונות וכדומה.
174. בעת שימוש באמצעי זיהוי קבועים הלשכה תגדיר נהלים המאפשרים ללקוח איפוס סיסמה.
175. רישום לקוח לפעילות בערוצים מקוונים, תחייב קבלת הסכמה מתועדת של הלקוח באמצעות טופס דיני או טופס אלקטרוני או באמצעות חשבון המקוון של הלקוח באתר האינטרנט של החברה.
176. ללקוח תינתן הזכות לחזור בו מהסכמתו כאמור.

### בקרה על הזדהות לקוחות

177. הלקוח יקבל בכל כניסה חדשה למערכות הלשכה פרטים על מועד התקשרות קודמת.
178. לקוח יוכל לעדכן פרטים אישיים, למעט פרטים המשמשים לצורך זיהוי.
179. תקנים בקרה שהגורם שעדכן את פרטי הלקוח הוא הלקוח עצמו.

### ניהול סיסמאות לקוח

180. הלשכה תגדיר נהלים לוודוא חוזק סיסמה, שמירה על סודיותה, החלפת סיסמה ראשונית על ידי המשתמש ותוקף הסיסמה הראשונית.
181. סיסמה ראשונית, לרבות כזו הניתנת ללקוח בעת שחרור סיסמה, תימסר ללקוח באמצעות ערוץ תקשורת מאושר ע"י הלקוח כשהיא חסויה אף מהמוסר.

182. הלשכה תיזום החלפת סיסמה ראשונית ללקוח מיד לאחר ההתקשרות הראשונה וכן עדכון ססמה אחת לתקופה.
183. הלשכה תנקוט באמצעים שונים להגנה על המכשירים המשמשים את הלקוח להתקשרות, מפני שימוש לא מורשה וחשיפת מידע אודותיו, כגון: מניעת שמירת הסיסמה בדפדפן, מניעת שמירת דפי אינטרנט בזיכרון מטמון וכדומה.
184. הלשכה תבטל את הסיסמה, שנמסרה ללקוח, במקרים הבאים:
- 184.1 הסיסמה הראשונית לא הופעלה תוך 7 ימים מהנפקתה.
  - 184.2 לבקשת הלקוח או אם קיים חשד שנעשה שימוש לא מורשה בסיסמה.
  - 184.3 לאחר מספר מסוים של נסיונות כניסה כושלים, אשר בכל מקרה לא יעלה על חמישה נסיונות כושלים רצופים.

#### מסירת מידע באמצעים דיגיטליים

185. קבלת בקשות לשרותי הלשכה ושליחת מסרים מהלשכה למבקשים יכולה להיעשות גם באמצעות אמצעים דיגיטליים בכפוף לקיום התנאים הבאים:
- 185.1 זיהוי מבקש המידע וקבלת הסכמתו לשליחת המסרים.
  - 185.2 ווידוא כי מבקש המידע זכאי לקבל את המידע.
  - 185.3 בקשת מבקש המידע תתועד.
186. מבקש המידע יכול לחזור בו מהסכמתו זו בכל עת, לפני מסירת הדוח.
187. הלשכה תשמור כל מידע תפעולי הנחוץ לצורך בקרה, ניהול ומעקב אחר קיום תנאי שליחת מידע באמצעים דיגיטליים.
188. הלשכה תשמור תעוד לפנייה ולמסירת המידע בכפוף להוראות החוק ותקנותיו.
189. הלשכה תקיים הליכי בקרה למניעת העברה שגויה של מסרים או מידע למי שאינו רשאי להעביר את המידע.
190. הלשכה תנטר ותבקר את ערוצי המידע הדיגיטליים על מנת למנוע דלף מידע או הוצאתו באמצעים לא מורשים.
191. הלשכה תספק ללקוחותיה הנחיות המסייעות לנקוט באמצעי זהירות נדרשים לשמירה על פרטיות מידע, ותנחה אותם כיצד לנהוג במקרה של חשד לאירוע אבטחת מידע.
192. כל הודעה הנשלחת באמצעים דיגיטליים תישא כותרת המשקפת את תוכנה. דוח ריכוז נתונים הנשלח ללקוח באמצעים דיגיטליים יוגן בסיסמה.



**פרק ז': תיעוד, מחיקה, אחזור וגיבוי המידע, והפסקת פעילות לשכה****תיעוד**

193. הלשכה תשמור ותתעד מידע שהתקבל, נוצר, עובד ונמסר לאחרים במסגרת השירותים שהיא מספקת כלשכה, לרבות:
- 193.1 פניות לקוחות ללשכה כולל קבצי מסמכים, קבצי קול, פרטי פניה מתחילתה ועד סגירתה ואופן הטיפול בפניה, למשך תקופה של 7 שנים לפחות.
- 193.2 פניות לקוחות בבקשות לדוחות אשראי או דירוגים יכללו בנוסף הוכחת זיהוי המבקש ובדיקה כי התקבלה הסכמת הלקוח, למשך תקופה של 7 שנים לפחות.
- 193.3 נתונים המועברים ללשכה מהמאגר אודות לקוח ישמרו בהתאם לחוק ותקנותיו.
- 193.4 נתונים המועברים ללשכה מהמאגר עבור נותן אשראי, לשם עריכת דוח אשראי או חיובי אשראי או מתן הודעה על שינוי בנתוני אשראי של לקוח (ניטור), ישמרו לתקופה המזערית הנדרשת ללשכה לשם מתן השירותים על ידה, שתיקבע בנהלי הלשכה.
- 193.5 תהליכי בקרה ופעולות שביצעה לצורך יישום הנחיות הוראה זו, וכן נתוני אירועי אבטחת מידע ותקלות שמעלות חשד לאירועי אבטחת מידע, למשך תקופה של 24 חודש לפחות.
194. הלשכה תתעד ל - 7 שנים לפחות מסמכים הקשורים לפעילותה והתנהלותה כדוגמת:
- 194.1 מדיניות ונהלים שקבעה לעמידה בתנאי החוק והתקנות מכוחו, תכנית היערכות לניהול אירועי אבטחת מידע ואופן הטיפול באירועי אבטחת מידע, הערכות סיכונים, דוחות ביקורת ותכניות עבודה וטיפול בליקויים שזוהו בדוחות הביקורת.
- 194.2 דוחות הנוגעים לתכנית ציות ובקרה על ציות.
- 194.3 מסמכים ומידע המהווים בסיס למודל הדרוג.
- 194.4 תכנית בקרה פנימית ודוחות בקרה פנימיים כולל כל המסמכים הנדרשים לשם ביצוע

**מחיקת מידע**

195. הלשכה תקבע נוהל עבודה למחיקת הנתונים המזוהים המתקבלים מהמאגר בהתאם להוראה זו ולכללי אבטחת מידע.
196. הממונה על אבטחת מידע יהיה אחראי לגיבוש ויישום נוהל עבודה למחיקת הנתונים המזוהים.
197. הלשכה תקבע נוהל עבודה למחיקת הנתונים הבלתי מזוהים המתקבלים מהמאגר, שיכלול בין היתר, הוראות לעניין הנושאים המפורטים להלן:
- 197.1 אחריות הממונה לאבטחת מידע לגיבוש ויישום הנוהל.
- 197.2 תדירות ועיתוי המחיקה.
- 197.3 זיהוי המערכות בהן נדרש לבצע מחיקה.
- 197.4 אמצעי המחיקה.

197.5 תהליכי בקרה שוטפים.

198. הלשכה תיישם נתיב בקרה הולם לפעולות המחיקה במערכותיה בהתאם לדרישות הקבועות בהוראה זו.

199. הביקורת הפנימית בלשכה אחראית לבקר, לפחות אחת לשנה, את אופן יישום נהלי המחיקה.

#### אחזור מידע

200. הלשכה תפעל לשימור יכולת איחזור כל נתון, מידע, מסמך ותוכנית מחשב המתועדים לפי דרישות מסמך זה ולפי הוראות החוק. איחזור משמעותו היכולת להציג, להפעיל או לחשב כפי שהיה במקור.

201. הלשכה תשמר גירסאות תוכנה, חומרה, מערכות הפעלה ועוד ככול שידרש כדי שיאפשרו אחזור חומר.

#### גיבוי ואחזור נתונים

202. הלשכה תקבע נהלים לגיבוי נתונים ואפליקציות באופן שוטף וכן לגיבוי אגב שינויים במערכות המידע שלה. נתונים ואפליקציות שגובו ישמרו באתר נפרד, באופן מדויק ועדכני בהתאם לנהלי הגיבוי של הלשכה.

203. הלשכה תקבע נהלי התאוששות וחזרה לשגרה בפרק זמן סביר בקרות אירוע כשל באתר הראשי, כדי להבטיח התאוששות מהירה.

#### סיום או הפסקת פעילות לשכה

204. החליטה הלשכה על פירוקה מרצון או על הפסקת פעילותה, או שבוטל רשיונה של הלשכה על ידי הממונה, תעביר הלשכה לידי הממונה בתוך שבעה ימי עסקים ממועד הפסקת הפעילות או ביטול הרשיון, מקור או העתק מדויק של כל החומר המתועד המצוי ברשות הלשכה; לחומר יצורפו סכימה ואינדקס שיאפשרו איתור מסמך, מידע, נתון וכדומה בחומר שהעבירה הלשכה לממונה.

\* \* \*