



## ניהול המידע והגנתו

### תוכן

3	פרק א': כללי
3	מבוא
3	תחולה
3	הגדרות ומינוחים
5	פרק ב': פיקוח וניהול
5	דירקטוריון
5	ההנהלה
6	ממונה על אבטחת מידע
7	ביקורת פנימית
7	דיווחים לממונה
8	פרק ג': הגנת המידע
8	מסגרת עבודה (Framework) לניהול הגנת מידע
8	סקר הערכת סיכוני אבטחת מידע ומבחני חדירה
9	בקרה וניטור
10	תהליכי תחזוקה ופיתוח
11	אבטחת רשת וגישה מרחוק
11	קישוריות לרשת האינטרנט
12	הוצאת נתונים והצפנה
12	אבטחת מערכות ועדכון
13	אבטחת מערכות קצה
13	מניעת קוד עיון
13	הפרדה בין סביבות ואבטחתן
14	ניהול משתמשים
14	סיסמאות ואמצעי הזדהות
15	ניהול הרשאות ובקרת גישה
16	יישום בקרות
16	תכנית היערכות לניהול אירועי אבטחת מידע
17	מיקור חוץ (Outsourcing)
18	שירותי מחשוב ענן
19	פרק ד': הגנה פיסיית
19	אבטחה פיסיית
20	אבטחת ציוד וניירת



20	תחקור אירועי אבטחת פיסית
<b>21</b>	<b>פרק ה': משאבי אנוש והדרכה</b>
21	גיוס עובדים
21	הוראות לעניין יישום נהלי אבטחת מידע
22	ניוד או סיום העסקה
22	עובדי חוץ ומבקרים
22	הדרכה
<b>24</b>	<b>פרק ו': פעילות בערוצי תקשורת</b>
24	בקורות בתהליך הרישום לביצוע פעולות
24	בקרה על הזדהות לקוחות
24	ניהול סיסמאות לקוח
25	מסירת מידע באמצעים אלקטרוניים
<b>26</b>	<b>פרק ז': תיעוד איחזור וגיבוי המידע</b>
26	תיעוד
26	אחזור מידע
26	גיבוי ואחזור נתונים
26	סיום או הפסקת פעילות לשכה



## פרק א': כללי

### מבוא

1. ניהול נכסי המידע וההגנה עליהם מהווה רכיב מרכזי בהפעלת שירותי נתוני אשראי ושירותי 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. הוראה זו קובעת עקרונות וכללים לניהול והגנה על נכסי המידע שבידי הלשכה באופן שתשמר פרטיות הלקוחות, תובטח שלמות המידע וזמינותו, וימוזער הסיכון לחשיפת או העברת המידע לגורמים שלא הורשו להחשף לו.
4. לאור חשיבות פעילות הלשכה והצורך לשמור על פרטיות לקוחות הלשכה, מצופה ממנה לאמץ סטנדרטים גבוהים לניהול הגנת המידע ואבטחתו.

### תחולה

5. הוראה זו תחול על לשכת אשראי (להלן - **הלשכה**) כמשמעותה בחוק נתוני אשראי, התשע"ו - 2016 (להלן - **החוק**). על לשכת מידע על עוסקים יחולו תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.
6. ההוראה חלה על פעילות הלשכה במתן שירותים לפי סעיפים 12 ו-13 לחוק נתוני אשראי, לרבות עיסוקים אשר הותרו לה לפי כללי נתוני אשראי.
7. האיום העיקרי שהנחיות מסמך זה מתמודדות איתו הינו זליגת מידע של לקוחות פרטיים שמקורו במאגר נתוני האשראי, אשר יעובד ויישמר במערכות הלשכה. ההנחיות משקפות נהלים מיטביים הנהוגים בארגונים המנהלים מאגרי מידע רגיש.
8. לשכת אשראי שתפעל בסביבת האירוח של בנק ישראל (באופן מלא או חלקי), או תפעל באופן שבו לא נשמרים נתוני אשראי מהמאגר במערכת, רשאית לפנות לממונה על שיתוף נתוני אשראי (להלן - **הממונה**) ולבקש הקלות ביישום סעיפי ההוראה, או יישום ההנחיות רק על אזורים מסויימים ומבודדים בלשכה החשופים למאגר האשראי והמידע שבו.
9. הממונה רשאי לפטור לשכה מקיום סעיפים מסויימים בהוראה זו, לאחר שבחן את בקשתה ונימוקיה אשר נמסרו לו בכתב, ורשאי הממונה לקבוע כי הפטור יינתן לתקופה קצובה כפי שתקבע על ידו.

### הגדרות ומינוחים

.10

- כהגדרתו בחוק הגנת הפרטיות, תשמ"א-1981, וכל מידע אשר סווג על ידי הלשכה כמידע רגיש לעניין הוראה זו.	"מידע רגיש"
---	-------------



<p>- כלל המערכות התומכות בפעילות העסקית ואשר יש להן חשיבות בהיבטי אבטחת מידע, לרבות ציוד ממוכן, תשתיות וטכנולוגיות התומכות בתפעולן, בין השאר: שרתים, ציוד תקשורת, ציוד הגנת מידע.</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>- סריקה לאיתור חולשה במערכת העלולה להוביל להתממשות איום.</p>	<p><b>"סריקת חשיפות אבטחת מידע – Vulnerability Scan"</b></p>
<p>- קוד המושגל על ידי משתמש זדוני ועשוי לגרום לביצוע פעולות לא רצויות, פגיעה במערכות הלשכה וזליגת 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>- 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

11. לפחות אחת לשנה ובעת ביצוע שינוי מהותי ידון דירקטוריון הלשכה במסמך המדיניות לניהול המידע והגנתו ויאשר אותו.
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 מידי לדירקטוריון.
  - 12.11. הגדרת דיווחים נוספים לממונה, מעבר לדיווחים שנקבעו בסעיף 27 להלן.
13. לפחות אחת לשנה ובעת ביצוע שינוי מהותי ידון הדירקטוריון בחשיפות לסיכונים הנובעים מניהול המידע והגנתו כפי שהם מוצגים במסמך סקר הסיכונים לרבות מבחני החדירה ובעקבות ממצאי דוחות הביקורת בנושא וכן ידון בתוכנית להפחתת הסיכונים שזוהו.
14. לפחות אחת לשנה ידון הדירקטוריון באירועי אבטחת מידע מהותיים שהתרחשו ובהחלטות והפעולות שבוצעו.

### ההנהלה

15. תקיים מסגרת עבודה מתאימה שתבטיח בין היתר יישום אפקטיבי של מדיניות הדירקטוריון.
16. תדון, לכל הפחות אחת לשנה, בתוצאות מסמך סקרי הסיכונים לרבות מבחני החדירה בדגש על הסיכונים המרכזיים, ובתוכנית שנקבעה להפחתת הסיכונים, תעמיד לה משאבים נאותים, ותעקוב לכל הפחות ברמה רבעונית אחר יישומה.
17. תדון בממצאי דוחות הביקורת בנושא אבטחת מידע והגנת הפרטיות של המבקר הפנימי ושל הממונה שיועברו אליה ותבחן את הצורך בעדכון מסמך המדיניות, נוהלי העבודה ואמצעי הבקרה ואבטחת המידע.
18. לפחות אחת לרבעון תדון ההנהלה באירועי אבטחת מידע שהתרחשו (לרבות כאלו שלא הובילו לפגיעה חמורה) ההחלטות והפעולות שבוצעו.



19. 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. תגדיר את סוגי הפעילויות והאירועים לגביהם נדרש דווח, לרבות דיווח בזמן אמת, והגורמים המוסמכים לטיפול באירועים כאמור.

#### ממונה על אבטחת מידע

21. ההנהלה 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 והגנתו, 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 תוכנית לבקרה שוטפת אחר העמידה בדרישות חוק הגנת הפרטיות ותקנותיו, בצע 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 שנקנתה 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 חודשיים.
  - 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.

### ביקורת פנימית

25. תוכנית הביקורת הפנימית תכלול ביקורת, שתבצע 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 מיידי במקרים הבאים :

- 27.1. ארוע של פגיעה בשלמות המידע.
  - 27.2. נפגעו או הושבתו מערכות ייצור המכילות מידע רגיש ליותר מ-3 שעות, למעט השבתה יזומה.
  - 27.3. יש אינדיקציות לכך שמידע רגיש אודות לקוחות הלשכה נחשף או דלף אל מחוץ לכותלי הלשכה.
  - 27.4. התממשות אירועים חריגים, לרבות ניסיונות מהותיים של חדירה ותקיפה, חדירה בפועל למערכות מחשב, קריסה של מערכות מרכזיות, הפעלת תוכנית להתמודדות עם אירועים חריגים וכיוצא באלה.
  - 27.5. הפסקה של שירותים מהותיים כתוצאה מהשבתה לא מתוכננת של פעילות המערכות הממוכנות למשך יום עסקים אחד או יותר.
  - 27.6. כל אירוע משמעותי אחר שהתרחש או כמעט והתרחש בעל השפעה מהותית על ניהול המידע והגנתו.
28. הממונה רשאי להורות ללשכה, להודיע על אירוע האבטחה בהתאם לנסיבות.
29. הלשכה תעביר לממונה, מראש ובתוך פרק זמן סביר דיווחים לגבי הנושאים הבאים :
- 29.1. שינויים מהותיים צפויים במדיניות ניהול טכנולוגיית המידע ;
  - 29.2. הסבה מהותית של מערכות מחשב או מחשב מחדש של מערכות מרכזיות ודומיהם ;
  - 29.3. שינוי מהותי בערוצי התקשורת ;
  - 29.4. יוזמה טכנולוגית חדשה ;
  - 29.5. כל נושא אחר בעל השפעה מהותית על ניהול המידע והגנתו.



## פרק ג': הגנת המידע

### מסגרת עבודה (Framework) לניהול הגנת מידע

30. מסגרת העבודה לניהול הגנת המידע תתייחס בין היתר לנושאים הבאים :
- 30.1. מדיניות לניהול המידע והגנתו שיתבסס על תפיסת הגנת המידע לכל הפחות כמפורט בהוראה זו ;
- 30.2. סקר הערכת סיכוני אבטחת מידע ומבחני חדירה כחלק מסקר הערכת סיכונים כאמור בהוראה לגבי ניהול סיכונים ;
- 30.3. מסגרת ארגונית הכוללת סמכויות ותחומי אחריות, קווי דיווח, גופי פיקוח ובקרה, היבטים של משאבי אנוש והדרכות ;
- 30.4. 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.

### סקר הערכת סיכוני אבטחת מידע ומבחני חדירה

31. הלשכה תיישם, כחלק מתכנית העבודה הרב-שנתית סקר אבטחת מידע ומבחני חדירה המכסים את מערכות המידע והתהליכים הארגוניים ותיישם תכניות להפחתת הסיכונים שהתגלו.
32. הסקר ומבחני החדירה (להלן **סקרים**) יבחנו את התאמת כל מערכות המידע והתהליכים העסקיים למדיניות ולנהלי אבטחת המידע של הלשכה, לרבות ברמת בדיקת קיום ואפקטיביות הבקורות להגנה על המידע בפני סיכונים פנימיים וחיצוניים.
33. הערכת הסיכונים תתייחס למכלול של איומים פוטנציאליים, ביניהם משתמשי המערכת, סביבת המערכת ומיקור חוץ.
34. הערכת הסיכונים תתייחס הן לסביבת הייצור (Operation Technology) והן לסביבות הפיתוח הבדיקות והגיבוי, המכילות מידע רגיש.
35. 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.
36. תכנית העבודה לביצוע הסקרים תיישם את הנושאים הבאים :
- 36.1. כיסוי של כל רמות האבטחה של התהליכים והמערכות, לרבות: הגנות פיסיות וסביבתיות, הגנות תשתיות הכוללות אחסון, מערכות הפעלה, רשתות, בסיסי נתונים, רכיבי תוכנה<sup>1</sup> (Middleware) ודומיהם, הגנות אפליקטיביות, הגנות ברמת הלוגיקה העסקית המיושמת במערכת וכן התהליכים הסובבים את המערכת כגון ניהול משתמשים והרשאות, תהליכי גיבוי, ניטור וכדומה.

<sup>1</sup> תוכנת מחשב המחברת רכיבי תוכנה או יישומים. למשל תוכנה בין יישומים לשרתי מסד נתונים.





- 36.2. ביצוע מבחני חדירה תקופתיים הכוללים : מבחן המדמה ניסיון תקיפה מרשתות חיצוניות (כגון רשת האינטרנט, חיבור לספקים או שותפים עסקיים), בדיקות הנדסה חברתית, התחזות ופישננג, ותקיפה מתוך הרשת. ה"פורצים" יפעלו הן כמשתמש קיים והן כפורץ ללא חשבון קיים.
- 36.3. 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.
37. תדירות ביצוע הסקרים תיקבע בהתאם למידת החשיפה של המערכת לאיומים, רגישות המידע המנוהל במערכת ושינויים שבוצעו במערכת או בסביבתה.
38. תדירות ביצוע הסקרים למערכות מידע שיש אליהן גישה מרשת ציבורית לא תפחת מאחת ל-12 חודשים. תדירות ביצוע הסקרים עבור מערכות שאין אליהן גישה מרשת ציבורית, בהתאם לרגישות המערכת, לא תפחת מאחת לשנתיים.
39. על אף האמור לעיל, יש לבצע סקרים טרם הטמעת שינוי משמעותי במערכת מידע, או בסביבתה הטכנולוגית, או טרם יישום של שירות חדש.
40. הסקרים יבוצעו על ידי גורם מקצועי, עצמאי, ובלתי תלוי שאינו מעורב בפיתוח והטמעת מערכות בלשכה או בבעל עניין בה ושהינו בעל ניסיון של 3 שנים לפחות בביצוע פעילות דומה (להלן- גורם מבקר).
41. לאחר תיקון הליקויים יתבצעו בדיקות חוזרות ע"י הגורם המבקר על מנת לוודא שאכן בוצעו התיקונים הנדרשים.
42. הלשכה תגדיר תכנית לביצוע הסקרים אצל ספקי מיקור חוץ המאחסנים 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 שיזם ספק מיקור החוץ ובתנאי שהוא עומד בדרישות חוזר זה לביצוע סקרים ושהסקרים בוצעו על ידי גורם בלתי תלוי.

#### **בקה וניטור**

43. 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 התכחות.
44. נתיב הבקרה יוגן משינוי בלתי מורשה, יתבסס על רישום ממוכן ויכלול את המידע הבא :
- 44.1. פעולות לרבות ניסיונות חיבור למערכות, שאילתות, עדכוני נתונים, הדפסת דוחות ושליחת מידע המבוצעים במערכות המידע כולל ניסיונות לביצוע פעולות כאמור.



- 44.2. מידע על מועדי הגישה למערכת, תיעוד המקור לביצוע הפעולות והגורם שביצע או ניסה לבצעה, רכיב המערכת אליו בוצעה הגישה, סוג הגישה, היקפה ואם הגישה אושרה או נדחתה.
- 44.3. במערכות שהמידע המנוהל בהן עשוי להשפיע באופן מהותי על עסקי הלשכה ויציבותה ישמר ערך טרום ביצוע הפעולה ולאחריה.
45. פרק הזמן לשמירת נתיב בקרה יתאים למטרות הנתיב ובכל מקרה לא יפחת מ-24 חודשים.
46. הלשכה תקיים מערך לניטור מערכות מידע (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, תוך מתן דגש למערכות תשתית ומערכות אפליקטיביות.
47. הלשכה תקיים נוהל בדיקה שגרתי של נתוני נתיב הביקורת ודיווחי הניטור, ותערוך דוח של הבעיות שהתגלו וצעדים שננקטו בעקבותיהן.
48. 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.

#### תהליכי תחזוקה ופיתוח

49. שילוב ניהול הגנת המידע בתהליכי פיתוח ותחזוקה יכול לכלל הפחות, את השלבים הבאים:
- 49.1. ייזום ואפיון מערכת: הערכת סיכוני חשיפת מידע רלוונטיים והגדרת דרישות הגנה מתאימות בעת ייזום ואפיון מערכת.
- 49.2. פיתוח מערכת: מימוש והטמעת דרישות האבטחה המופיעות באפיון המערכת. הגנת המידע תוטמע בכל רכיבי המערכת, לרבות: תשתיות, אפליקציה (ככל שרלוונטי), וברמת הלוגיקה העסקית המיושמת במערכת.
- 49.3. בדיקת מערכת: מבחני חדירה לרבות סקר אבטחת מידע, יבוצעו בטרם הטמעת המערכת, על ידי גורם בלתי תלוי שאינו מעורב בפיתוח והטמעת המערכות.
- 49.4. קליטת מערכת: קבלה והתקנה מאובטחת ומאושרת של המערכת על ידי גורמים מוסמכים לכך, תוך וידוא יישום דרישות הגנת המידע.
50. הלשכה תוודא כי סיכונים שעלולים להיווצר בעת ביצוע פעולות תחזוקה ופיתוח במערכות מידע ובתהליכים לרבות במערכות מקוונות או בתהליכי הזדהות של לקוחות לשירותים אלקטרוניים, יטופלו באופן מספק, טרם ביצוע השינוי.
51. ממונה על אבטחת מידע יקבל דיווח טרם ביצוע פעולות פיתוח ותחזוקה במערכות המידע, ויקבע את רמת המעורבות הנדרשת מצדו בהתאם לאופי השינוי, לרגישות נתונים ולהשפעה אפשרית של השינוי על סיכונים וחשיפות המערכת.
52. בעת התקשרות לפיתוח מערכת מידע, הלשכה תבטיח כי קוד המקור עבר בדיקה נגד חשיפות אבטחת מידע ואי קיום קוד עוין.



### אבטחת רשת וגישה מרחוק

53. הלשכה תשתמש באמצעי הגנה המתאימים לסיכוני גישה מרחוק לרשת הלשכה, כגון אמצעי סינון תקשורת ותוכן, אמצעי ניטור ותהליכי בקרה.
54. האמצעים יותאמו לסיכונים ייחודיים לשירותי רשת שונים, כגון דואר אלקטרוני, מתחמי כתובות - 2DNS, שירותי העברת קבצים, שירותי Web ועוד.
55. 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.
56. הלשכה תיישם מנגנונים למניעת חיבור של אמצעים בלתי-מורשים לרשת הלשכה.
57. רשת הגיבוי תיושם כרשת ייעודית, נפרדת מרשתות אחרות כולל אמצעי גישה לרשת זו בעזרת זיהוי ביומטרי או כרטיס חכם המאפשר גישה חד-חד ערכית למשתמש.
58. 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:
- 58.1. הפרדה לוגית, הכוללת חסימת גישה ישום אחד למסד הנתונים האחר.
- 58.2. הגנות לוגיות נוספות, כגון שימוש בשמות מסדי נתונים וטבלאות שונות.
- 58.3. הפרדה לוגית בין האפליקציות, הכוללת מסכי הזדהות שונים ומובחנים זה מזה של עובדי הלשכה.
59. הלשכה תגדיר אמצעי אבטחה מיוחדים כגון הצפנה מקצה לקצה וניטור מוגבר על גבי תשתית תקשורת ציבורית.
60. הלשכה תיישם מנגנונים שינטרו ויצמצמו את הסיכונים הנובעים מחיבור התקן נייד זר או התקן נייד בלתי-מאובטח לרשת הלשכה.

### קישוריות לרשת האינטרנט

61. אפשרות גישה מן הרשת הפנימית כלפי חוץ, תותר רק אל שרתים הנמצאים באזורי החיץ. לא תתאפשר גישה ישירה מתחנות ומשרתי הרשת הפנימית לרשת חיצונית כלשהי.
62. 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.
63. גישה משתמשים לרשת האינטרנט הציבורית תבוצע באמצעות מערכת גלישה וירטואלית.
64. קישוריות רשת הלשכה לאינטרנט תאובטח לפחות ע"י אנטי וירוס, מסנני תוכן, מערכת לאיתור ניסיונות חדירה (IDS) ו firewall.

<sup>2</sup> שרות הממיר כתובות IP לכתובות מילוליות (URL) ובכך מקל את השימוש ברשת האינטרנט.



65. 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.

#### הוצאת נתונים והצפנה

66. הלשכה תמפה את ערוצי התקשורת שלה עם לקוחותיה.
67. הלשכה תקבע את האופן שבו תאושר הוצאת נתונים אל מחוץ לחצרותיה, בהתאם לרמת רגישותם.
68. הלשכה תגדיר ותיישם תהליכי הגנה הכרחיים להעברת מידע מחוץ לחצרותיה (כגון: הצפנת תווך התקשורת והנתונים מקצה לקצה, וידוא הגעת נתונים ליעדם, הגבלת גישה לנתונים על בסיס "הצורך לדעת" וכדומה) בהתאם לרמת רגישות מידע.
69. הלשכה תצפין נתוני אשראי למניעת האזנה או התערבות במקרים הבאים:
- 69.1. תקשורת באמצעות האינטרנט;
  - 69.2. גישה מרחוק למחשבי הלשכה;
  - 69.3. סיסמאות לבעלי הרשאת גישה;
  - 69.4. תקשורת בין סניפי הלשכה, ככל שישנם;
  - 69.5. תקשורת ללקוחות קבועים של הלשכה;
  - 69.6. מקרים נוספים כפי שיבחנו ויוגדרו ע"י הלשכה כבעלי סיכון גבוה.
70. הלשכה תיישם הצפנה להגנה על חיסיון מידע רגיש בתווך בהתקשרות מחוץ לחצרותיה.
71. הלשכה תיישם טכניקות הצפנה מוכרות שהוכחו כיעילות, ותתקף את האפקטיביות של אלה באופן תקופתי.
72. הלשכה תגדיר נהלים מתאימים ליצירה, עדכון, חידוש, התקנה וביטול של מפתחות הצפנה ככל שרלוונטי לפעילותה.

#### אבטחת מערכות ועדכון

73. הלשכה תשמור רשימה עדכנית של תשתיות ומערכות מידע לצורך הגנה על המידע. הלשכה תגדיר תהליכים לשמירת עדכניות הרשימה.
74. הלשכה תגדיר ותיישם עדכוני אבטחת מידע שוטפים ומבוקרים למערכות המידע ולתשתיות באופן תקופתי, תוך התייחסות למקוריות קבצי העדכון, בדיקת עדכונים בטרם יישומם, ושמירה על יציבות מערכות בתהליך העדכון.
75. הלשכה תשמור על רמת עדכניות גבוהה של גרסאות מערכות הפעלה ובסיסי נתונים, אשר לא תפחת מ- 2 גרסאות עיקריות לאחור של היצרן.
76. הלשכה תתייחס לסיכונים הנובעים מחוסר עדכניות או היעדר תמיכה במערכות המידע.
77. הלשכה תעקוב באופן תדיר אחר פרסום עדכוני אבטחת מידע למערכותיה, ותיישם עדכונים קריטיים בתוך פרק זמן שלא יעלה על חודש ימים ועדכונים ברמת חשיבות שאיננה קריטית



בתוך פרק זמן סביר, בהתייחס לרמת החשיפה של מערכותיה לסיכונים הקשורים לעדכונים אלה. לא ייעשה שימוש במערכות מידע שהיצרן לא תומך בהיבטי אבטחה שלהן אלא אם כן ניתן מענה אבטחתי מתאים.

#### **אבטחת מערכות קצה**

78. הלשכה תיישם אמצעי הגנה על מערכות קצה, תוך התחשבות בסיכוני הפעלת קוד עוין וסיכוני חדירה למערכות, תוך ניצול התקנים המחוברים למערכות קצה.
79. הלשכה תיישם מנגנונים טכנולוגיים אשר יודאו כי רק אפליקציות שאושרו להתקנה ע"י גורמי אבטחת המידע יוכלו להיות מותקנות על גבי מערכות קצה.
80. הלשכה תשתמש במערכות בקרה, שמטרתן צמצום סיכון של זליגת נתונים רגישים ממערכות קצה או הגבלת היכולת לשמור מידע רגיש על מערכות קצה.
81. הלשכה תיישם הצפנת מידע רגיש במערכות קצה ניידות (כגון מידע הנמצא על מחשבים ניידים, טאבלטים, התקני אחסון ניידים וטלפונים ניידים), במטרה למזער את הסיכון של חשיפת נתונים רגישים.

#### **מניעת קוד עוין**

82. הלשכה תטמיע אמצעי אבטחה למניעת חדירה והתפשטות קוד עוין במערכותיה, שיכללו מספר שכבות אבטחה כגון: סינון תקשורת וקבצים נכנסים, סריקת מערכות קבצים, הגנה בזמן אמת על שרתים או תחנות קצה, ומערכות ניטור ומניעה ייעודיות.
83. הלשכה תעדכן בתדירות גבוהה את אמצעי האבטחה האמורים לעיל, ותגדיר תהליכים לוודוא עדכניות אמצעי האבטחה כאמור (כגון: קבלת התרעות על כשל בעדכון קבצי חתימות).
84. בעת חיבור אמצעי מדיה למערכות מידע יעשה שימוש במנגנוני הגנה אפקטיביים המונעים חדירת קוד עוין, כגון שימוש במערכות "הלבנת קבצים". חיבור אמצעי מדיה למערכות הלשכה תתבצע בהתאם ל"רשימה לבנה" מנוהלת מרכזית, של אמצעים מורשים לחיבור.

#### **הפרדה בין סביבות ואבטחתן**

85. סביבת היצור תופרד מסביבות אחרות, כגון פיתוח ובדיקות.
86. 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.
87. רשת המשתמשים תופרד מסביבות אחרות וכל גישה מהסביבה תסונן על ידי מערכת חומת אש (firewall).
88. הפרדת הסביבות תתייחס גם לתשתיות עזר תומכות סביבת התקשוב.
89. הרשאות משתמשים לסביבות ייצור תנוהלנה בנפרד מההרשאות לסביבות האחרות.
90. העברת נתונים מסביבת ייצור לסביבה אחרת תתבצע באישור הממונה על אבטחת המידע, או מי מטעמו.



91. העברת מערכות ונתונים מסביבות פיתוח ובדיקות לסביבת ייצור תיערך בצורה מבוקרת, בהתאם לנהלים, כדי למנוע פגיעה בנתונים בסביבת הייצור.

#### ניהול משתמשים

92. הלשכה תבצע זיהוי אישי חד ערכי של כל גורם בעל גישה למערכות המידע כתנאי מוקדם למתן גישה. במקרים חריגים של ספקים ועובדים בהם לא ניתן לקיים האמור לעיל תיישם הלשכה אמצעים חלופיים מתאימים.

93. יקבעו כללים וכלים לזיהוי ולמתן הרשאות לגורמים שונים לרכיבי טכנולוגיית המידע. כללים אלו יביאו בחשבון את רמות הסיכון הנגזרות ואת מסגרת האחריות והסמכות של המשתמשים, על פי סיווג לקבוצות.

94. 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 בתום הפעילות.

95. 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.

96. חשבון משתמש ישויך לעובד מסוים, ותוגדר אחריותו של העובד על חשבון זה ועל הפעולות המבוצעות במערכות הלשכה באמצעות חשבון זה.

97. 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. בנוסף, תוגדר מדיניות החלפת סיסמאות סדירה במשתמשים אפליקטיביים.

98. הלשכה תגדיר תהליכי סקירה תקופתיים ומתועדים שמטרתם לוודא את הצורך בקיום חשבונות המשתמשים. תהליכי הסקירה לכלל החשבונות, יבוצעו לכל הפחות אחת לשנה.

99. הלשכה תגדיר את אופן נעילת חשבון משתמש במקרה של אי שימוש בחשבון במשך תקופה ממושכת, לכל היותר 90 יום, ואת תהליך אישור שחרור נעילה זו.

#### סיסמאות ואמצעי הזדהות

100. הלשכה תגדיר אופן הזדהות למערכות מידע, באופן המתאים לרמת רגישות המידע המנוהל במערכת ולסיכונים השונים בתהליך ההזדהות.

101. הלשכה תגדיר נהלים המתייחסים למסירת אמצעי הזדהות, כגון מסירת אמצעי הזדהות באופן מאובטח למשתמש לאחר זיהויו, שמירה על סודיות הסיסמה והחלפת סיסמה ראשונית על ידי המשתמש.

102. יש לאמת את זהות המשתמש כאשר נמסרת לעובד סיסמה ראשונית למערכת. המשתמש יחויב לשנותה בהתחברות הראשונה למערכת. תוקף הסיסמה הראשונית ייקבע למינימום אפשרי, בהתאם לאופי השימוש בחשבון ולא יעלה על 14 ימים.



103. סיסמאות או אמצעי הזדהות אחרים לא יישמרו באופן גלוי (Clear Text) או באופן הניתן לשחזור ברשומות, בזיכרון או במאגרי מידע.
104. 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.
105. מנהלני מערכות וגורמים בעלי הרשאת גישה לנתוני אשראי פרטניים יבצעו הזדהות באמצעות 2-Factor Authentication.

### ניהול הרשאות ובקרת גישה

106. 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.
107. מתן הרשאות גישה יתבצע על בסיס הגדרות תפקיד. הרשאות הגישה לכל תפקיד תהיה במידה הנדרשת לביצוע התפקיד בלבד.
108. 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.
109. לצורך בקרת 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, סודיות ושלמות הנתונים ומניעת הכחשה.
110. לא תותר העתקת נתוני אשראי ממחשב של הלשכה להתקני אחסון נתיקים.
111. גישה מרחוק אסורה, למעט אם הוסדר מנגנון שיופעל לפי הערכת הסיכונים לנושאים הבאים:
- 111.1. קבלת אישור גישה מרחוק לכל אירוע, מתן אישור בעת ביצוע הגישה במחשב אליו ניגשים;
- 111.2. הפעלת מנגנון ניתוק התקשורת, גישה מרחוק, לאחר פרק זמן שיקבע;
- 111.3. יופעל רישום, LOG, של הפעילות הנעשית באירוע "גישה מרחוק";
- 111.4. 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;



- 111.5. כלי לזיהוי ולרישום גישה לרשת מגורמים מרוחקים, ניסיונות חדירה, ניסיונות זליגת מידע רגיש החוצה וגישה לקבצים רגישים. כלי זה יעקוב אחר הפעילות ברמת הרשת;
- 111.6. תיעוד ברמת האפליקציה של גישה למידע רגיש ע"י משתמש. התיעוד יבדיל בין סוגי הגישה לנתונים: יצירה, קריאה/צפייה, כתיבה;
- 111.7. תיעוד ברמת האפליקציה של ניסיונות לעקוף את מנגנוני ההזדהות;
- 111.8. כלים לאכיפה של הקשחת השרתים ותיעוד ניסיונות לחרیגה ממדיניות ההקשחה;
- 111.9. כלים להגנת מסדי נתונים מניסיונות חדירה, גניבת נתונים, שיבוש, הזרקת קוד, מחיקה והשתלה של נתונים שלא ע"י האפליקציות הייעודיות;
- 111.10. הפעלת מנגנון הקלטת תעבורה מלאה (Full Packet Capture) או כל מנגנון אחר שיתעד את הפעולות שבוצעו בעת התחברות מרחוק.
112. הלשכה תגדיר תהליכי סקירה תקופתיים, שמטרתם לוודא את הצורך בקיום הרשאות משתמשים. תהליכי הסקירה לכלל הרשאות, יבוצעו לכל הפחות אחת לשנה.
113. תהליכי סקירה תקופתיים של הרשאות ספקים חיצוניים, עובדי מיקור חוץ ועובדים זמניים יבוצעו בתדירות גבוהה יותר.

#### יישום בקרות

114. הלשכה תגדיר בקרות מתאימות להתמודדות עם סיכונים הגנת המידע בהתאם להערכת הסיכון. הבקרות יתייחסו לכל הפחות, להגנה על המידע באזורים ותהליכים אלו:
- 114.1. בציוד קצה.
- 114.2. בתהליך העברת המידע בין אתרים או בין ארגונים.
- 114.3. בשרתים, מסדי נתונים ובגיבויים.
- 114.4. בתהליכי הזדהות והרשאות.

#### תכנית היערכות לניהול אירועי אבטחת מידע

115. הלשכה תגדיר תכנית היערכות לניהול אירועי אבטחת מידע, בהתאם להערכת סיכונים ולניתוח תרחישי איום (כגון: גישה לא מורשית לנכסי המידע בלשכה, זליגת מידע, התחזות, נוזקות, הונאה, מניעת שירות וכדומה) אשר תתייחס לשלבי האירוע הבאים:
- 115.1. גילוי - גילוי וזיהוי השלב בו נמצא האירוע תוך פירוט שלבי פעולה (בידוד, חקירה, איסוף ראיות, הסקת מסקנות וכדומה).
- 115.2. הערכת מצב - בירור וניתוח האירוע ובחינת דרכי פעולה להתמודדות, לרבות הפסקת פעילות באופן זמני באירועים בחומרה גבוהה.
- 115.3. הכלה - השגת שליטה על האירוע.
- 115.4. בלימה - עצירת החמרה של האירוע.
- 115.5. התאוששות - הכרעת האירוע תוך מזעור הנזק שנגרם.
- 115.6. חזרה לשגרה - חזרה לפעילות מלאה של הלשכה לאחר תיקון כל נזק שנגרם.





116. בנוסף, התכנית תתן ביטוי לנושאים הבאים לפחות:
- 116.1. דרכי תגובה ופעולה, בהתייחס לתרחישי איום שונים, והגורמים האחראים על הפעלתן.
  - 116.2. דרכי התקשרות והעברת מסרים עם גורמים פנימיים וחיצוניים, ובכללם לקוחות, בהתאם לתרחישים שונים.
  - 116.3. מתכונת ותדירות הדיווח על האירועים, גורם מדווח, נמען הדיווח וזמן התגובה הסביר לדיווח.
117. התכנית תעודכן על בסיס שנתי, בהתאם להערכת סיכונים מעודכנת, ותכלול התייחסות גם לעובדים חדשים ולמיקור חוץ.
118. הלשכה תקבע מנגנון דיווח על אירועי אבטחת מידע שיהיה נגיש לעובדים.
119. הלשכה תקים צוות תגובה להתמודדות עם אירועי אבטחת מידע.
120. הלשכה תקיים, לכל הפחות, אחת לשנה תרגול של כלל המערכים הרלוונטיים שמטרתו להכין אותו להפעלת התוכניות שהוזכרו לעיל ולשיפורן בהתאם ללקחי התרגול.
121. 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)

122. הלשכה תיישם את ההוראות הבאות הנוגעות להתקשרות והגנה על המידע בעת השימוש במיקור חוץ:
- 122.1. התקשרות לצורך מיקור חוץ תיעשה בהסכם כתוב.
  - 122.2. בכל התקשרות לקבלת שירותי מיקור חוץ יש לבחון את סיכוני אבטחת מידע הכרוכים בהתקשרות.
  - 122.3. 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.
  - 122.4. אין לבצע מיקור חוץ לשירותי דרוג אשראי והפקת דוח אשראי.
  - 122.5. הלשכה תגדיר נוהל לדרישות הגנת מידע בהתייחס לסיכוני מיקור חוץ ולאבטחת שרשרת האספקה. נוהל זה ייושם בעת התקשרות עם גורם מיקור חוץ חדש.
  - 122.6. בהסכם התקשרות לקבלת שירותי מיקור חוץ יש להתייחס, בין היתר, לנושאים הבאים:
    - 122.6.1. הגדרת תחומי אחריות של כל אחד מהצדדים להסכם לרבות קבלני משנה.
    - 122.6.2. הגדרת רמת שרות (SLA).
    - 122.6.3. חובת סודיות, אבטחת מידע וגיבוי.



- 122.6.4. הסדרים להפסקת הסכם וליישוב מחלוקות.
- 122.6.5. יכולת הלשכה לבצע ביקורות על פעילות נותן השירות.
- 122.6.6. אפשרות שהלשכה תתפעל ותתחזק את פעילות מיקור החוץ במקרים בהם נותן השירות חדל ממתן השירות, כגון ע"י החזקת תוכנות מקור והרשאות אצל נאמן.
- 122.6.7. 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.
- 122.6.8. בעת הצורך בהעברת נתונים, יבוצע תהליך של גישה מבוקרת לנתונים פרטניים ולא שכפול כלל בסיס הנתונים.
123. אספקה של שירותי תחזוקה מרחוק (מידע, תוכנה או ציוד תקשורת) על ידי גורמי מיקור חוץ, תבצע בתנאים הבאים :
- 123.1. נותן שירות מיקור חוץ יקבל אישור פוזיטיבי להתחברות, לפני תחילת עבודתו. הממונה על אבטחת המידע יקבע מי בעל הסמכות לאשר התחברות מסוג זה.
- 123.2. גישה מרחוק תתאפשר באמצעות משתמש ייעודי לכל נותן שירות מיקור חוץ ובתיאום מראש עם הלשכה לאופן ההתקשרות ותדירותה.
- 123.3. גישה מרחוק תתאפשר לזמן מוגבל על פי סוג הפעילות אותה יבצע נותן שירות מיקור החוץ.
- 123.4. הלשכה תיישם הזדהות חזקה לצורך כל גישה מרחוק של נותן שירות מיקור חוץ.
- 123.5. הלשכה תיישם הצפנה מקצה לקצה לכל אורך נתיב ההתקשרות מרחוק שהינה הצפנת תווד התקשורת/הנתונים מהתחנה/השרת.
- 123.6. הלשכה תנטר כל פעילות שבוצעה בגישה מרחוק.
- 123.7. חשיפת נותן שירות מיקור חוץ למידע אודות לקוחות תצומצם עד למינימום הכרחי, ובמידת האפשר תחסם במלואה.

#### שירותי מחשוב ענן

124. הלשכה רשאית להעביר לסביבת ענן ציבורי רק מערכות שאינן מנהלות מידע רגיש.
125. שימוש בשירותי מחשוב ענן יהיה כפוף להנחיות לעניין מיקור חוץ.
126. בטרם הפעלת מערכות מבוססות ענן, על הלשכה לבצע הערכת סיכונים ייעודית ולדון בסיכונים אפשריים, משימוש בשירותים כאמור.
127. גישה לנתונים בענן תבוצע דרך כתובות הלשכה בלבד.
128. הלשכה תעשה שימוש בטכנולוגיות כגון הצפנה, מיסוך נתונים או טוקניזציה בעת שימוש במערכות בסביבת ענן.



129. 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.
130. הלשכה תיידע את הממונה 3 חודשים מראש לגבי כוונתה להעביר מערכות לסביבת ענן ציבורי ותקבל את אישורו לכך.
131. אין בהנחיות לגבי מיקור חוץ בכדי לגרוע מאחריות הלשכה לכל פעולה הנעשית מטעמה או בהסכמתה ע"י אחרים.

### פרק ד': הגנה פיסית

#### אבטחה פיסית

132. הלשכה תיישם את ההוראות הבאות בנוגע לבקרות אבטחה פיסיות שיתייחסו למכלול הסיכונים הפיסיים והסביבתיים באזורים המאובטחים כאמור להלן:
- 132.1. הלשכה תחלק את האתר וסביבת העבודה לאזורים מאובטחים לפי רמת רגישות המידע אליו ניתן לגשת.
- 132.2. הלשכה תיישם מעגלים של בקרות ותיעוד גישה פיסית שרמתם תותאם לרמת רגישות המידע. מעגלים אלו יכללו בקרות מונעות (כגון דלתות נעולות, שערים אלקטרוניים, ומערכות למניעת שריפות) ובקרות מגלות (כגון מערכת מצלמות ומערכות אזעקה).
- 132.3. 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.
- 132.4. 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.
- 132.5. 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.
- 132.6. אזורים המכילים מידע רגיש ימודרו בפני גישה של אנשים שאינם בעלי הרשאה למידע.
133. מידע רגיש יאובטח באמצעות שילוב מושכל של האמצעים הבאים:
- 133.1. אתר חוות שרתים, חדר מחשב מרכזי, ארונות תקשורת ימצאו במבנה קשיח ויזכו באמצעי הגנה פיסיים ההולמים לרמת הסיכון.
- 133.2. בקרת גישה באמצעות אזעקה המחוברת למוקד חיצוני ומופעלת כאשר האתר אינו מאויש.



- 133.3. מחוץ לשעות הפעילות יבוצעו סיוורים יזומים לבדיקת תקינות המערכות, לשמירת נוהלי אבטחה ולפעילות מניעה.
- 133.4. ספקים חיצוניים המגיעים לביצוע עבודות באתרי הלשכה יבדקו טרם ביצוע עבודתם, יזוהו ויירשמו בכניסתם וביציאתם.
- 133.5. באחריות האשראי לאבטחת מידע לקבוע נהלים להגנה ושמירה על מחשבים ואמצעי אחסון ניידים המכילים מידע רגיש.
- 133.6. באחריות האשראי לאבטחת מידע לקבוע נהלים לליווי מבקרים מזדמנים וספקים כולל מחויבותם לשמירת הסודיות.
- 133.7. הלשכה תעזר בחוות דעת של מומחה לאבטחת מידע פיסית.

#### **אבטחת ציוד וניירת**

134. אופן הוצאת ציוד המכיל מידע רגיש מאחד ממעגלי האזורים המאובטחים תיעשה בהתאם להערכת סיכונים.
135. הלשכה תבצע השמדה של ציוד רגיש (פיסי או דיגיטלי) שאין בו שימוש ותגדיר את אופן הטיפול והשמירה עד להשמדתם.
136. ציוד המועבר להשמדה או תחזוקה אל גורם מחוץ ללשכה לא יכיל מידע רגיש.
137. 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 מפוקח.

#### **תחקור אירועי אבטחת פיסית**

138. בעת אירוע אבטחה פיסית נדרש :
- 138.1. לחקור ולתעד את האירוע.
- 138.2. לערב גורמי חקירה חיצוניים ככול שנדרש.
- 138.3. לערב את הממונה על אבטחת המידע וגורמים נוספים בלשכה, בהתאם לאופי האירוע.
- 138.4. להכין דוח אירוע ולהפיצו להנהלה.
- 138.5. לבצע הליך הפקת לקחים ולהפיץ את הידע לגורמים רלוונטיים.



## פרק ה': משאבי אנוש והדרכה

### גיוס עובדים

139. 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.
140. 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.
141. הממונה על אבטחת המידע בשיתוף גורם משאבי אנוש ובתיאום עם גורמים רלוונטיים בלשכה יתוו ויגדירו את יישומם של:
- 141.1. תהליכים ואמצעים לוודא מהימנות עובדים, בהתאם לצורך.
  - 141.2. טיפול בחריגים.
  - 141.3. אופן ביצוע פיקוח והבקרה על עובדים.
142. חוזה הנחתם עם עובדים חדשים יכלול התייחסות לאחריות העובד בכל הנוגע להיבטי סיכונים אבטחת מידע והגנת פרטיות, וילווה בהצהרת סודיות, והכל בהתאם למידת רגישות המידע לו הם יקבלו גישה.
143. חוזה של הלשכה עם חברות להשמת כוח אדם או עם חברות המספקות שירותי מיקור חוץ, יכלול אף הוא התייחסות לסעיפים לעיל.
144. 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.
145. יתבצע תיעוד הכולל פירוט הליכי הגיוס.

### הוראות לעניין יישום נהלי אבטחת מידע

146. 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.
147. האחריות לאבטחת המידע, בין אם הנה מוטלת על עובדי הלשכה ובין אם על מנהליו, מתייחסת לכל ההבטים הרלבנטיים, כולל בין השאר, אבטחה פיסית, אבטחת הרשומות והאבטחה הלוגית.
148. על מנת לוודא כי כל עובד יודע ומודע 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.
149. 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

150. 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.
151. 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 חוק וכו'.
152. 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.
153. יש להסדיר באופן הולם את החובה של העובד על שמירת חסיון המידע לו היה חשוף גם לאחר סיום עבודתו בלשכה.

### עובדי חוץ ומבקרים

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

### הדרכה

156. הלשכה תגדיר תכנית להעלאת רמת מודעות של עובדים לסיכוני אבטחת מידע והגנת הפרטיות (להלן - התכנית).
157. התכנית תשולב במערך הדרכה של הלשכה ותכלול התייחסות לאוכלוסיות העובדים השונות, לרבות עובדי מיקור חוץ.
158. התכנית 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.
159. התכנית תסייע להטמעת נהלי אבטחת המידע והגנת הפרטיות בתהליכי העבודה של הלשכה.
160. 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.



161. עובד חדש, או עובד ששוננו לגביו הקפי ההרשאה, יתודרך 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

### בקרות בתהליך הרישום לביצוע פעולות

162. הלשכה תוודא זהות לקוח (ארגוני או פרטי) בטרם השלמת רישומו לקבלת שירותים מקוונים. הרישום יכול להיות רישום תקופתי או חד פעמי, בהתאם לצורכי הלקוח.
163. 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 לתנוך התקשורת וכדומה. בערוצים מבוססי אינטרנט יעשה שימוש באמצעי הזדהות חזקים או אמצעי הזדהות שאינם קבועים, כגון סיסמאות חד פעמיות הנשלחות בהודעת SMS.
164. 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 הזדהות ללקוח, וצמצום הסיכון לגניבת או העתקת אמצעי זה בדרך אל הלקוח.
165. הלשכה תוודא כי לעובדיה אין גישה לאמצעי הזדהות של לקוחות, העלולה לאפשר ניצול לרעה של חשבון לקוח, למעט עובדים מורשים.
166. 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.
167. בעת שימוש באמצעי זיהוי קבועים הלשכה תגדיר נהלים המאפשרים ללקוח איפוס סיסמה.
168. רישום לקוח לפעילות בערוצים מקוונים, תחייב קבלת הסכמה מתועדת של הלקוח באמצעות טופס ידני או טופס אלקטרוני או באמצעות חשבון המקוון של הלקוח באתר האינטרנט של החברה.
169. ללקוח תינתן הזכות לחזור בו מהסכמתו כאמור.

### בקרה על הזדהות לקוחות

170. הלקוח יקבל בכל כניסה חדשה למערכות הלשכה פרטים על מועד התקשרות קודמת.
171. לקוח יוכל לעדכן פרטים אישיים, למעט פרטים המשמשים לצורך זיהוי.
172. תקיים בקרה שהגורם שעדכן את פרטי הלקוח הוא הלקוח עצמו.

### ניהול סיסמאות לקוח

173. הלשכה תגדיר נהלים לוודוא חוזק סיסמה, שמירה על סודיותה, החלפת סיסמה ראשונית על ידי המשתמש ותוקף הסיסמה הראשונית.
174. סיסמה ראשונית, לרבות כזו הניתנת ללקוח בעת שחרור סיסמה, תימסר ללקוח באמצעות ערוץ תקשורת מאושר ע"י הלקוח כשהיא חסויה אף מהמוסר.
175. הלשכה תיזום החלפת סיסמה ראשונית ללקוח מיד לאחר ההתקשרות הראשונה וכן עדכון ססמה אחת לתקופה.





176. 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.
177. הלשכה תבטל את הסיסמה, שנמסרה ללקוח, במקרים הבאים:
- 177.1. הסיסמה הראשונית לא הופעלה תוך 7 ימים מהנפקתה.
  - 177.2. לבקשת הלקוח או אם קיים חשד שנעשה שימוש לא מורשה בסיסמה.
  - 177.3. לאחר מספר מסוים של נסיונות כניסה כושלים, אשר בכל מקרה לא יעלה על חמישה נסיונות כושלים רצופים.

#### מסירת מידע באמצעים אלקטרוניים

178. קבלת בקשות לשרותי הלשכה ושליחת מסרים מהלשכה למבקשים יכולה להיעשות גם באמצעות אמצעים אלקטרוניים בכפוף לקיום התנאים הבאים:
- 178.1. זיהוי מבקש המידע וקבלת הסכמתו לשליחת המסרים.
  - 178.2. ווידוא כי מבקש המידע זכאי לקבל את המידע.
  - 178.3. בקשת מבקש המידע תתועד.
179. מבקש המידע יכול לחזור בו מהסכמתו זו בכל עת, לפני מסירת הדוח.
180. הלשכה תשמור כל מידע תפעולי הנחוץ לצורך בקרה, ניהול ומעקב אחר קיום תנאי שליחת מידע באמצעים אלקטרוניים.
181. הלשכה תשמור תעוד לפנייה ולמסירת המידע בכפוף להוראות החוק ותקנותיו.
182. הלשכה תקיים הליכי בקרה למניעת העברה שגויה של מסרים או מידע למי שאינו רשאי להעביר את המידע.
183. הלשכה תנטר ותבקר את ערוצי המידע האלקטרוניים על מנת למנוע זליגת מידע או הוצאתו באמצעים לא מורשים.
184. הלשכה תספק ללקוחותיה הנחיות המסייעות לנקוט באמצעי זהירות נדרשים לשמירה על פרטיות מידע, ותנחה אותם כיצד לנהוג במקרה של חשד לאירוע אבטחת מידע.
185. כל הודעה הנשלחת באמצעים אלקטרוניים תישא כותרת המשקפת את תוכנה.



## פרק ז': תיעוד איחזור וגיבוי המידע

### תיעוד

186. הלשכה תשמור ותתעד מידע שהתקבל, נוצר, עובד ונמסר לאחרים במסגרת השירותים שהיא מספקת כלשכה, לרבות:
- 186.1. פניות לקוחות ללשכה כולל קבצי מסמכים, קבצי קול, פרטי פניה מתחילתה ועד סגירתה ואופן הטיפול בפניה.
- 186.2. פניות לקוחות בבקשות לדוחות אשראי או דירוגים יכללו בנוסף הוכחת זיהוי המבקש ובדיקה כי התקבלה הסכמת הלקוח.
- 186.3. נתונים המועברים ללשכה מהמאגר אודות לקוח ישמרו בהתאם לחוק ותקנותיו.
- 186.4. נתונים המועברים ללשכה מהמאגר עבור נתון 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.
187. הלשכה תתעד ל - 7 שנים לפחות מסמכים הקשורים לפעילותה והתנהלותה כדוגמת:
- 187.1. נהלים שקבעה לעמידה בתנאי החוק והתקנות ומכוחו.
- 187.2. דוחות הנוגעים לתוכנית ציות ובקרה על ציות
- 187.3. מסמכים ומידע המהווים בסיס למודל הדרוג
- 187.4. תכנית בקרה פנימית ודוחות בקרה פנימיים כולל כל המסמכים הנדרשים לשם ביצוע בקרה על פעילות הלשכה תנועת עובדים, ספקים ולקוחות.

### אחזור מידע

188. 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.
189. הלשכה תשמר גירסאות תוכנה, חומרה, מערכות הפעלה ועוד ככול שידרש כדי שיאפשרו אחזור חומר.

### גיבוי ואחזור נתונים

190. 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.
191. הלשכה תקבע נהלי התאוששות וחזרה לשגרה בפרק זמן סביר בקרות אירוע כשל באתר הראשי, כדי להבטיח התאוששות מהירה.

### סיום או הפסקת פעילות לשכה

192. פורסמה הודעה על פירוק הלשכה, או החליט בעל הלשכה על הפסקת פעילותו, או ביטל הממונה את רשיונו של בעל הלשכה ינקוט בעל הרשיון פעולות אלה:



- 192.1. יעביר לידי הממונה בתוך שבעה ימי עסקים ממועד הפסקת הפעילות או ביטול הרשיון, מקור או העתק מדויק של כל החומר המתועד המצוי ברשות הלשכה.
- 192.2. לחומר תצורף סכימה ואינדקס שיאפשר איתור מסמך, מידע, נתון וכדומה בחומר שהעבירה הלשכה לממונה.

\* \* \*