לשכת עורכי הדין בישראל
ISRAEL BAR ASSOCIATION
نقابة المحامين في إسرائيل

את/1/22

גילוי דעת מקדים בדבר אבטחת המידע המצוי בידי עורכי הדין

הוועדה המייעצת לוועדת האתיקה בנושא אבטחת מידע

ועדת האתיקה הארצית

לשכת עורכי הדין בישראל
ISRAEL BAR ASSOCIATION
نقابة المحامين في إسرائيل

לשכת עורכי הדין בישראל
ISRAEL BAR ASSOCIATION
نقابة المحامين في إسرائيل

ועדת האתיקה הארצית

א. פתח דבר

1. החלטה זו מהווה גילוי דעת מקדים מטעם ועדת האתיקה הארצית באשר לחובות החלות על עורך דין ביחס לשמירת סודיות המידע המצוי בידיו בראי העידן הטכנולוגי המודרני.[1] חובת אבטחת המידע חלה על מידע סודי[2] המוחזק בידי ו/או המצוי בשליטתו האפקטיבית של עורך הדין לצורך מילוי תפקידיו.
2. ברי כי כלל 19 (חובת הסודיות) כמו גם כלל 20 (שמירת סודיות בידי העובדים) לכללי לשכת עורכי הדין (אתיקה מקצועית), תשמ"ו-1986,[3] וכללי לשכת עורכי הדין (שמירת חומר ארכיוני במשרדי עורכי דין), תשל"א-1971,[4] מקימים חובות אתיות ומשמעתיות החלות על עורך הדין בדבר שמירת סודותיו של הלקוח, וממילא מקפלים בחובם גם חובה אתית לאבטחת המידע הסודי.
3. עם זאת, התקדמות העיתים מזמנת שאלות וסוגיות רבות הנוגעות לאופן מימוש חובות אלה במרחב הדיגיטלי – בטלפון הנייד של עורך הדין, במחשבו האישי, ברשת המחשב המשמשת את פעילותו, ובשירותים מקוונים המהווים חלק מניהול משרד עורכי דין בעידן זה. הזמינות, האינטואיטיביות והפשטות בשימוש בטכנולוגיה מביאה לכך שהמשתמש בה לרוב לא נותן את הדעת לחשיפות או לסיכונים הגלומים בה. דומה כי התקפות סייבר ואירועי זליגת מידע בארץ ובעולם, ההולכים ומתגברים, מחייבים את ציבור עורכי הדין להגדיל את תשומת הלב והמשאבים לצורך אבטחת המידע הסודי ולהביאו לרמה הולמת המתחייבת על פי דין.[5]
4. המורכבות והדינאמיות בעולם הדיגיטלי מחד, ושינוי האיומים מאידך, מחייבים את ועדת האתיקה הארצית להתוות שביל אמצע באשר לאופן אבטחת המידע הסודי וקביעת סף חובה אשר אי עמידה בו יביא להפרת החובות האתיות והמשמעתיות.
5. החלטתה זו הינה פרי עבודתם של אנשי מקצוע בתחום האתיקה, הטכנולוגיה והגנת המידע, לאחר בחינה של דין משווה ממדינות שונות בעיקרם בארה"ב. הוועדה, בדומה למוסדות מקבילים בעולם, מבקשת לשרטט באמצעות החלטה זו ובאמצעות החלטות וגילויי דעת שיפורסמו מעת לעת, את אורח הפעילות הסביר וההולם הנדרש בהפעלת אמצעים טכנולוגיים על ידי עורכי הדין, תוך שמירה על גמישות טכנולוגית בכפיפה אחת עם הצורך באבטחת המידע ובעמידה בחובת הסודיות החלה על עורך הדין ביחס למידע הסודי של לקוחו.
6. חובת אבטחת המידע אינה חלה בחלל הריק, ואינה הערך היחיד עליו יש להגן. שהרי, יש לאפשר את הקדמה הטכנולוגית בתחום עריכת הדין, נוכח הצורך כמו גם החובה של עורך הדין לפעול באמצעים מתקדמים לצורך ייעול השירות, הוזלת השירות, זמינות מידע לטובת הלקוח, מתן מענה מיטבי ללקוח, שמירה בצורה מיטבית על החומרים של הלקוח, גיבוי המידע לטובת שרידותו וכדו'.
7. כך, לשם הדוגמה, מרבית משרדי עורכי הדין עובדים באופן חלקי או מלא בסביבה טכנולוגית מבוססת שירותי ענן. עם התקדמות הטכנולוגיה ויכולת הגנה מיטבית על החומרים המאוחסנים

---

[1] להלן: "**חובת אבטחת המידע**".
[2] "**מידע סודי**" – מידע שאינו פומבי, אשר הובא לעורך הדין על ידי הלקוח או מי מטעמו או על ידי צד שלישי בקשר עם לקוח, וכן, מידע שנערך על ידי עורך הדין או מי מטעמו בקשר עם או עבור הלקוח.
[3] להלן: "**כללי האתיקה**".
[4] להלן: "**כללי ארכיונים**".
[5] ראה חוק הגנת הפרטיות, התשמ"א-1981 (להלן: "**חוק הגנת הפרטיות**"); תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 (להלן: "**תקנות אבטחת מידע**").

בענן, הורחב השימוש בשירותי טכנולוגיה מבוססים ענן הן במגזר הפרטי והן במגזר הממשלתי,[6] אך טבעי שעורכי דין פרטיים ומשרדי עורכי הדין ישתמשו אף הם בשירותים מעין אלו. ואולם, גם כאשר השירותים ניתנים על ידי ספקי שירותי ענן, חלקם אף זרים, על עורך הדין לוודא את התאמת ההתקשרות, על מאפייניה החוזיים והטכנולוגיים, לחובותיו המקצועיות והאתיות.

8. אבטחת מידע הוא עולם תוכן המבוסס על ניהול סיכונים. חובותיו הנורמטיביות של עורך הדין לשמור בסודיות את המידע הסודי היא אחידה ותקפה כלפי כלל עורכי הדין. עם זאת, יישום החובה הנגזרת לאבטח את המידע איננו דומה מעורך דין אחד למשנהו, וממשרד אחד למשנהו. חובתו האתית של כל עורך דין היא לעמוד באורח מתאים והולם בהוראות הדין, על פי המדרגים השונים, בנוגע לשמירת מידע והגנת הפרטיות ובכלל זאת הוראות חוק הגנת הפרטיות ותקנותיו. אופן העמידה בחובות נגזר, בהתאם לתפיסות מקובלות של אבטחת מידע והגנת סייבר, מניהול סיכונים הנובע ממאפייני הפעילות הדיגיטלית. כך, לא דומה מעטפת אבטחת המידע הנדרשת למחשב נייד (המשמש כלי עבודה מרכזי של משרד של עורך דין יחיד), למול רשת של משרד גדול המעסיק עשרות או מאות עובדים.

9. ככלל, משרד עורכי דין גדול, בו מספר רב של "בעלי הרשאה" מסווג ברמת "אבטחה גבוהה" יותר כהגדרתם בתקנות,[7] יוצר בדרך כלל סיכון גדול יותר למתקפות סייבר או דלף מידע ובתוך כך לפגיעה אפשרית בחובת הסודיות המוטלת על עורכי דין. מכאן מצופה ממשרדים אלו ליישם רמת אבטחת מידע גבוהה ובכלל זה ליישם אמצעים ותהליכים ברמה גבוהה יותר מזו שתחול בדרך כלל על משרדי עורכי דין קטנים. מובהר כי לראיה כללית זו יש כמובן יוצאים מן הכלל ועורכי הדין מצווים תמיד להעריך נכונה את רמת הסיכון הרלבנטית לרגישות המידע הסודי ולהיערך לאבטחתו באופן הולם, ובמידת הצורך אף בעזרת אנשי המקצוע המתאימים.

10. החובות המהותיות לאבטחת המידע קבועות בחוק הגנת הפרטיות ובתקנות אבטחת המידע, המגדירים, בין היתר, את הפעולות שעל 'בעל' ו'מחזיק' מאגר לבצע. 'בעל מאגר מידע' הינו מי שאוסף ומעבד מידע אישי כחלק מפעילותו, ו-'מחזיק מאגר מידע' הינו מי שנותן לבעל המאגר שירותים הקשורים במידע האישי, ובכלל זה שירותי מחשוב. תשומת הלב תוסב לכך שלעת הזו דיני הגנת הפרטיות מחייבים את עורך הדין, בין אם היה בעל מאגר ובין מחזיק בו, ומחילים עליו חובה לרושמו או לדווח על החזקתו והכל בהתאם להוראות הדין.[8]

11. בכוונת הוועדה לקדם עבור עורכי הדין פטור מהחובה לעמוד בדרישות תקנות אבטחת המידע, זאת בהתאם לקבוע בתקנה 20 לתקנות, המקנה סמכות לרשם לפטור מאגר מסוים מהחובות הקבועות בתקנות אלו, כולן או חלקן, על פי נסיבות העניין, ובין השאר בהתחשב בגודל המאגר, סוג המידע שנמצא בו, היקף הפעילות של המאגר או מספר בעלי ההרשאות בו. בסיס אפשרי לפטור כאמור יכול להתבסס על עמידה בהוראות מסמך ייחוס או רגולציה אחרת בעניין אבטחת מידע כדוגמת מערכת נורמטיבית פנימית מוסדרת ומוסכמת אשר תוכוון באמצעות וועדה זו,[9] ואולם, עד לקבלת פטור זה, על עורכי הדין להקפיד לפעול בהתאם לדין הקיים.[10]

---

[6] לדוגמא, רשות התקשוב הממשלתי הוציאה אל הפועל מכרז מסגרת מספר 17/21 למתן שירותי ענן ציבורי, כחלק מיישום החלטה 2097 של הממשלה ה-33 "הרחבת תחומי פעילות התקשוב הממשלתי, עידוד חדשנות במגזר הציבורי וקידום המיזם הלאומי 'ישראל דיגיטלית'" (10.10.2014).

[7] כהגדרתם בתקנה 1 לתקנות אבטחת מידע.

[8] ראה לעניין זה מכתב מהרשות למשפט, טכנולוגיה ומידע במשרד המשפטים (כיום, הרשות להגנת הפרטיות), ללשכת עורכי הדין בישראל, בעניין תחולת החובות המוטלות על בעל מאגר מידע בחוק הגנת הפרטיות על עורכי דין (19.4.2009, לעיון לחץ כאן).

[9] תקנה 20(ב) לתקנות אבטחת המידע.

[10] לשלמות התמונה, הוועדה תסב את תשומת הלב להצעת חוק הגנת הפרטיות (תיקון מס' 14), התשפ"ב-2022 אשר עברה ביום 24.1.22 בקריאה ראשונה.

ב. המשמעות הנורמטיבית – החובה האתית לאבטחת המידע

וועדת האתיקה מגלה בזאת דעתה בדבר רף מינימלי של חובת אבטחת המידע. אי עמידה ברף המינימלי תשמש כחזקה לכאורה (הניתנת לסתירה), בדבר הפרת חובתו האתית של עורך הדין בקשר עם חובת הסודיות וחיסיון עו"ד/לקוח המוטלת עליו לאבטחה הולמת של המידע הסודי.

עמידה ברף המינימלי כשלעצמה תהווה תנאי חיוני אך לא בלעדי בכדי להוות ראיה לכאורה בדבר עמידת עורך הדין בחובתו. על מנת שעורך הדין ייהנה מהחזקה לתקינות פעולתו עליו להראות כי נקט באמצעי אבטחה התואמים את אופי המידע הסודי ופעילות משרדו, והכל כפי שיפורט בהרחבה בפרק ד' – המלצות הגנה (אבטחת מידע והגנת סייבר) במשרדי עורכי דין. **עמידה בהמלצות אלו תשמש כבסיס לכאורי להנחה כי עורך הדין עמד בחיוביו האתיים לאבטחת המידע אף אם יתברר בדיעבד כי המידע זלג.**

12. מערכות המחשוב המשמשות את עורך הדין בעבודתו הן בעיקר מערכות לניהול תיקי הלקוחות, לתקשורת עם לקוחות, ולכתיבה משפטית במסגרת השירותים המשפטיים. החובות המוטלות בהחלטה זו חלות על שימוש עורך הדין באמצעים טכנולוגיים באופן כללי למגוון רחב של שימושים, ולדוגמה: מחשב שולחני, מחשב נייד, מחשב לוח (tablet computer), מערכות מאגר המשמשות את המאגר ואשר יש להן חשיבות בהיבטי אבטחת מידע, מחשב שרת (server) כוננים חיצוניים ונשלפים, תשתיות מחשוב ותקשורת נוספים, תכנות ויישומים מבוססי ענן המשמשים את עורך הדין בעבודתו – לניהול ואחסון מסמכים, להעברת מסמכים, לתקשורת חיצונית ופנימית, ניהול העבודה והמשרד ועוד. החובות עוצבו כבסיס למדיניות שתהא רלוונטית לכל אמצעי טכנולוגי חדש שיתווסף בעתיד.
13. הסביבה הטכנולוגית מביאה להתייעלות עורך הדין בעבודתו, מהווה אמצעי להתמודדות עם אתגרים, ומשתנה בהתאם לצורך – כך לדוגמה משבר הקורונה שהחל בראשית 2020, הביא עמו האצה במגמת עבודה מרחוק או עבודה מהבית.
14. לצד זאת, אמצעי המחשוב (טלפונים חכמים, מחשבים נייחים וניידים ועוד) ומערכות המחשב (רשתות ושרתים) של משרדי עורכי הדין מהווים יעד לתקיפה של גורמים זדונים, הן לצרכי "כופרה" או סחיטה והן בכדי להגיע למידע רגיש של לקוחות המשרד והגברת הקישוריות מייצרת חשיפה נוספת למערכות אלו.
15. משרדי עורכי הדין מהווים יעד אטרקטיבי לתקיפה שכן על פי רוב רמת ההגנה שלהם נמוכה מאשר זו של לקוחותיהם, המידע שהם מחזיקים קל יותר לאיתור בידי תוקף, וריכוז המידע במערכות עורך הדין מאפשר איסוף מידע אודות לקוחות רבים בעת ובעונה אחת.[11] תקיפות סייבר אינן נחלתן של ארגונים גדולים בלבד. תקיפות סייבר כנגד משרדי עורכי דין בחו"ל, קטנים

[11] David G. Ries "2018 Cybersecurity" **American Bar Association Techreport** (28.1.2019) www.americanbar.org/groups/law_practice/publications/techreport/ABATECHREPORT2018/2018Cybersecurity/ ("**ABA report**").

כגדולים, הביאו להשבתת פעילותם, חשפו אותם להליכי אכיפה ולתביעות משפטיות, ויתרה מכך, הביאו לפגיעה באמון לקוחותיהם באופן העלול לאיים על המשך פעילות המשרד.[12]

16. **דרכי התמודדות עם איומי הסייבר – אבטחת מידע והגנת סייבר**

16.1. צמצום החשיפה לאיומי סייבר ושיפור המוכנות להתמודדות עם תקיפות סייבר, מבוסס על תחום אבטחת המידע והגנת הסייבר. תחום ידע זה עוסק בפעולות ההגנה הנדרשות בכדי לצמצם את החשיפה לתקיפות סייבר, וכן פעולות שיש לבצע לשם התמודדות עם התקיפה, במהלכה ולאחריה.

16.2. הגנת סייבר מורכבת מאיתור סיכוני הסייבר ונקיטת אמצעים הנדרשים לצמצום סיכונים אלה. פעולות אלו בראש ובראשונה הינן פעולות ניהוליות, שביטויין בהעלאת מודעות המשתמשים, קביעת נהלי עבודה ושימוש נכון בטכנולוגית המידע ובטכנולוגיות הגנה. עמידה בהוראות ההחלטה הינה פרקטיקה נאותה לעוסקים בעריכת דין ותשמש בסיס לכאורי להנחה כי עורך הדין עמד בחיוביו האתיים לאבטחת המידע אף אם יתברר בדיעבד כי המידע הסודי זלג.

16.3. חלק משמעותי מתקיפות הסייבר נובע מטעויות אנוש או פעולות של הונאה או שיטוי בבעלי ההרשאות הלגיטימיים למערכות, בידי התוקף. הוועדה תפנה את תשומת הלב לערכת ההדרכה הבסיסית שפורסמה על ידי מערך הסייבר הלאומי, במסגרתו מובהר מהם סיכוני הסייבר ומה תפקיד העובדים בהגנת הסייבר.[13]

16.4. עקב כך על משרד עורכי הדין לוודא קיום נוהל הכשרה ל"מודעות אבטחת מידע וסייבר" לעובדים חדשים ולריענון הנוהל לפחות אחת לשנה לעובדים וותיקים. הוראה זו תאפשר גם להעביר לעובדי משרדי עורכי הדין את חובתם בהתאם לכלל 20 לכללי לשכת עורכי הדין (אתיקה מקצועית), התשמ"ו- 1986, ובהתאם להוראת סעיף 24.10 להלן.

17. **<u>ועדת האתיקה הארצית רואה לנכון לפרסם את עמדתה המוקדמת בדבר חיוביו של עורך הדין באשר לחובותיו הכלליים לאבטחת המידע</u>**:

17.1. הוועדה שבה ומזכירה כי על עורך הדין חלה החובה לשקוד על שמירת המידע הסודי, מפני גישה לא מורשית ושימוש בלתי מורשה או בחריגה מהרשאות השימוש ומפני פגיעה בשלמות המידע הסודי בדרך של, בין היתר, אובדן המידע מבלי היכולת לשחזרו.

17.2. גישה של גורם שאינו מורשה למידע הסודי, שימוש במידע הסודי ללא רשות או בחריגה מרשות או פגיעה בשלמות המידע הסודי, תהווה הפרה אתית לכאורה של החובה האמורה, אשר ניתנת לסתירה באם יוכיח עורך הדין כי נקט באמצעים סבירים והולמים למניעת זליגת המידע ו/או חשיפת המידע בהתאם להמלצות במסמך זה.

17.3. ועדת האתיקה הארצית מגלה בזאת את דעתה כי עמידה בהוראות החלטה זו, בדגש על הוראות פרק ד' להחלטה זו, ובעדכונים שיופצו לעורכי הדין מעת לעת, תשקף התנהלות ראויה של עורך הדין בדבר אבטחת המידע הסודי, במישור האתי.

---

[12] **ABA report**, ה"ש 11.

[13] "ערכת הדרכה בנושאי איומי סייבר ואבטחת מידע" **מערך הסייבר הלאומי** (2020) www.gov.il/he/Departments/General/instructiontools.

17.4. בנוסף ומבלי לגרוע מהאמור לעיל, ועדת האתיקה הארצית תראה בעורך דין המקיים את הנחיית רשם מאגרי מידע 3/2018[14] ושהוא בעל תקן ISO 27001, המתחדש מעת לעת במידת הצורך, כמי שעל פניו נקט בפרקטיקה ראויה לאבטחת המידע הסודי.

17.5. גורמים אשר יילקחו בחשבון בקביעת סבירות מאמציו של עורך הדין כאמור, יכללו את האמצעים שנקט כדי למנוע את הגישה הלא מורשית בהתאם לעקרונות החלטה זו ובין היתר את השימוש באמצעי אבטחת מידע מקובלים וסבירים בנסיבות העניין, עלות השימוש באמצעים, מקומו של עורך הדין בהיררכית הארגון או משרד עורכי הדין בו הוא עובד, המשמעות של יישומם על מידת יכולת עורך הדין לספק את שירותיו ללקוחותיו – והכל בראי רמת הסיכון הנגזרת ממידת הרגישות של המידע הסודי והיקפו.

17.6. עורך הדין ולקוחו יוכלו לסכם בכתב את אופן אבטחת המידע הסודי המועבר לעורך הדין באופן המחמיר מהמפורט בהחלטה זו. עם זאת, במקרים נקודתיים הנוגעים לאבטחת המידע בדרכי התקשורת בין עורך הדין ללקוחו, יכולים עורך הדין והלקוח לסכם בכתב גם אופן אבטחת מידע שונה מהאמור בהנחיה זו. יובהר כי הדבר יסוכם בין הצדדים באופן נקודתי (אך לא גורף כגון בהסכם ההתקשרות), מראש ובכתב, תוך מתן גילוי נאות כלפי הלקוח לגבי נורמת אבטחת המידע הנדרשת מהחלטתנו זו ותוך פרוט מפורש בדבר אורח החריגה המוסכם, הרקע הצריך לכך, והשלכות ויתור זה. למותר לציין כי הלקוח ועורכי דינו אינם יכולים לסכם אופן אבטחת מידע סודי מופחת בכל הנוגע לצדדים שלישיים. אין בהוראה זו כדי לגרוע מחובותיו של עורך הדין בהיבטי אבטחת מידע לפי דין.

17.7. עורך הדין יעשה שימוש באמצעיים טכנולוגיים שונים בהתאם למידת רגישות החומרים ומידת ההשפעה על הלקוח במידה ויחשפו. על עורך הדין להתעדכן מעת לעת בהתקדמות הטכנולוגיה בקשר עם הגנת המידע, ולוודא כי המערכות בהן משתמש יהיו מעודכנות דיו על מנת להגן על המידע הסודי ולהתגונן מפני אירועי סייבר.

17.8. לצד החובה לאבטח את המידע הסודי כשהוא שמור ונעשה בו שימוש באמצעי טכנולוגיות מידע, על עורך הדין גם לוודא נקיטת אמצעים לצורך האבטחה הפיזית של המידע הסודי ובכלל זה נקיטת אמצעים הולמים לאבטחת סביבת העבודה, הן במשרד והן מחוצה לו (לשם הדוגמה מחשבים ניידים) ובפרט מקום בו חלק ניכר מהעובדים עובדים מרחוק ומתחברים למערכות המשרד מרשת שאינה הרשת המשרדית.

17.9. הנחת העבודה הינה כי עורך הדין הינו מומחה למקצוע המשפטי. האחריות הכוללת הנובעת מהוראות הסודיות מחייבת לצד אחריות ניהולית והדרכות עובדים גם מימוש האמור במערכות הטכנולוגיות ובמערכות ההגנה. המשמעות הינה כי ככל ולעורך הדין אין את הידע והגישה הנדרשים, עליו להיוועץ באיש מקצוע לצורך אבטחת המידע הסודי המצוי במערכותיו בהתאם להנחיות החלטה זו.

---

[14] הנחיה 03/2018 של רשם מאגרי מידע "תחולת תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017 על ארגונים המוסמכים לתקן ISO/IEC 27001" (26.4.2018,להלן: "**הנחיית הרשם 03/2018**").

17.10. ועדת האתיקה הארצית מסבה את תשומת הלב של עורכי הדין להם מאגרי מידע ברמת אבטחה בינונית או גבוהה, כי חלה עליהם חובת דיווח לרשות להגנת הפרטיות במקרה בו התרחש במשרדם אירוע אבטחה חמור[15] והכל בהתאם לתקנות אבטחת מידע.[16]

17.11. בנוסף, ועדת האתיקה הארצית מגלה בזאת דעתה כי חלה על כל עורך דין חובה לעדכן את הלקוח נוכח גילוי פרצת אבטחה למידע סודי הקשור לייצוג הלקוח. יידוע כאמור יעשה מקום בו פרצת האבטחה עלולה לפגום בסודיות המידע של הלקוח, ואשר קיים חשד סביר כי נתונים אלו נחשפו או אבדו או הושמדו וכן מקום בו פרצת האבטחה פוגעת באופן מהותי ביכולת עורך הדין לבצע את השירותים המשפטיים עבורם נשכר.

17.12. חובת היידוע ללקוח כאמור בסעיף 17.11 לעיל, תכלול את הפרטים אודות האירוע וכן את הפעולות המבוצעות או שבוצעו על ידי עורך הדין או מי מטעמו כדי להכיל את האירוע (Containment), להקטין את הנזק שנגרם או העלול להיגרם כתוצאה ממנו (Mitigation) ולתיקון ולהשבת הפעילות לסדרה (Remediation).

17.13. משרדי עורכי דין יטמיעו במשרדם נוהל אבטחת מידע בהתאם לתקנות אבטחת המידע, ונוהל התמודדות עם אירועי אבטחת מידע ומתקפות סייבר.

17.14. **<u>התקשרות עם ספקי מיקור חוץ בתחום שירותי טכנולוגיה</u>**:

17.14.1. משרדי עורכי דין רוכשים שירותים שונים שיש להם נגיעה למערכות המידע או לתהליכי העבודה המשלבים מידע של המשרד. נגישות זו מייצרת סיכונים חיצוניים לאבטחת המידע הידועים כ-"סיכוני שרשרת אספקה".[17]

17.14.2. לצורך התמודדות עם סיכון זה על המשרד לבחון את מהימנות הספקים, ולוודא כי הבטיח בחוזה השירות את קיום החובות החלות על המשרד גם לגבי הספק. יש להדגיש את חשיבות קביעת תניות חוזיות מתאימות העוסקות בהגנת סייבר, ולוודא כי כלל הספקים עומדים בהתחייבויות שניתנו מצדם.

17.14.3. ככלל, עורך הדין ימנע מלנהל מידע סודי על גבי שירותים חינמיים, זאת אלא אם עורך הדין בדק ווידא שהספק החינמי עומד באופן מלא ומיטבי בדרישות אבטחת מידע בהתאם להחלטה זו.

מובהר כי חזקה היא שספק שירותי טכנולוגיה חינמי, החשוף למידע סודי, אינו עומד בדרישות אבטחת המידע הנדרשות. על עורך הדין המשתמש בשירות החינמי יוטל העול בהפרכת החזקה.

17.14.4. על עורך דין המבקש להשתמש באמצעי טכנולוגי כלשהו לבצע בדיקות רקע הולמות כדי לוודא שלספק של אמצעי השירות יש מוניטין הולם בתחום אבטחת המידע (לדוגמה, שהספק לא נתבע בתביעה הנוגעת לכשל באבטחת המידע על ידו ולא בוצעה כנגדו פעולת אכיפה של רשות להגנת מידע אישי בקשר עם הפרות הנוגעות לעיבוד או להחזקת מידע).

17.14.5. עורך הדין יבחן את אמצעי ומדיניות אבטחת המידע של הספק (לדוגמה ביקורות אבטחת המידע שהספק מבצע בעצמו), גיבוי המידע הסודי, שחזור נתונים ומידע במידת הצורך, ניהול ההרשאות והגישה לנתונים, יכולת גורמים

---

[15] "**מאגר מידע שחלה עליו רמת אבטחה בינונית**"; "**מאגר מידע שחלה עליו רמת אבטחה גבוהה**"; "**אירוע אבטחה חמור**" – כהגדרתם בתקנה 1 לתקנות אבטחת מידע.

[16] תקנה 11(ד) לתקנות אבטחת מידע.

[17] "תקיפת ארגונים באמצעות שרשרת אספקה" מערך הסייבר הלאומי (11.3.2020) www.gov.il/he/Departments/publications/reports/supply-chain.

שלישיים לצפות ו/או לגשת למידע הסודי וכדו'. עורך הדין יוודא כי מדיניות אבטחת המידע ואמצעי אבטחת המידע של הספק תואמת בנסיבות העניין לחובת אבטחת המידע הסודי המוטלת על עורך הדין.

17.14.6. מקום בו המידע הסודי נשמר על ידי הספק, יבהיר האחרון את מיקום השרתים בהם נשמר המידע. במידת הצורך, עורך הדין יוודא כי תקנות העברת מידע מחוץ לגבולות המדינה מתקיימות,[18] כמו גם הנחיות וגילויי הדעת של הדעת של הרשות להגנת הפרטיות בעניין זה.[19]

17.14.7. בהסכם ההתקשרות מול ספק שירותי טכנולוגיה יובהר מפורשות כדלקמן:

17.14.7.1. המידע והנתונים המועברים ו/או הנשמרים ו/או המוצגים באמצעות מערכת הספק אינם קניינו, ואין לו כל זכות לצפות בהם ו/או להשתמש בהם שלא לצורך התקשרות זו עם עורך הדין;

17.14.7.2. ספק השירותים מנוע משימוש במידע הסודי לצורך פרסום ו/או טיוב נתונים ו/או כל שימוש אחר שאינו לצורך מתן השירותים לעורך הדין והוא בלבד;

17.14.7.3. ספק השירותים מנוע מהעברת המידע הסודי לצד ג' כלשהו, וזאת למעט לספק שירותי משנה מטעמו לצורך מתן השירותים לעורך הדין ולו בלבד, המחויב להתחייבויות המנויות בסעיף זה;

17.14.7.4. הספק מאבטח את המידע בהתאם לסטנדרטים מקובלים והולמים את רמת הרגישות של המידע הסודי;

17.14.7.5. הספק מספק גיבוי למידע באופן המנותק מסביבת המידע העיקרית, שתאפשר שחזור של המידע הסודי, המידע בסביבת המידע העיקרית ניזוק, הושמד או הוצפן במתקפת כופר;

17.14.7.6. הספק ידווח לעורך הדין באופן מידי על כל אירוע אבטחה שפגע או עלול לפגוע במידע הסודי ועל כל הליך משפטי שהספק מעורב בו ושעלול להשפיע על המידע הסודי;

17.14.7.7. כי הספק ימחק את המידע הסודי בתום ההתקשרות, אך לא לפני שיאפשר לעורך הדין להעתיק או לנייד את המידע הסודי;

17.14.7.8. הספק יאפשר לעורך הדין לנייד את המידע בצורה ישימה וללא צורך בהשקעת משאבים משמעותיים, מהספק לספק אחר;

17.14.7.9. הספק יתחייב לסודיות מול עורך הדין באופן אשר יחייב אותו ואת עובדיו;

17.14.7.10. הספק איננו פוטר את עצמו מכל אחריות בקשר עם פגיעה בסודיות ואבטחת המידע הסודי;

17.14.7.11. הספק יודיע לעורך הדין באופן מידי בכל מקום בו מוגשת בקשה ו/או תביעה בקשר עם המידע הסודי.

---

[18] תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001.

[19] במועד עריכת החלטה זו תלויה ועומדת להערות הציבור טיוטת גילוי דעת של הרשות להגנת הפרטיות בנושא פרשנות תקנה 3 לתקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001. וכן ראו גילוי דעת בעניין העברת מידע אישי מישראל לארצות הברית בעקבות פסק הדין של בית המשפט האירופי לצדק בפרשת שרמס 2 https://www.gov.il/he/departments/news/privacy-shrems2-usa.

17.14.8. מבלי לגרוע בכל האמור לעיל, חזקה היא שספק בעל תקן ISO 27001 בתוקף (ואם הוא ספק ישראלי –הוא מצהיר גם על עמידה בהוראות הנחיית רשם מאגרי המידע 3/2018) או ספק בעל דו"ח בקורת SOC2 Type 2 עדכני, בהתאם לתקן SSAE18, הרשום במאגר הספקים המאושרים המפורסם על ידי מערך הסייבר הלאומי, ככל שזה יקים מאגר ספקים זה, עומד בדרישות אבטחת המידע להתקשרות עמו.

על אף האמור, מידע סודי בעל רגישות מיוחדת עשוי לחייב בתקני אבטחה נוספים, כדוגמת ISO 27799 כאשר המידע הסודי כולל מידע רפואי.

17.14.9. מבלי לגרוע מכל האמור לעיל חזקה היא שספק הנותן שירותי ענן ואשר הינו בעל תקן ISO 27017/8 לניהול אבטחת ענן תקף ומקיים את הוראותיו, עומד בהוראות החלטה זו בעניין אבטחת המידע ושמירת הסוד הדרושים להתקשרות עמו.

17.14.10. ועדת האתיקה הארצית ומערך הסייבר הלאומי יפרסמו רשימת ספקי תוכנות או ספקים בעלי גישה למידע של עורכי דין, אשר נבדקו ואושרו על ידו בהתאם לאמור בסעיף 17.14.8 לעיל. בדיקה כאמור תיעשה לספק ולא לשירות קונקרטי.

ג. <u>החובות בסיסיות המוטלות על עורך הדין בקשר עם אבטחת המידע</u>

18. ועדת האתיקה הארצית מגלה בזאת דעתה מראש כי על עורך דין המחזיק בידו מידע של לקוח, אף באם מדובר במידע מצומצם שאינו כולל מידע בעל רגישות יתרה, לנהל בצורה מסודרת את השימוש במערכות מידע ותקשורת.

כך, עורך הדין יגבש לעצמו רשימה ובה תיאור כללי של מערכות המידע בשימוש המשרד, ובכלל זה מחשבים, שרתים, שירותים במיקור חוץ, שירותי ענן, שימוש במכשירים ניידים, והתוכנות השונות המשמשות את המשרד. כל אלה הם "נכסים טכנולוגיים" אשר מחזיקים בנכסי המידע של המשרד.

19. על מנת לסייע לעורכי הדין בדבר הטמעת כלל החובות האתיות החלות עליהם בקשר עם אבטחת המידע, ועדת האתיקה הארצית ניסחה שאלון עזר פנימי עבור עורכי הדין בדבר **תבנית מדיניות הגנת סייבר**. שאלון זה יהווה כלי עזר למשרד עורכי הדין ולגורמי אבטחת המידע מטעמו בזיהוי המערכות והמידע הסודי הנדרשים באבטחת המידע. שאלון זה מצורף **כנספח ב'** להחלטה זו.

20. על הנהלת המשרד לוודא כי עובדי המשרד מכירים את סוג איומי הסייבר להם חשוף המשרד, ואת נהלי העבודה אשר נועדו להתמודד עם איומים אלה. במסגרת זאת יש לעדכן את העובדים על אמצעי ההגנה והניטור, ולבצע ריענונים תקופתיים.

21. **חשוב להדגיש כי למרות שאבטחת מידע מגנה על טכנולוגיה, חלק משמעותי בקידום ההגנה, מבוסס על פעולות שאינן טכנולוגיות במהותן, אלא ניהוליות הכרוכות בין היתר בהתנהלות אישית קפדנית.** כפועל יוצא מהחלטות מדיניות אלה, נגזרים התהליכים הטכנולוגיים השוטפים בארגון והגדרות אופן השימוש של הארגון בטכנולוגית ייעודיות לאבטחת מידע.

22. מימוש האחריות בא לידי ביטוי בשילוב של אמצעים נהליים וכלים טכנולוגים, המבוססים על היכרות של ההנהלה והעובדים את הנכסים החשובים ואופן ההגנה עליהם. היא מסייעת לצמצם

את סיכוני הסייבר ולהגן על המידע החסוי של הלקוחות, פרטיות העובדים והרציפות התפקודית של המשרד.

23. על משרד עורכי הדין לנהל בצורה מסודרת את השימוש במערכות מידע ותקשורת, באופן הכולל את ההיבטים הבאים:

23.1. תיאור כללי של מערכות המידע בשימוש המשרד, ובכלל זה מחשבים, שרתים, שירותים במיקור חוץ, שירותי ענן, שימוש במכשירים ניידים, והתוכנות השונות המשמשות את המשרד. כל אלה הם "נכסים טכנולוגיים" אשר מחזיקים בנכסי המידע של המשרד.

23.2. להגדיר את היעדים להגנה, ואת תרחישי הסיכון האפשריים, הנובעים מאופי השירותים המשפטיים שמעניק המשרד והמידע הנשמר במערכותיו.

23.3. קביעת מדיניות הגנת סייבר שממנה נגזרים כללי התנהגות המחייבים את העובדים יש לבחון עדכניות מדיניות זו מעת לעת בהתאם לשינוי באתגרי הסייבר שבה ויכולת המשרד להתמודד מול אלה.

23.4. יש ליישם דרישות אלה גם בהתקשרויות של המשרד עם ספקים בתחום המחשוב או הגישה למידע של המשרד.

23.5. נדרש להקצות את המשאבים הנדרשים להיבטים אלה, ולבצע בקרה תקופתית.

24. לצורך מימוש המדיניות, על עורך הדין להחזיק, ולו באורח מינימאלי, את המערכות הבאות (להלן: "**המערכות הבסיסיות**"):[20]

	נושא	תיאור
.1	הגנה רציפה על הרשת הארגונית (ככל שעורך הדין מחזיק רשת כזו) כולל: 1. FireWall 2. Antivirus &Anti malware	התקנת פיירוול דור חדש Next FW Generation (NGFW) של אחד מ 5 היצרנים המובילים בעולם. התקנה בתצורה שירות מנוהל (למעט אם עורך עובד באופן יחידני ללא צוות עורכי דין ועובדים אחרים).
.2	הגנה על ערוץ הדוא"ל	שירות מנוהל כחלק מחבילת ה NGFW ספאם ופישינג Anti-spam
.3	הגנה על ערוץ הגלישה לאינטרנט WEB	שירות מנוהל כחלק מחבילת ה NGFW למניעת גלישה לאתרים זדוניים
.4	הגנה על שירות ה WiFi של המשרד ואבטחת רשת ה – WiFi באמצעות סיסמה חזקה.	שירות מנוהל כחלק מחבילת ה NGFW
.5	הגנה על הגישה מרחוק לארגון באמצעות תקשורת מוצפנת ואבטחת גישה באמצעות הזדהות דו-שלבית	שירות מנוהל כחלק מחבילת ה NGFW

[20] עמידה בהוראות פרק זה ופעולה בהתאם לתבנית המערכות הבסיסיות תאפשר עמידה בהוראות תקנה 2, 4, ו- 13(א) לתקנות אבטחת מידע.

.6	הגנה על תחנות הקצה (מחשבים ניידים, נייחים, שרתים)	מלבד גרסאת AV גם שירות EDR מנוהל ע״י ספק התקשורת או ה HOSTING
.7	שירות גיבויים מנוהל	שירות גיבויים אוטומטי מנוהל ע״י ספק התקשורת או ה HOSTING

24.1. תכנות המחשב המצויות בשימוש עורך הדין יהיו תכנות ברישיון, חוקיות ועדכניות.

24.2. עורך הדין יהא בעל רישיון בתשלום, חוקי ועדכני, של מערכת הפעלה למחשב מוכרת וידועה. על עורך הדין לוודא עדכון שוטף של מערכת ההפעלה.

24.3. עורך הדין יהא בעל רישיון בתשלום, חוקי ועדכני, של מערכת אנטי וירוס (Anti-virus/malware) מוכרת וידועה, הנתמכת בידי היצרן. על עורך הדין לוודא עדכון שוטף של המערכת.

24.4. עורך הדין יהא בעל רישיון בתשלום, חוקי ועדכני, של מערכת EDR ו/או XDR מוכרת וידועה, הנתמכת בידי היצרן. על עורך הדין לוודא עדכון שוטף של המערכת.

24.5. עורך הדין יהא בעל רישיון בתשלום, חוקי ועדכני, לשרתי דואר אלקטרוני מאובטח כראוי. ועדת האתיקה הארצית תראה בעורך הדין המשתמש לקבלת ושליחת מידע של לקוחות בשרת דואר חינמי כמי שלכאורה מפר את חובת אבטחת המידע כאמור בסעיף 17.14.3 לעיל.

24.6. על עורך הדין לאבטח את הליך הכניסה מרחוק לאמצעים הטכנולוגיים באמצעות שימוש באמצעים מקובלים ועדכניים לאבטחה דוגמת אימות דו שלבי.[21]

24.7. על עורך הדין חלה החובה לאבטח את הליך הכניסה לאמצעים הטכנולוגיים בסיסמאות מורכבות שלא יתגלו בנקל.[22]

24.8. עורך הדין יהא בעל מערכת לגיבוי נתונים מאת ספק מוכר וידוע.

24.9. על עורך הדין לוודא כי אמצעי התקשורת החזותית בה הוא עושה שימוש הן כמארגן הישיבה והן כמשתתף בה, אינו מותיר גישה לצד שלישי ללא אישור מארגן הישיבה, וכן אינו נצפה ו/או מוקלט ו/או מוסרט בידי צדי שלישי בלא ידיעת המשתתפים בישיבה.

24.10. עורך הדין ישתתף בהדרכה בנושא אבטחת מידע וחשיבותו וזאת במהלך שנת 2022. לאחר מכן עורך הדין ישתתף מעת לעת בהדרכות עדכניות בנושא זה ולפחות אחת לשנתיים. הדרכות כאמור יכול ויעשו תוך השתתפות מומחי אבטחת מידע וזאת באופן פרטני, ויכול ויעשו באמצעות השתלמויות שתבצע לשכת עורכי הדין או על ידי מי מטעמה.

25. עורך הדין שלא מחזיק במערכות הבסיסיות המפורטות בטבלה לעיל, יוחזק כמי שלכאורה אינו מקיים את חיוביו בקשר עם שמירת הסודיות ואבטחת המידע הסודי.

[21] ראה לעניין זה פרק ד(5).3 בהחלטה זו.
[22] ראה לעניין זה פרק ד(5).2 בהחלטה זו.

ד. המלצות ההגנה (אבטחת מידע והגנת סייבר) – משרדי עורכי דין[23]

26. פרק זה סוקר את תחום אבטחת המידע והגנת הסייבר באופן שמיועד למי שאינם אנשי מקצוע בתחום הגנת הסייבר.
27. הגנת סייבר מורכבת מאיתור סיכוני הסייבר ונקיטת אמצעים נדרשים לצמצום סיכונים אלה. פעולות אלה הינן קודם כל פעולות ניהוליות, אשר ביטוין הינו בהעלאת מודעות המשתמשים, קביעת נהלי עבודה, ושימוש נכון בטכנולוגית המידע ובטכנולוגיות הגנה.
28. תחום אבטחת המידע והגנת הסייבר מבוסס על ניהול סיכונים, המכתיבים קביעת תהליכי עבודה שנועדו להתמודד איתם, הדרכה והטמעה, ושימוש נכון ומאובטח בטכנולוגיה ובטכנולוגיות הגנת סייבר. בעידן הסייבר נדרשת תפיסת ניהול סיכונים רחבה, באופן שלצד קיום עקרונות אבטחת המידע המקובלים, נדרש גם ניטור רציף ומעמיק יותר של מערכות המידע. זאת, כדי לאפשר איתור חשד לתקיפת סייבר מוקדם ככל האפשר, זיהוי התקיפה, מניעתה במידת האפשר, הכלתה במידת הצורך וקביעת דרכי התמודדות עמה, ולאפשר להנהלת הארגון תמונת מצב רציפה על אודות תפקוד המערכות הנדרשות לפעילות הארגון.
29. השקעה נאותה ותשומת לב ניהולית ממוקדת באמצעים לאבטחת מערכות המידע והתקשורת הארגונית יכולה להפחית במידה רבה מאוד את החשיפה לתקיפות סייבר, לקצר את זמן ומורכבות הטיפול בעת שקורית תקיפה, ולסייע בהתאוששות לאחריה.
30. בהתאם לכך, מסמך זה נועד לסייע לעורכי הדין לממש את אחריותם ולהתוות את ההחלטות הנדרשות בממשל טכנולוגית המידע והסיכונים, ובהתאמה להן, את הכלים והשירותים הטכנולוגים הנדרשים ליישום ההחלטות.[24]
31. המלצות אלו עשויות לסייע בקיום החובות החלות על מי שמעבד ומחזיק מידע אישי לפי תקנות אבטחת מידע. עם זאת, הן נועדו לצמצם את הסיכונים לכלל פעילות המשרד (ולא רק מידע אישי) במרחב הדיגיטלי.

ד(1). היבטים מתקדמים של ממשל ניהול סיכוני סייבר

32. הרשות להגנת הפרטיות במשרד המשפטים, קבעה בהנחיה 03/2018[25] כי עמידה בהוראות תקן אבטחת המידע ISO 27001 ואחיזה בתעודת הסמכה לתקן, בנוסף למספר תקנות ספציפיות מאפשרת למשרד לוודא כי הוא נוקט אמצעים סבירים ומקובלים להגן על עצמו. קבלת הסמכה לתקן, מהווה אישור חיצוני המאפשר להציג גם לצדדים שלישים כי המשרד עומד בדרישות הגנה מקובלות.
33. בלי לגרוע מהאמור בסעיף 17 ב בחוק הגנת הפרטיות המפרט את הגופים החייבים עפ"י חוק במינוי ממונה אבטחת מידע, הוועדה סבורה כי מינוי "נאמן אבטחת מידע" במשרד, מסייע בדרך כלל לריכוז הידע והאחריות להיבטים השוטפים של תחום אבטחת המידע, ומייעל את הממשק

---

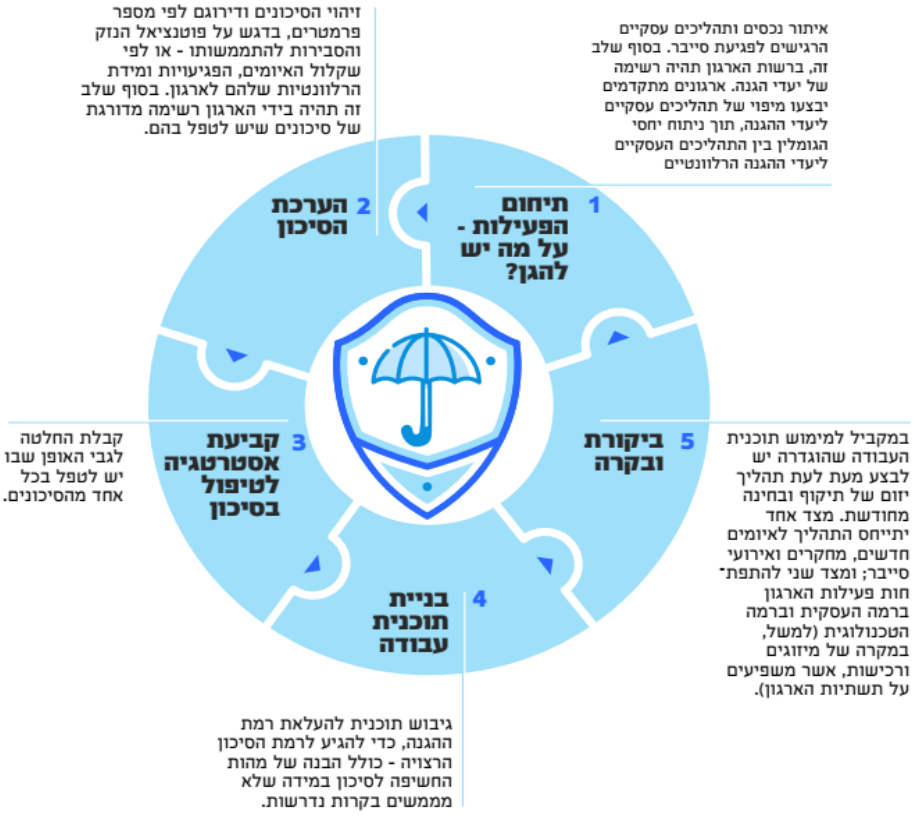
[23] **פרק זה נכתב בשיתוף פעולה עם מערך הסייבר הלאומי**, תוך שימוש במסמך תורת ההגנה 2.0, המלצות המערך בנושא "עסקים קטנים","גיבויים", "הדרכות עובדים", "הזדהות", וכן, המלצות רשות הסייבר הבריטית לעסקים קטנים.

[24] המסמך עוסק בהמלצות שחלקן נוגע במיוחד לעורכי דין שהם בעלי המשרד בו הם פועלים ואשר עליהם החובה הישירה להעמיד מערכת מאובטחת לשימושם ולשימוש עובדיהם. באשר לעורכי דין שכירים ברי כי יחולו עליהם בעיקר החובות החלות על עובדים או מורשי גישה למערכות.
לעניין עורכי דין שהם שכירים בלשכה משפטית של ארגון, הלקוח המרכזי שלהם ובעל הסודיות (הארגון) הינו לרוב גם מי שמספק להם את משאבי המחשוב. במצב דברים זה על הארגון לעמוד מחד בהוראות הדין החלות עליו ומאידך עליו לספק לעורך הדין סביבת עבודה בו יוכל עובדו לעמוד בחיוביו האתיים.

[25] הנחיית רשם מאגרי המידע מס' 03/2018 תחולת תקנות הגנת הפרטיות (אבטחת מידע) התשע"ז-2017 2 על ארגונים המוסמכים לתקן ISO/IEC 27001.

לגורמי המקצוע השונים. מינוי ממונה אבטחת מידע, במשרה מלאה, חלקית או נוסף על תפקיד, מהווה אמצעי נוסף המאפשר לשפר את רמת ההגנה במשרד עקב היכרות של גורם קבוע עם המאפיינים של פעילות המשרד, הסיכונים הכרוכים בפעילותו, והתאמה של מעטפת ההגנה לפעילותו ועדכונה לפי הצורך. לעניין זה תפנה הוועדה להמלצות הרשות להגנת הפרטיות בעניין מינוי ממונה הגנה על הפרטיות בארגון ותפקידיו.[26]

34. מומלץ לקיים לפחות אחת לשנה ביקורת של גורם חיצוני על מצב סיכוני הסייבר של המשרד על נכסי המידע ומערכות המידע שלו.
35. מומלץ להתקשר עם גורם מקצועי מתאים בתחום טיפול באירועי סייבר אשר יתמוך במשרד במקרה של אירוע סייבר ויפעל על פי נוהל תגובה לאירועים שמתאים למשרד.
36. למשרדים גדולים[27] מומלץ לקיים מעת לעת תרגול לעובדים ולהנהלה.
37. מומלץ להירשם לעדכוני אבטחה של מערך הסייבר הלאומי, באמצעות אגף ה- CERT הלאומי. מומלץ לתעד ולדווח למוקד מערך הסייבר הלאומי בטלפון ***119** על כל חשד לאירוע סייבר או אירוע שקרה בסמיכות הקרובה ביותר לאירוע עצמו. הדיווח מאפשר למערך לאתר מגמות תקיפה במשק, ולסייע למשרד ולארגונים אחרים בהתגוננות בפני אותה תקיפה.
38. זאת, מבלי לגרוע כמובן מהחובה למסור דיווח לרשות להגנת הפרטיות **על כל אירוע אבטחת מידע חמור**, כמתחייב מתקנה 11(ד) לתקנות אבטחת מידע.[28]



[תרשים מספר 1 – מחזור הטיפול בסיכונים בתחום הגנת הסייבר – מנקודת המבט של ההנהלה][29]

---

[26] "מינוי ממונה הגנה על הפרטיות בארגון ותפקידיו" הרשות להגנת הפרטיות, משרד המשפטים (24.1.2022). https://www.gov.il/BlobFolder/reports/dpo_doc_kit/he/dpo_doc.pdf .

[27] בהתאם לאמור בסעיפים 8-9 להחלטה זו.

[28] ראו סעיף 17.10 להחלטה זו, וכן להלן טופס דיווח על אירוע אבטחת מידע חמור באתר הרשות להגנת הפרטיות: https://formspdf.justice.gov.il/PrivacyProtectionAuthority/ReportingSecurityIncident.aspx

[29] מקור: מערך הסייבר הלאומי, תורת ההגנה 2.0.

ד(2). מחשבים ותוכנות – שימוש בתוכנות ברישוי ומניעת סיכונים הנובעים מחולשות[30]

39. תקיפות סייבר רבות מנצלות "חולשות" בתוכנות. חולשות הן "באגים" בתוכנה המאפשרים שימוש לרעה בידי תוקפים. עקב כך, טיפול בחולשה מסייע מאוד להפחתת החשיפה של המשרד.
40. **על משרד עורכי הדין לנקוט אמצעים סבירים לוודא כי התוכנות בשימושו מעודכנות ומקבלות עדכוני אבטחה שוטפים. הדבר נדרש לכלל התוכנות שבשימוש המשרד.**
41. לצורך כך יש חשיבות לשימוש בתוכנות שרישיון השימוש בהן בתוקף. החשיבות של תוכנות ברישוי היא שהן מקבלות עדכוני אבטחה באופן שוטף. תוכנות ללא רישוי (או "פרוצות") אינן מקבלות עדכונים בכלל ועדכוני אבטחה בפרט. בתוכנות בהן יש אפשרות כזו, יש לקבוע "עדכוני אבטחה אוטומטיים".
42. על אנשי המחשוב וספקי התקשורת של המשרד להגדיר בכל התוכנות המותקנות על כלל אמצעי המחשוב "עדכוני תוכנה אוטומטיים". הדבר קריטי במיוחד במערכת ההפעלה ובתוכנות שנעשה בהן שימוש רב (כדוגמת Windows Update). עדכוני תוכנה מצמצמים את קיומן של חולשות מוכרות, וכתוצאה מכך את החשיפה לשימוש לרעה בידי תוקפים. עדכונים נדרשים גם במכשירים ניידים ובאפליקציות המותקנות עליהם. נדרש כי המערכות יאספו לוגים על פעולתם באופן שוטף על מנת לאפשר איתור פעילות חריגה או תחקורה בעקבות אירוע.

ד(3). שימוש באמצעים טכנולוגים מקובלים להגנה על מחשבים, מכשירים ניידים ושרתים – אנטי וירוס, EDR, XDR

43. יש להגן על מחשבי המשרד (תחנות קצה – המצויות בשימוש עובד, ושרתים – המהווים את ליבת הרשת הארגונית) באמצעות תוכנות אנטי-וירוס (AV) עדכניות של יצרנים מוכרים ומובילים. יש להגן גם על מכשירים ניידים בתוכנות אנטי-וירוס. תוכנת אנטי-וירוס מגנה בכך שהיא מאתרת באמצעות "חתימות"[31] ידועות מראש פוגענים המגיעים אל המחשב. בכך יתרונה של תוכנת ה-AV, אך בכך גם חסרונה – היא אינה יודעת להגן בפני איומים חדשים שטרם "נחתמו".
44. **יש לוודא שתוכנת אנטי-וירוס תהיה מותקנת על כל המחשבים במשרד, כולל כל המחשבים הניידים, על הנייחים, על השרתים, ושהתוכנה תתעדכן (בחתימות) בתדירות גבוהה (לפחות פעם ביום).**

ד(3).1. שימוש באמצעים טכנולוגים מקובלים להגנה על טלפוניים ניידים

45. יש להגן על טלפוניים ניידים באמצעות תוכנות אנטי-וירוס עדכניות של יצרנים מוכרים ומובילים ולוודא כי הגישה למידע על גבי המכשיר הנייד תהיה מוגבלת רק לבעלי הרשאה, על ידי נעילת הטלפון בסיסמא חזקה. כמו כן, יש לבחון שימוש במערכת MDM או מקבילה אליה לשם אכיפת מדיניות אבטחה מרכזית, הכוללת לכל הפחות:
    45.1. הצפנת מידע ארגוני המאוחסן במנוחה ובתנועה.
    45.2. חיוב השלמת תהליך הזדהות מוצלח בטרם מתן גישה למידע.
    45.3. יכולת מחיקה מרחוק במקרה של אובדן או גניבת מכשיר הטלפון (Remote Wipe).

---

[30] עמידה בפרק זה תהווה סיוע לעמידה בהוראות תקנה 13 לתקנות אבטחת מידע.
[31] "חתימה" היא "טביעת אצבע דיגיטלית" ייחודית וחד ערכית של קובץ, והיא מאפשרת סימון ואיתור קבצים באופן מהיר.

46. תפיסת אבטחה מתקדמת יותר מחייבת ניטור הגנתי אקטיבי יותר מאשר זה המבוצע בידי אנטי-וירוס. ניטור הגנתי זה מאפשר לאתר תהליכים חריגים במחשב, עוד בטרם הם מזוהים ונחתמים כפעילות חריגה. לכן המלצה מקובלת היא לא להסתפק בתוכנת אנטי-וירוס פשוטה שרמת ההגנה שלה מפני תקיפות מתקדמות עלולה שלא להיות מספקת. בהתאם לכך מומלץ לדרוש התקנה של תוכנה מתקדמת להגנה על תחנות קצה מסוג **EDR** ("Endpoint Detection and Response") או לרכוש שירות מנוהל כזה. תוכנות ה EDR המובילות מספקות הגנה טובה יותר גם עבור מתקפות כופרה מתקדמות הנפוצות כיום בארץ ובעולם.

ד(4). <u>הגנה על הגישה לרשת המשרד</u>

47. הגישה של עובדי המשרד, ספקיו ולקוחותיו לרשת הארגונית ולשירותי הענן היא קריטית במיוחד בעת שימוש גובר בחיבור מרחוק.

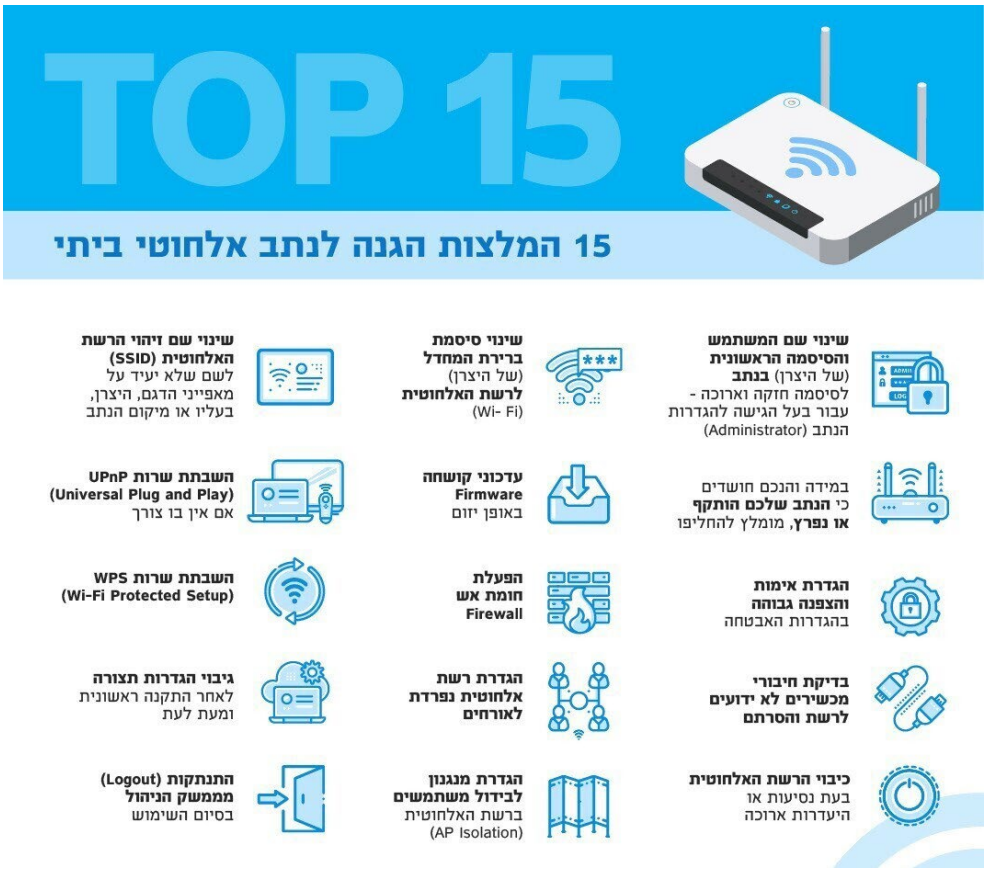
ד(4).1. <u>הגנה על הרשת הארגונית</u>

48. על המשרד לוודא כי הרשת הארגונית מוגנת באמצעות רכיב Firewall דור חדש ("Next Generation FW") עדכני של יצרן מוכר ומוביל. יש לוודא כי איש מקצוע בעל מומחיות מתאימה התקין והגדיר אופן פעולת הרכיב בהתאם להמלצות היצרן ו- "הקשיח" את התצורה באופן שמצמצם את החשיפה של הקישוריות של הרשת הארגונית למינימום הנדרש לתפעול המשרד. רצוי לדרוש שה Firewall כולל גם תכונות סינון וחסימה (IPS ואנטי-בוט) עם יכולת עדכון חתימות ב on-line מהיצרן. ניטור סייבר רציף ושמירה על רשומות אבטחה מסייע באיתור מוקדם של פעילות חריגה ובהתמודדות איתה. אם הרשת הארגונית משרתת מספר משרדים, יש לוודא הפרדה ומידור בין הנכסים הדיגיטליים הזמינים לכל אחד מהם על פי הרשאותיו.
רכיבים אלה והתקנתם מסופקים גם כשירות בידי ספק התקשורת או חברת שירותי האירוח של המשרד.

ד(4).2. <u>הגנה על הרשת האלחוטית</u>[32]

49. במידה שהמשרד עושה שימוש ברשת אלחוטית יש להבחין בין נקודת WIFI שמטרתה אפשרות גלישה באינטרנט בלבד, לבין נקודת WIFI שמטרתה חיבור אלחוטי לרשת המשרד.
50. באופן כללי, יש לוודא ששירותי ה WIFI במשרד מאובטחים בצורה המיטבית ומוצפנים וששונו סיסמאות ברירת המחדל של היצרן. כמו כן במידה שהמשרד מעוניין לאפשר לעובדי גישה אלחוטית לרשת המשרד, יש להגדיר רשתות אלחוטיות נפרדות לעובדים ולאורחים בעלי הרשאות גישה שונות וסיסמאות שונות. ניתן לקבל שירות זה מספק התקשורת. (במקרים רבים נתב ה-WIFI נכלל ביחידת הפיירוול ומאפשר חיבור מאובטח). כמו כן, יש לוודא בעת התקנת ציוד האלחוט כי השידור אינו חוצה את גבולות המשרד הפיזיים, כך שלתוקף יהיה קשה לקבל נגישות לרשת זו מרחוק. ניתן לבקש סיוע מספק התקשרות לשם וידוא עמידה בהמלצה זו.

[32] עמידה בהוראות פרק זה תהווה סיוע לעמידה בתקנה 14 לתקנת אבטחת המידע.



[תרשים מספר 2 – המלצות להגנה על נתב אלחוטי WIFI][33]

ד(5). הגנה על המידע

51. על המשרד להגן על הגישה למידע ומערכות המחשוב וכן על המידע עצמו מפני גישה לא מורשית. על המשרד לוודא כי מיושמים האמצעים הבאים.

ד(5).1. ניהול הרשאות גישה וחשבונות משתמשים

52. על המשרד לוודא כי הוא מנהל באופן שוטף הרשאות גישה וחשבונות משתמשים בהתאם להמלצות המקובלות בתחום. בכלל זה, יש לוודא כי לכל משתמש מוקצה משתמש אישי, ולא שיתופי. כמו כן, יש לוודא סגירה של חשבון משתמש לאחר סיום העסקה או יציאה לחופשה ממושכת.
53. יש לוודא כי ההרשאות מוקנות בהתאם לעקרון מתן הרשאות נמוכות, וכי מדי רבעון מתבצע בדיקה שוטפת כי אין חשבונות משתמשים מיותרים במערכות המחשוב השונות, וכי רמת ההרשאה אשר הוקנתה למשתמש הולמת את אופי התפקיד.

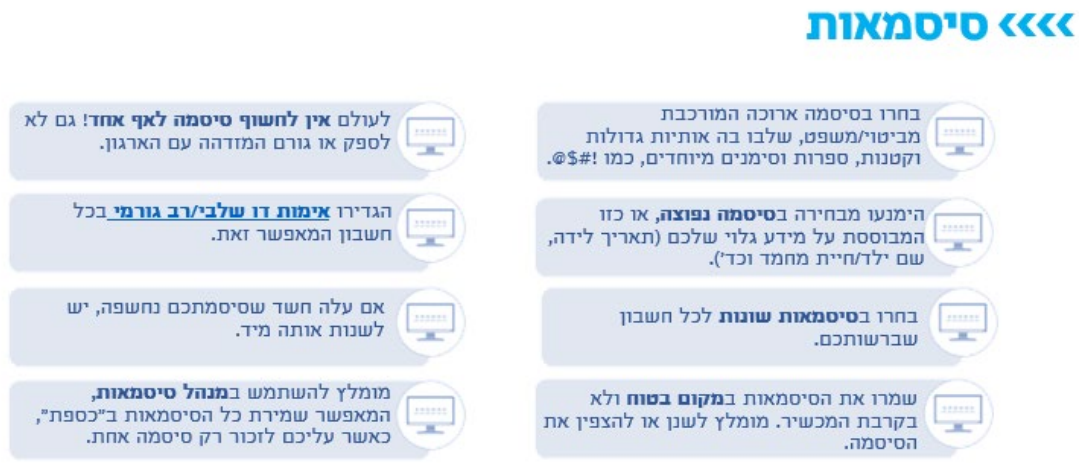
ד(5).2. סיסמאות הזדהות חזקות והגדרת נעילה לאחר כמה ניסיונות הזדהות כושלים

54. אחד מערוצי התקיפה הנפוצים מתבסס על ניסיונות פריצה באמצעות ניחוש סיסמאות. בעת תהליך התקיפה מתבצע תהליך הרצה של "מילון סיסמאות" במטרה לנסות לנחש את הסיסמה.

[33] מקור: מערך הסייבר הלאומי.

שימוש בסיסמה פשוטה מאפשר קלות ניחוש וגישה למערכות המחשוב. רצוי להגדיר סיסמה ארוכה וקשה לניחוש, המורכבת מצירוף של ספרות, אותיות גדולות וקטנות ותווים מיוחדים.

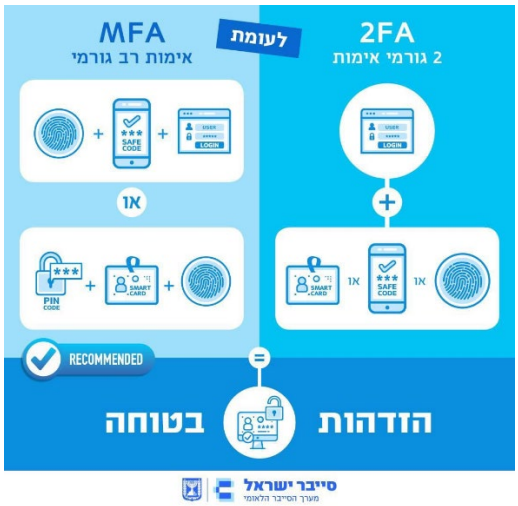
55. סיסמה חזקה חשובה במיוחד לתפקידים רגישים ברשת או לבעלי הרשאות גבוהות (כלומר בעלי תפקידים בעלי הרשאה במערכת להגדיר משתמשים או לשנות את הגדרות הרשת). יש לעבוד לפי נוהל שינוי סיסמאות ולא לחזור על סיסמאות שהיו בשימוש. מומלץ להשתמש בסיסמה ייחודית לכל אפליקציה.

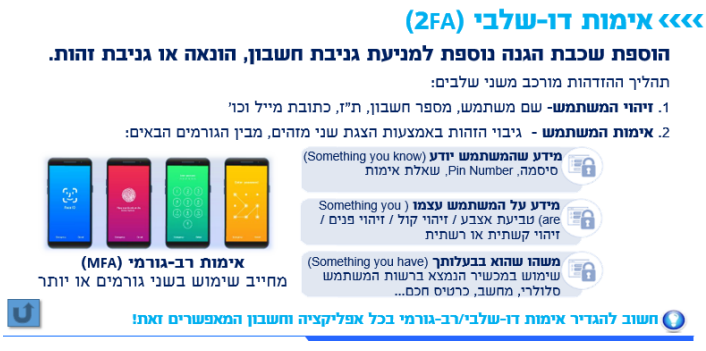


[תרשים מספר 3 – המלצות בנושא סיסמאות][34]

ד(5).3. מנגנון אימות דו-שלבי ("two factor authentication" או "2FA")

56. מנגנון אימות דו שלבי יוצר רובד אבטחה ומענה טוב אל מול ניסיונות גניבת הסיסמאות גם ב-"פישינג" (ראו להלן עוד על "פישינג"). פעולות פשוטות אלו יצמצמו את סיכוני התקיפה המבוססים על ניחוש סיסמאות. יישום מנגנון אימות דו שלבי מומלץ מאוד בכל אפליקציה ושירות שמאפשר אופציה זו. בהתאם לכך יש לדרוש מספק שירותי המחשוב ליישם זאת כל היכן שניתן.





[תרשים מספר 4 – אימות דו שלבי ורב גורמי][35]

---

[34] מקור: מערך הסייבר הלאומי.
[35] מקור: מערך הסייבר הלאומי.

ד(5).4. <u>הצפנת מידע</u>

57. מטרת ההצפנה היא לשמור על חשאיות הנתונים מפני גורמים שאינם מורשים. פתרונות ההצפנה המקובלים נותנים מענה לשמירת המידע בתנועה (כדוגמת דרישה מהספק לפתרונות HTTPS כפרוטוקול מאובטח) וכן לשמירת המידע באופן מוצפן גם בשרתים ובמחשבי המשרד, נוסף על מעגלי אבטחה נוספים. תהליך ההצפנה המתבצע ע"י צוות נותני שרות המחשוב במשרד או באמצעות ספקית השירות מחייב הצטיידות בתוכנות מתאימות, ניהול מפתחות הצפנה וכד'. במחשבים ניידים בעלי מערכת הפעלה Windows יש אפשרות להפעיל הצפנת דיסק מובנית מסוג bit locker.

ד(6). <u>קישוריות וצמצום חשיפה לסיכוני סייבר</u>

58. הקישוריות בין מחשבים, ניידות, עבודה מרחוק, אפליקציות מובייל, שימוש בענן מגדילים את ערוצי החיבור למשרד ו-"משטח התקיפה" של המשרד, אותו יכולים תוקפי סייבר לנצל לרעה.
59. **ערוצי הקישור המרכזים החשופים לסיכונים הם ערוץ הדואר האלקטרוני וערוץ הגלישה באינטרנט, ובנוסף סיכון הנובע משימוש במדיה נתיקה (במידה שהמשרד מאפשר זאת).**

ד(6).1. <u>הגנה על ערוץ הדואר האלקטרוני</u>

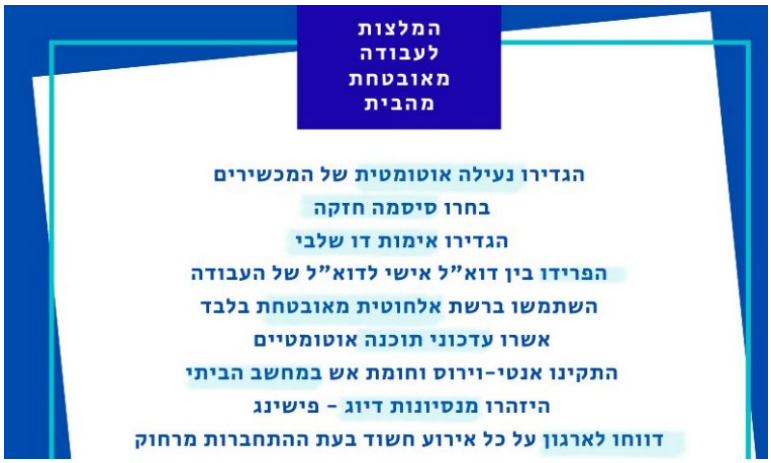
60. **ערוץ הדוא"ל הוא אחד הערוצים הפגיעים ביותר והוא מהווה ערוץ הכניסה המרכזי של תוקפים לארגון.** על משרד עורכי הדין לנקוט אמצעים מקובלים סבירים להגנה על מערכות הדואר האלקטרוני שלו מפני שימוש לרעה. באופן כללי ניתן לרכוש שירותי הגנה ברמה גבוהה מספק שירותי התקשורת או הענן. בפרט, שירותי סינון פישינג ואנטי-ספאם מפחיתים את החשיפה של עובדי המשרד לניסיונות הונאה.
61. במסגרת זאת יש לתת את הדעת שהעברת מידע בדואר אלקטרוני, ללא הצפנה, מאפשרת לגורמים לא מורשים ליירט מידע זה בצורה קלה יותר. לכן מומלץ ליישם שיטות הצפנה מקובלות על הדואר האלקטרוני או להעביר את המידע כשהוא מוצפן. יש לתת את הדעת לקיום החובה האתית גם כלפי ספק הדואר, ולוודא כי תנאי השימוש של ספק אפליקציית הדואר אינם מפרים את חובת הסודיות.

ד(6).2. <u>הגנה על ערוץ שירותי גלישה</u>

62. הגלישה באינטרנט מבוססת על קיום תקשורת נכנסת ויוצאת מרשת המשרד, ולכן כשם שהיא מאפשרת לעובדי המשרד להתחבר לאתרי אינטרנט, היא מאפשרת גם לאתרי אינטרנט וגם לתוקפים לנצל ערוץ זה להפעלת קבצים זדונים ברשת המשרד.
63. על משרד עורכי הדין להגן על ערוץ שירותי הגלישה באמצעים מקובלים וסבירים, על מנת למנוע גישה לאתרים פוגעניים מצד אחד ולשמירה על אתר האינטרנט של המשרד מצד שני. שירותים אלו חיוניים גם לטובת הגנה על לקוחות וספקים של המשרד.
64. על המשרד לדרוש מספק תשתיות התקשורת של המשדר לספק שירותי הגנה על הגלישה במסגרת חבילת התקשורת אותה המשרד רוכש.

ד(6).3. <u>עבודה מרחוק – הגנה על חיבור מרחוק אל רשת המשרד (לעובדים, לספקים ולצורך שירות תמיכה מרחוק)</u>

65. על המשרד לוודא כי חיבור מרחוק אל הרשת הינו אך ורק באמצעות רכיב VPN-SSL המצפין את תעבורת המידע לכל חיבור מרחוק, תוך וידוא כי המחשב המתחבר עומד בדרישות היגיינה בסיסיות דוגמת העדר נוזקות וקיומם של עדכוני אבטחה אחרונים. יש לוודא כי המנגנון כולל מנגנון הזדהות כפולה 2 Factor Authentication על מנת לאמת שרק עובדים או ספקים המורשים לכך יכולים להתחבר למשרד באופן מאובטח. על המשרד לדרוש מספקי התקשורת לספק שירותי VPN.
66. היקף העבודה מרחוק והקישוריות למערכות המשרד מגדיל את החשיפה של הרשת הארגונית, ומייצר סיכון לפגיעה באבטחה. עם זאת, קישוריות זו נדרשת לצורך פעילות המשרד. עקב כך יש להקפיד על אמצעי ההגנה בכניסה לרשת הארגונית ועל מדיניות סיסמאות חזקה (כפי שתואר לעיל).
67. רצוי כי הגישה מרחוק תתבצע מאמצעי קבוע אשר "מוכר" למשרד, כלומר נרשם וזוהה במערכות הנהלות את הגישה. רצוי לאפשר גישה מרחוק לתיקיות חיוניות בלבד, ולהפריד בין גישה לדוא"ל לבין גישה לשרת/תיקיות/נכסים רגישים. אחת לתקופה, יש לבדוק אם ההרשאות אשר הוקנו עדיין רלוונטיות ואם לא יש להסיר את ההרשאות שאינן נדרשות. יש להגביל גם את משך החיבור מרחוק. יש להפקיד על עדכניות גרסאות התוכנה של רכיב ה- VPN שבשימוש על מנת למנוע ניצול חולשות אבטחה בערוץ קריטי זה.
68. יש לוודא בחוקת ה- Firewall כי הרשאות הגישה מרחוק נקבעת במינימום הנדרש, וכן כי מתקבלים לוגים לתיעוד ההתחברות. איסוף לוגים שגרתי הינו חלק משמעותי מהיכולת לאתר תקיפה ואת אופן פעולתה. בנוסף, מומלץ להגדיר מדינות ואזורים אשר מורשים להתחבר למשרד.
69. במחשב נייח/נייד, יש להגביל את הגישה לשורת פקודה) דוגמת PowerShell) כך שלא יהיה ניתן להריץ סקריפטים שמקורם לא ידוע, או שמקורם ממחשב אחר.
70. מומלץ ליישם התחברות דרך ממשק מאובטח, כגון "Terminal Services".
71. לצורך הגברת אמצעי האבטחה בצד המשרד, יש להקפיד על המלצות לעובדי המשרד המתחברים אל הרשת הארגונית מרחוק.

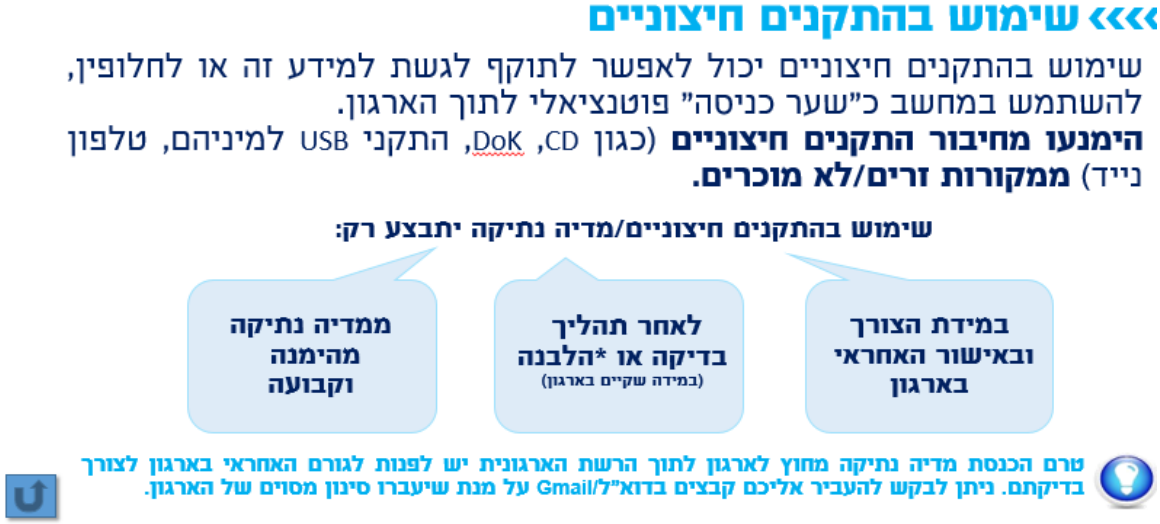


<u>[תרשים מספר 5 – המלצות לעובדים לעבודה מרחוק]</u>[36]

[36] מקור: מערך הסייבר הלאומי.

ד(6).4. שימוש בטוח ב- Disk on Key (DOK)[37]

72. על המשרד ליישם נוהל עבודה עם אמצעי מדיה נתיקה מסוג DOK או אחרים אשר יכולים להוות משטח תקיפה משמעותי עבור מערכות המחשוב של המשרד.
73. יש להמעיט ככל שניתן בשימוש באמצעים אלו וכאשר נעשה בהם שימוש יש לעשות זאת אך ורק עם אמצעים חדשים שנרכשו ברשתות קמעונאיות מוכרות ולשימוש ראשוני ע"י עובדי המשרד בלבד. מומלץ להחליף אמצעים אלו בחדשים מהאריזה לעיתים תכופות ולהשמיד את הישנים.



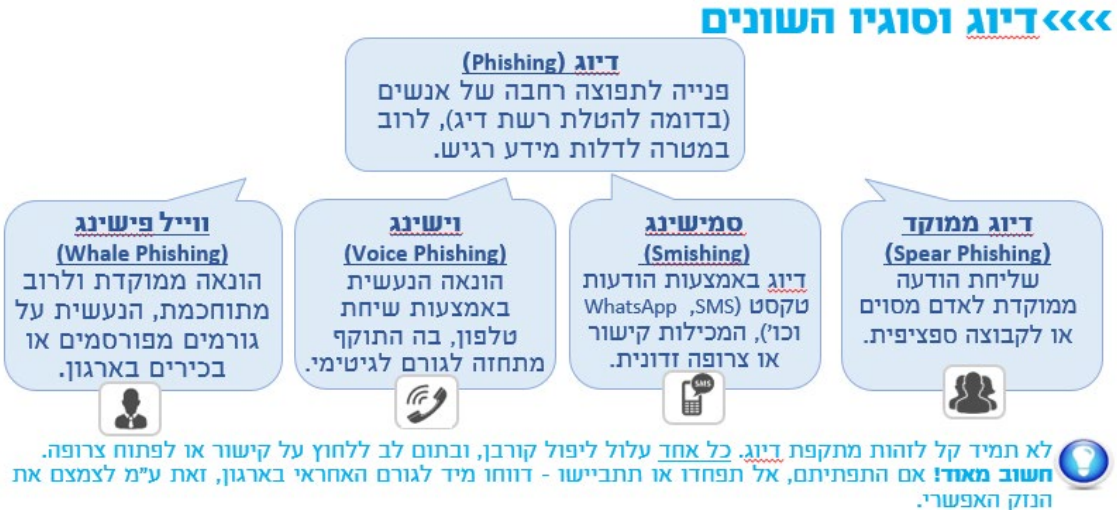
[תרשים מספר 6- שימוש ב- disk on key][38]

ד(7). מודעות עובדים

74. חלק משמעותי מתקיפות הסייבר נובעות מטעויות אנוש או פעולות של הונאה או שיטוי של בעלי ההרשאות הלגיטימיים למערכות, בידי התוקף. מערך הסייבר הלאומי פירסם ערכת הדרכה בסיסית המבהירה מהם סיכוני הסייבר ומה תפקיד העובדים בהגנת הסייבר.[39]
75. טכניקה נפוצה שמבוססת על הטעייה של עובדים, היא משלוח דואר מתחזה (פישינג), שמעודד לחיצה על קישור המוביל להורדת תוכנה זדונית. מנהלים ועובדים פותחים הודעות מייל או SMS זדוניות שנראות תמימות ולגיטימיות ולוחצים על קישור (לינק) או על קובץ מצורף שגורם להדבקה.

---

[37] עמידה בפרק זה תהווה סיוע לעמידה בתקנה 12 לתקנות אבטחת מידע.
[38] מקור: מערך הסייבר הלאומי.
[39] ערכת הדרכה בנושאי איומי סייבר ואבטחת מידע, ה"ש 13 לעיל.



[תרשים מספר 7 – סוגים שונים של דיוג][40]

76. התקפות מתקדמות יותר מבוססות על "הנדסה חברתית" שהינה הונאה ברמת תחכום גבוהה יותר, כגון שימוש בשפה או מונחים ייחודים לארגון המקנים למסר לגיטימיות.
77. לאחר לחיצה על קישור זדוני שלא נחסם במערכות ההגנה, עלולה להתחיל שרשרת הדבקה של מערכות המחשוב והתפשטות הנוזקה בארגון, אשר יכולה להסתיים בגניבת כל המידע של הארגון והצפנת הקבצים אשר בעקבותיה לרוב מגיעה דרישה לתשלום כופר. בנוסף הארגון עלול לסכן את מי שמחובר אליו כגון לקוחות וספקים.
78. **הסוגים השונים של דיוג (כמפורט בתרשים מספר 7) מהווים נכון להיום "ציר הכניסה" המרכזי של תוקפים, ולכן החשיבות הרבה של מודעות עובדים לכך.**
79. עקב כך על משרד עורכי הדין לוודא קיום נוהל הכשרה ל"מודעות אבטחת מידע וסייבר" לעובדים חדשים ולריענון הנוהל לפחות אחת לשנה לעובדים וותיקים. הוראה זו תאפשר גם להעביר לעובדי משרדי עורכי הדין את חובתם בהתאם לכלל 20 לכללי לשכת עורכי הדין (אתיקה מקצועית), תשמ"ו-1986.

ד(8). ספקים ו – "שרשרת אספקה"

80. משרדי עורכי דין רוכשים שירותים שונים שיש להם נגיעה למערכות המידע או לתהליכי העבודה המשלבים מידע של המשרד. נגישות זו מייצרת סיכונים חיצוניים לאבטחת המידע הידועים כ-"סיכוני שרשרת אספקה".[41]
81. לצורך התמודדות עם סיכון זה על המשרד לבחון את מהימנות הספקים, ולוודא כי הבטיח בחוזה השירות את קיום החובות החלות על המשרד גם לגבי הספק. כמו כן, פיקוח ובקרה כנדרש בתקנה 15 לתקנות אבטחת מידע. יש להדגיש את החשיבות של קביעת תניות חוזיות מתאימות העוסקות בהגנת סייבר,[42] ווידוא כי הספקים עומדים בהתחייבויות שניתנו מצדם. על הספק להתחייב

[40] מקור: מערך הסייבר הלאומי.
[41] תקיפת ארגונים באמצעות שרשרת אספקה, ה"ש 17 לעיל.
[42] בין היתר, התניות הקבועות בסעיף 17.14.7 להחלטה זו.

לרמת האבטחה הנדרשת בידי המשרד, וכן לעדכן את המשרד על חשש לאירוע אבטחה שעלול להשפיע על המשרד.

82. לעניין זה נפנה להוראות סעיף 17.14 לעיל.

ד(9). <u>התאוששות מאירוע סייבר</u>

83. על המשרד להתכונן באופן פעיל לקראת אירוע סייבר. אירוע סייבר אינו שאלה של "אם" אלא שאלה של "מתי". על המשרד להתכונן להתרחשות אירוע סייבר ברמת סבירות גבוהה על מנת להבטיח התאוששות מהירה והגנה על העובדים והלקוחות.

ד(9).1. <u>חשיבות גיבוי המידע</u>

84. תהליך גיבוי מוסדר מאפשר יכולת התאוששות ושחזור המידע לאחר מתקיפות סייבר שונות. קיימות שיטות גיבוי שונות, לדוגמא:

84.1. גיבוי מקומי – גיבוי "חם" – המגבה את כל המידע באופן אוטומטי לדיסק נוסף המחובר באופן קבוע.

84.2. גיבוי מקומי – גיבוי "קר" – להתבצע בצורה ידנית פעם במספר ימים על גבי דיסקים חיצוניים או קלטות אשר לא מחוברים קבוע למחשבי המשרד. יש לוודא הוצאה של הגיבוי מחוץ לחצרות הארגון, וזאת במטרה לצמצם את ההשפעה במקרה של אירוע סייבר או אירוע אחר דוגמת שריפה.

84.3. גיבוי לשירות ענן – גיבוי אוטומטי לשירות ענן חיצוני המסופק ע"י חברת התקשורת ו/או חברה המתמחה בכך.

85. על עורך הדין לבצע גיבוי למידע הסודי. ועדת האתיקה הארצית תראה בכל אחד מהגיבויים לעיל כגיבוי מספק (במיוחד שמירה בענן), ואולם מערך הסייבר הלאומי ממליץ אף על קיום גיבוי משולש של שלושת האפשרויות המנויות לעיל.

86. על המשרד לוודא כי קיים נוהל גיבויים ושחזורים תקף ועדכני וכן לבצע בדיקה של נוהל זה בפועל מעת לעת, לפחות פעם בשנה. יש לוודא מול אנשי המחשוב כי קיים תהליך גיבוי מתאים.[43]

ד(9).2. <u>היערכות לאירועי סייבר</u>

87. הוועדה תמליץ למשרדי עורכי דין להתקשר בהסכם עם חברת שירותי סייבר אשר תערוך עבורם תכנית תגובה לאירועי סייבר המותאם למשרדם. בעת אירוע סייבר על המשרד להפעיל את הנוהל ולפעול על פיו. מומלץ לבצע תרגול של נוהל זה מעת לעת, לפחות אחת לשנה על מנת לוודא מוכנות המשרד ועדכניות התוכנית תגובה לאירועים.

[43] לעניין זה הוועדה תפנה ל"המלצות גיבוי לעסקים קטנים" מערך הסייבר הלאומי (13.10.2021) https://www.gov.il/he/departments/general/smb_backup.

ה. הוראת מעבר

88. ככלל, ועדת האתיקה הארצית, בהחלטותיה המשמעתיות לשנת 2022, בנושאים נשוא החלטה זו, תעדיף להתריע בפני עורך הדין ולדרוש עמידה בהוראות החלטה זו על פני העמדה לדין משמעתי וזאת למעט במקרים חריגים.
89. תלונות וגילויי דעת בנושא ירוכזו וינוהלו בידי ועדת האתיקה הארצית, עד להטמעה מלאה של הנושא.

ו. מערך הסברה

90. הלשכה תקיים בעצמה או באמצעות ספקים מטעמה, השתלמויות הסברה לעורכי הדין – החלטת ועדת האתיקה הארצית "סודיות עו"ד לקוח – אבטחת מידע" הלכה למעשה. השתתפות בהשתלמויות אלו ייחשבו כעמידה בחובה הקבועה בסעיף 24.10 בהחלטה זו.
91. הוועדה המייעצת לוועדת האתיקה בנושא אבטחת מידע תוציא מעת לעת המלצות נוספות אשר יסייעו לעורך הדין לאבטח את המידע הסודי באופן מיטבי. ועדת האתיקה תפיץ המלצות אלה בקרב עורכי הדין. ועדה זו תתייחס לטכנולוגיות חדשות, וסוגיות שיובאו לפתחה מקרב עורכי הדין ולקוחותיהם, וכן מקרב הספקים הרלוונטיים. הוועדה תפיץ המלצות אלו בקרב עורכי הדין.
92. ועדת האתיקה הארצית יחד עם מערך הסייבר הלאומי תפעל לפרסום רשימה של ספקי שירותים אשר אושרו על ידה כעומדים בדרישות החלטה זו, על מנת לסייע לעורכי דין ברכש שירותים.

נספח א' : **<u>המלצות תיקון כללי לשכת עורכי הדין</u>**

מבלי לגרוע מחובותיו של עורך הדין עפ"י הדין הקיים, כמפורט בהחלטתנו זו, מוצע לתקן את הכללים על מנת להדגיש את חובתו של עורך הדין לאבטחת מידע שהגיע מלקוחו וזאת באופן הבא:

1. **בכללי לשכת עורכי הדין (אתיקה מקצועית), תשמ"ו-1986**

1.1. תחת סעיף 19 לכללים, יוסף סעיף 19א.:

אבטחת מידע

19א. עורך דין ינקוט אמצעים הולמים לאבטחת המידע שיובא לידיעתו בידי לקוחו או מטעמו ואשר נשמר באמצעים דיגיטליים ובמערכות המידע בשליטתו ובשימושו.

1.2. סעיף 20 לכללים יוחלף בנוסח הבא:

שמירת סודיות ואבטחת המידע בידי העובדים

20. עורך הדין יעמיד את העובדים בשירותו על חובתם לשמור על סודיות העניינים המגיעים לידיעתם במהלך עבודתם **ועל חובתם בדבר אבטחת המידע.**

2. **כללי לשכת עורכי הדין (שמירת חומר ארכיוני במשרדי עורכי דין), תשל"א-1971**

מוצע להוסיף הוראה לעניין אבטחת המידע המורה לעורך הדין לנקוט באמצעים הולמים לאבטחת כל חומר ארכיוני ומסמכים השמורים בידיו ובכלל זאת אלו השמורים באמצעים דיגיטליים.

נספח ב': **<u>שאלון עזר פנימי – אבטחת המידע במשרדי עורכי הדין</u>**

1. **על מנת לסייע לעורכי הדין בדבר הטמעת כלל החובות האתיות החלות עליהם בקשר עם אבטחת המידע, ועדת האתיקה ניסחה שאלון עזר פנימי. שאלון זה יהווה כלי עזר למשרד עורכי הדין ולגורמי אבטחת המידע מטעמו בזיהוי המערכות והמידע הנדרשים באבטחת המידע.**

2. תחומי העיסוק של המשרד וגודלו (מספר לקוחות ומספר עובדים) משפיעים מאוד על רמת הסיכון אליו חשוף המשרד מבחינת משטח התקיפה שלו ע"י גורמים עוינים וסיכוני חשיפה לתקנות הפרטיות. משום כך חשוב מאוד להגדיר את פרופיל הסיכון של המשרד ולהתאים את חליפת ההגנה לפרופיל זה.

א. <u>תיאור כללי של פעילות המשרד</u>

תחומי העיסוק של המשרד[44]	סוג המידע הנאסף במסגרת תיקי הלקוחות בתחום זה	לעניין מידע אישי - סיווג המידע לפי התוספת לתקנות הגנת הפרטיות (אבטחת מידע)	מורשי גישה למידע מבין עובדי המשרד (תפקידים)	מורשי גישה אחרים (תפקידים/מספר)

ב. <u>פעילות ארגונית - תיקי עובדים</u>

צורות העסקה של המשרד	סוג המידע הנאסף במסגרת צורות העסקה	לעניין מידע אישי - סיווג המידע לפי התוספת לתקנות הגנת הפרטיות (אבטחת מידע)	מורשי גישה למידע מבין עובדי המשרד	מורשי גישה אחרים

ג. <u>הסיכונים המרכזיים לפגיעה באבטחת המידע הינם</u>:

1. פריצה למערך המחשוב של המשרד ו/או למחשבי עובדי המשרד שתוביל לפגיעה בחובת הסודיות ו/או בחוק הגנת הפרטיות ו/או למניעת גישה למידע.
2. פריצה למחשבי ספק שירות של המשרד (צד ג' בשרשרת האספקה).
3. שימוש לרעה בידי ספק שירות.
4. שימוש לרעה בידי עובד.
5. תקלת מחשוב או תקשורת שתביא לאי זמינות מערכות המשרד ותמנע גישה למידע.

[44] תשומת הלב תינתן לעיסוק בתחומים הכוללים בחובם אחזקת מידע רגיש דוגמת 'מידע פנים' כהגדרתו לחוק חוק ניירות ערך, תשכ"ח-1968; 'מידע אישי' החוסה בצל חוק הגנת הפרטיות בעל רגישות מיוחדת דוגמת תיקי מעמד אישי, אימוץ, צוואות, מידע רפואי וכיו"ב.

ג.1. הכנה ואכיפה של מדיניות ונהלים להגנה בסייבר למשרד עו"ד לטובת הימנעות ותגובתיות לאירועי סייבר

תיאור	סוג הנוהל	הטמעת הנהלים	פיקוח ומעקב אחר ביצוע	שם הגורם האחראי לציות לנהלים	שם הגורם הניהולי המנחה את הגורם האחראי

ג.2. אופן ביצוע פעילות מודעות עובדים להימנעות ותגובתיות ואירועי סייבר

תיאור	מחזוריות	הדרכה והסמכה	אימון ותרגול	שם הגורם האחראי למודעות	שם הגורם הניהולי המנחה את הגורם האחראי

ד. אופן ביצוע הפעילות הממוחשבת והתמודדות עם הסיכונים

ד.1. הגבלת גישה למערכות המידע ומימוש מדיניות הסיסמאות

תיאור/כמות	ניהול הרשאות משתמשים	ניהול סיסמה חזקה	2 Factor Authentication	שם הגורם הטכני האחראי להרשאות משתמשים	שם הגורם הניהולי המנחה את הגורם הטכני

ד.2. הגבלת גישה למידע ומימוש מדיניות הצפנות

תיאור/כמות	ניהול הרשאות משתמשים למידע	ניהול מפתחות הצפנה	בקרת גישה Audit	שם הגורם הטכני האחראי להרשאות משתמשים	שם הגורם הניהולי המנחה את הגורם הטכני

ד.3. הגבלת גישה למערכות המידע ומימוש מדיניות הפרדת רשתות (סגמנטציה)

תיאור/כמות	ניהול הרשאות גישה למשתמשים	ניהול חלוקת שירותים ל VLAN-ים	מדיניות ניהול WIFI	שם הגורם הטכני האחראי לרשת	שם הגורם הניהולי המנחה את הגורם הטכני

ד.4. מחשבים המצויים במשרד ובידי עובדי המשרד (נייחים, ניידים, טאבלטים)

תיאור/כמות	תוכנות	תצורת אבטחה מקסימלית של Windows10	אנטיוירוס [EDR]	שם הגורם הטכני האחראי לתחנות קצה	שם הגורם הניהולי המנחה את הגורם הטכני

ד.5. <u>מחשבים ושרתים שאינם במשרד ומשרתים את הפעילות (מיקור חוץ)</u>

תיאור	סוג השירות	אחריות להגנה על השירות	מפרט ההגנה על השירות	שם הגורם הטכני האחראי להגנה	שם הגורם הניהולי המנחה את הגורם הטכני

ד.6. <u>שירותי מחשוב ענן</u>

תיאור	סוג השירות	אחריות להגנה על השירות	מפרט ההגנה על השירות	שם הגורם הטכני האחראי להגנה	שם הגורם הניהולי המנחה את הגורם הטכני

ד.7. <u>שירותי תקשורת</u>

שם הספק	סוג השירות	אחריות להגנה על השירות	מפרט ההגנה על השירות	שם הגורם הטכני האחראי להגנה	שם הגורם הניהולי המנחה את הגורם הטכני

ד.8. <u>הגורם האחראי במשרד לטכנולוגיה תקשורת ואבטחת מידע</u>

שם	סוג השירות ורמת השירות (SLA)	מפרט השירות	מועד ההסכם	שם איש הקשר למשרד	שם הגורם הניהולי המנחה את הגורם הטכני

ה. **<u>הוראות אבטחה פיזית לעניין מערכות המידע</u>**

1. מערכות המידע המשמשות את המשרד והמצויות בחזקתו מוגנות באמצעים הבאים:
   א. חדר נפרד.
   ב. ארון נעול.
   ג. חדר שרתים.
   ד. אחר: _____.
2. ספקי שירותי מחשוב מחוייבים באבטחה פיזית לשירותים.
3. עובדי המשרד קיבלו הדרכה וריענון בתחום האבטחה הפיזית.

ו. **<u>הוראות לענין מורשי גישה</u>**

תחומי העיסוק של המשרד	סוג המידע הנאסף במסגרת תיקי הלקוחות בתחום זה	לעניין מידע אישי - סיווג המידע לפי התוספת לתקנות הגנת הפרטיות (אבטחת מידע)	מורשי גישה למידע מבין עובדי המשרד (תפקידים)	מורשי גישה אחרים (תפקידים/מספר)

1. מורשי הגישה חתמו על טופס כללי עשה ואל תעשה למורשי גישה, או נוהל שימוש במערכות המחשב והתקשורת של המשרד.
2. הדרכות שנתיות
3. פעולות נוספות להעלאת מודעות כדוגמת שיתוף מידע בזמן אמת של הודעות Phishing, מנוי לניוזלטר של מערך הסייבר הלאומי.

ז. <u>רישום מעודכן של סוג מורשי הגישה</u>:

מערכת	תפקיד/הרשאה	שם

מועד עדכון אחרון: _____

3. <u>תצורות מפרטי ההגנה</u>

להלן המלצה למפרט הגנת הסייבר על משרדי עו"ד בהתאם לשלושת הקטגוריות הבאות:

- קטגוריה א' – **תצורה בסיסית** של רמת הגנת סייבר על המשרד: זו התצורה המינימאלית המספקת רמת הגנה מאוד בסיסית וחיונית להגנת כל עסק קטן. תצורה בסיסית זו הינה התצורה הבסיסית המחויבת בהתאם להחלטת ועדת האתיקה של הלשכה מספר את/01/22.
- קטגוריה ב' – **תצורה מומלצת** של רמת הגנה סייבר על המשרד: זו התצורה המומלצת למרבית העסקים הקטנים והבינוניים במשק.
- קטגוריה ג' – **תצורה מתקדמת** של רמת הגנת סייבר על המשרד: זו התצורה המועדפת עבור עסקים בינוניים וגדולים או כאלה בעלי מידע בעל רגישות גבוהה.

המלצות חשובות בבחירת ספק שירותי סייבר מנוהלים:

1. ההמלצה לדרוש מהספקים פתרונות טכנולוגיים של אחד חמשת היצרנים המובילים בעולם כפי שמוגדר ע"י חברות הסיקור הגדולות ואשר להם נוכחות משמעותית בשוק הישראלי.
2. ההמלצה היא להתקשר לשירות מנוהל מקומי שכולל מגוון שירותים ופתרונות מובילים מתחום ה IT, תקשורת ואבטחת מידע: התקנה, עדכון, ניטור ותמיכה טכנית תחת SLA ברור.
3. ההמלצה היא לבחור ספק שירות מנוהל אשר הוסמך ברמה גבוהה ע"י יצרן ציוד הגנת הסייבר הנמכר ואשר מטמיע את המוצר בהקפדה בהתאם להוראות יצרן לתצורה שתמקסם את אבטחת המידע של המשרד.
4. ההמלצה היא לוודא שהשירות המנוהל מוזן בשירות on-line מעדכוני חתימות מודיעין וניטור לוגים של ספק הציוד המוטמע במשרד

טבלה 1 – מפרטת הדרישות עבור קטגוריה א' - תצורת הגנה בסיסית המחויבת במשרדי עורכי דין (כמפורט, הימנעות מתצורת הגנה בסיסית תחשב על פניו לאי עמידה לכאורה בחובות של עורך הדין כמפורט מעלה)

מס' דרישה	נושא	תיאור
.1	הגנה רציפה על הרשת הארגונית (ככל שעורך הדין מחזיק רשת כזו) כולל FireWall; וAntivirus &Anti malware	התקנת פיירוול דור חדש Next FW Generation (NGFW) של אחד מ 5 היצרנים המובילים בעולם. התקנה בתצורה שירות מנוהל (למעט אם עורך עובד באופן יחידני ללא צוות עורכי דין ועובדים אחרים).
.2	הגנה על ערוץ הדוא"ל	שירות מנוהל כחלק מחבילת ה NGFW ספאם ופישינג Anti-spam
.3	הגנה על ערוץ הגלישה לאינטרנט WEB	שירות מנוהל כחלק מחבילת ה NGFW למניעת גלישה לאתרים זדוניים
.4	הגנה על שירות ה WiFi של המשרד ואבטחת רשת ה – WiFi באמצעות סיסמה חזקה.	שירות מנוהל כחלק מחבילת ה NGFW
.5	הגנה על הגישה מרחוק לארגון באמצעות תקשורת מוצפנת ואבטחת גישה באמצעות הזדהות דו-שלבית.	שירות מנוהל כחלק מחבילת ה NGFW
.6	הגנה על תחנות הקצה (מחשבים ניידים, נייחים, שרתים)	מלבד גרסאת AV גם שירות EDR מנוהל ע"י ספק התקשורת או ה HOSTING
.7	שירות גיבויים מנוהל	שירות גיבויים אוטומטי מנוהל ע"י ספק התקשורת או ה HOSTING

טבלה 2 – מפרטת הדרישות עבור קטגוריה ב' – תצורת הגנה מומלצת

מס' דרישה	נושא	תיאור
.1	הגנה על הרשת הארגונית כולל: 1. FireWall 2. IPS 3. Antivirus &Anti bot 4. Application Control 5. Sandbox	התקנת פיירוול דור חדש Next FW Generation (NGFW) של אחד מ 5 היצרנים המובילים בעולם. התקנה בתצורה שירות מנוהל.
.2	הגנה על ערוץ הדוא"ל	שירות מנוהל כחלק מחבילת ה NGFW ספאם ופישינג Anti-spam
.3	הגנה על ערוץ הגלישה לאינטרנט WEB	שירות מנוהל כחלק מחבילת ה NGFW למניעת גלישה לאתרים זדוניים
.4	הגנה על שירות ה WIFI של המשרד	שירות מנוהל כחלק מחבילת ה NGFW
.5	הגנה על הגישה מרחוק לארגון SSL-VPN לכל תחנות הקצה הניידות כולל Mobile	שירות מנוהל כחלק מחבילת ה NGFW
.6	הגנה על תחנות הקצה (מחשבים ניידים, נייחים, שרתים)	מלבד גרסאת AV גם שירות EDR מנוהל ע"י ספק התקשורת או ה HOSTING
.7	שירות גיבויים מנוהל	שירות גיבויים אוטומטי מנוהל ע"י ספק התקשורת או ה HOSTING

טבלה 3 – מפרטת הדרישות עבור קטגוריה ג' – תצורת הגנה מתקדמת

מס' דרישה	נושא	תיאור
.1	הגנה על הרשת הארגונית כולל: 1. FireWall 2. IPS 3. Antivirus &Anti bot 4. Application Control 5. Sandbox	התקנת פיירוול דור חדש Next FW Generation (NGFW) של אחד מ 5 היצרנים המובילים בעולם. התקנה בתצורה שירות מנוהל.
.2	הגנה על ערוץ הדוא"ל	שירות מנוהל כחלק מחבילת ה NGFW ספאם ופישינג Anti-spam
.3	הגנה על ערוץ הגלישה לאינטרנט WEB	שירות מנוהל כחלק מחבילת ה NGFW למניעת גלישה לאתרים זדוניים
.4	הגנה על שירות ה WIFI של המשרד	שירות מנוהל כחלק מחבילת ה NGFW
.5	הגנה על הגישה מרחוק לארגון SSL-VPN לכל תחנות הקצה הניידות כולל Mobile	שירות מנוהל כחלק מחבילת ה NGFW
.6	הגנה על תחנות הקצה (מחשבים ניידים, נייחים, שרתים)	מלבד גרסאת AV גם שירות EDR מנוהל ע"י ספק התקשורת או ה HOSTING
.7	שירות גיבויים מנוהל	שירות גיבויים אוטומטי מנוהל ע"י ספק התקשורת או ה HOSTING
.8	שירות WAF מנוהל	להגנה על הגישה לאפליקציות WEB
.9	שירות DLP מנוהל	להגנה מפני דלף מידע מהארגון
.10	שירות SOC מנוהל	שירות מוקד ניתוח וניהול אירועי סייבר מנוהל 24/7

נספח ג' : **<u>צוות מייעץ בתחום אבטחת מאגרי מידע – מינוי הצוות ופעילותו</u>**

1. הצוות, אשר הוסמך על ידי יו"ר הוועדה, מונה את החברים הבאים :

1.1. יו"ר הוועדה, עו"ד מנחם מושקוביץ – יו"ר ועדת האתיקה הארצית בלשכת עורכי הדין ובעל משרד עורכי דין ;

1.2. מנכ"ל לשכת עורכי הדין, מר אורי אלפרסי ;

1.3. עו"ד גידי פרישטיק – שותף במשרד מיתר | עורכי דין, יועץ האתיקה של המשרד, סגן יו"ר (משותף) בביה"ד המשמעתי הארצי של לשכת עורכי הדין. מרצה בתחום האתיקה של עורכי הדין בפקולטה למשפטים באוניברסיטת בר אילן ;

1.4. עו"ד הדר אראל-קשפיצקי – עו"ד במשרד מיתר | עורכי דין ;

1.5. מר גולן אטיה – מנהל מערכות ואבטחת המידע במשרד מיתר | עורכי דין ;

1.6. עו"ד עמית אשכנזי– היועץ המשפטי ומנהל המחלקה המשפטית של מערך הסייבר הלאומי ומרצה מהחוץ במרכז למשפט וטכנולוגיה באוניברסיטת חיפה ;

1.7. מר דוד (דדי) גרטלר- ראש אגף בכיר טכנולוגיות, מערך הסייבר הלאומי ;

1.8. עו"ד ליאת גורפינקל ; סגנית היועץ המשפטי למערך הסייבר הלאומי ;

1.9. ד"ר עו"ד לימור זר גוטמן– ראש המרכז לאתיקה בבית הספר למשפטים במכללה למנהל. מומחית בתחום האתיקה והאחריות המקצועית של עורכי הדין והשופטים ;

1.10. עו"ד דרור ארד אילון– לשעבר ראש ועדת האתיקה הארצית ;

1.11. ד"ר נמרוד קוזלובסקי – מרצה וראש המסלול ללימודי סייבר באוניברסיטת תל אביב, יזם בתחום האינטרנט ואבטחת מידע ומלווה בליווי עסקי ומשפטי חברות אינטרנט וטכנולוגיה. שותף ב-JVP, קרן הון סיכון מובילה בישראל, ולמעבדות JVP-Cyber, חממת סייבר סקיוריטי בבאר שבע, תוך התמקדות ב-Cyber Security וב-Big Data ;

1.12. עו"ד דן אור-חוף – מייסד ובעל משרד אור-חוף, שותף מייסד בחברת היעוץ בתחום הגנת המידע Strand Advisory, חבר המועצה הציבורית להגנת הפרטיות, מייסד ויו"ר הפורום הישראלי לעוסקים בתחום הגנת המידע (IDPF), חבר ב – Advisory Board for Publications של ארגון מומחי הגנת הפרטיות IAPP, מרצה בפקולטה למשפטים (התוכנית לאומנויות המשפט) באוניברסיטת תל אביב ;

1.13. עו"ד דן חי – יו"ר ועדת הגנת הפרטיות בלשכת עורכי הדין ;

1.14. עו"ד מורן שניידר רוזנבלום – ראש אשכול חקיקה, הלשכה המשפטית משרד המשפטים ;

1.15. עו"ד רן סלבצקי – אשכול חקיקה, הלשכה המשפטית משרד המשפטים ;

1.16. עו"ד עדית נחמן – ייעוץ וחקיקה משרד המשפטים ;

1.17. עו"ד מיכל אברהם – ייעוץ וחקיקה משרד המשפטים.

1.18. עו"ד ניר גרסון – סגן היועץ המשפטי, הרשות להגנת הפרטיות ;

1.19. עו"ד לינא כמאל – הממונה על הפיקוח במחלקת האכיפה, הרשות להגנת הפרטיות ;

1.20. עו"ד רחל גולדשמיד ;

1.21. עו"ד אילן שדי – יו"ר (משותף) פורום משפט מדע וטכנולוגיה, לשכת עורכי הדין ;

1.22. עו"ד איתן עמרם – יו"ר (משותף) פורום משפט מדע וטכנולוגיה, לשכת עורכי הדין.

1.23. הצוות מלווה ביועץ מקצועי, עו"ד יעקב עוז, יו"ר ועדת הסייבר, אבטחת מידע והגנת הפרטיות בלשכת ארגוני העצמאים בישראל, מרצה, יועץ ומייצג בתחום הגנת הפרטיות – אבטחת מידע.

1.24. הצוות מלווה בחברי המנגנון בוועדת האתיקה הארצית בלשכה – עוה"ד שלי ואקנין אדם, דנית גבריאל, דניאל ברדה-אברהמוב.

2. **יעדי הוועדה כפי שהוגדרו בידי יו"ר ועדת האתיקה הארצית, הינם כלהלן:**

2.1. פרסום החלטה אשר תגלה את דעת הוועדה בדבר דרישות אבטחת המידע החלות על עורכי-הדין וכן המלצות נוספות ככול שתמצא לנכון.

2.2. להמליץ על שינויי כללי לשכת עורכי הדין הנדרשים לטעמה.

2.3. חלופת אבטחת מידע למשרדי עו"ד בשים לב לתיקוני החקיקה וסמכות הרשם לפי תקנה 20 לתקנות אבטחת מידע.

2.4. ועדת האתיקה הארצית תמשיך ותלווה את תחום אבטחת המידע והסייבר. צוות אבטחת המידע שהוקם לצורך כך בוועדה ימשיך וייתן מענה שוטף מעת לעת ויבחן את השינויים הטכנולוגיים, ככל שיהיו.