



406 – עמ' 1

הממונה על שיתוף בנתוני אשראי : הוראה למיופה כוח בתמורה  
ניהול סיכוני אבטחת מידע והגנת הסייבר [1] (12/22)

נתוני אשראי  
הקרדיט שמגיע לך



# ניהול סיכוני אבטחת מידע והגנת הסייבר

## תוכן עניינים:

3.....	פרק א' – כללי.....
3.....	מבוא.....
3.....	תחולה.....
4.....	הגדרות.....
6.....	פרק ב' – סיווג לקבוצות, שירות חדש, עריכת ביקורות.....
6.....	סיווג לקבוצות ורמות יישום, שינוי סיווג.....
7.....	עריכת ביקורת.....
7.....	הפעלת שירות חדש באמצעות פלטפורמה דיגיטלית.....
8.....	פרק ג' – דיווחים לממונה.....
8.....	דיווחים שנתיים לממונה.....
8.....	דיווחים מידיים/שוטפים לממונה.....
10.....	דיווחים נוספים שיחולו על מיופה כוח בתמורה המסווג לקבוצה 1.....
11.....	פרק ד' - דרישות שיחולו על מיופה כוח בתמורה הנכלל בקבוצה 1.....
11.....	פרק ה' - דרישות שיחולו על מיופה כוח בתמורה הנכלל בקבוצה 2.....
11.....	אחריות ההנהלה.....
13.....	בקרה וניטור.....
13.....	אבטחת רשת וגישה מרחוק.....
14.....	אבטחת מערכות ועדכון.....
15.....	הפרדה בין סביבות.....
15.....	אימות פרטי הגורם אליו מועבר מידע.....
15.....	גישה למסמכים, הצפנה.....
15.....	ניהול הרשאות ובקרת גישה, וניהול סיסמאות.....
17.....	תכנית היערכות לניהול אירועי אבטחת מידע.....
17.....	אבטחת שרשרת אספקה ומיקור חוץ.....
18.....	מחשוב ענן.....
19.....	אבטחה פיזית וסביבתית.....
20.....	משאבי אנוש והדרכה.....
21.....	עריכת ביקורת תקופתית.....
21.....	שמירה, גיבוי ושחזור של נתונים ומידע.....
21.....	פרק ו' - דרישות נוספות שיחולו על מיופה כוח בתמורה הנכלל בקבוצה 3.....



406 עמ' 2

הממונה על שיתוף בנתוני אשראי : הוראה למיזם כוח בתמורה  
ניהול סיכונים אבטחת מידע והגנת הסייבר (12/22)

נתוני אשראי  
הקרדיט שמגיע לך



- 21..... חובת התאגדות כחברה.
- 21..... אחריות הדירקטוריון.
- 22..... אחריות ההנהלה.
- 23..... סקר סיכונים אבטחת מידע ומבחני חדירה.
- 23..... תהליכי פיתוח ותחזוקה.
- 23..... אבטחת רשת.
- 24..... אבטחת מערכות ועדכון.
- 24..... הפרדה בין סביבות.
- 24..... ניהול הרשאות ובקרת גישה.
- 25..... מניעת דלף מידע ואובדן מידע.
- 25..... שימוש בתעודה דיגיטלית.
- 25..... ניהול משתמשים.
- 25..... תכנית היערכות לניהול אירועי אבטחת מידע.
- 26..... אבטחת שרשרת אספקה ומיקור חוץ.
- 26..... מחשוב ענן.
- 26..... שימוש במכשירים ניידים.
- 27..... מסירת מידע באמצעים דיגיטליים.
- 27..... ניהול סיסמאות לקוח.
- 28..... משאבי אנוש והדרכה.
- 28..... שמירה גיבוי ושחזור של נתונים ונהלים.
- 28..... פרק ז – תחילה.**
- 29..... פרק ח' – מתכונת דיווחים לממונה.**
- 29..... נספח א' – מתכונת דיווח שנתי על סיווג לקבוצה.
- 30..... נספח ב' – מתכונת דיווח על שינוי קבוצת סיווג.
- 31..... נספח ג' – מתכונת דיווח על אירוע משמעותי שהתרחש או כמעט והתרחש, שיש לו השפעה על ניהול המידע והגנתו.
- 32..... נספח ד' – מתכונת דיווח על אירוע צפוי בעל השפעה מהותית על ניהול המידע והגנתו.
- 33..... נספח ה' – מתכונת דיווח על שירות טכנולוגי חדש.

## פרק א': כללי

### 1. מבוא

- 1.1. פעילות מיופה כוח בתמורה מתבטאת לרוב בקבלה ושמירה של דוחות ריכוז נתונים של לקוחות לצורך מתן שירותים עבורם, בהתאם לתקנה 6 בתקנות נתוני אשראי, התשע"ח-2017, וסעיף 13 בכללי נתוני אשראי (הוראות שונות). שירותים אלו עשויים לכלול ייעוץ בתחומי האשראי, לרבות משכנתאות, וההתנהלות הפיננסית של לקוחות. בשל המידע הרגיש אליו נחשף מיופה כוח בתמורה במסגרת השירות ללקוחות, נדרשת אסדרת עקרונות בסיסיים לניהול נכסי המידע וההגנה עליהם.
- 1.2. מתוקף סמכותי לפי סעיף 68 לחוק נתוני אשראי, התשע"ו-2016 (להלן – **החוק**), ולאחר התייעצות עם הוועדה המייעצת, הריני קובע הוראה זו, אשר מסדירה את הניהול וההגנה על נכסי המידע שבידי מיופה כוח בתמורה, וקובעת דרישות ליישום בהיבטי אבטחת מידע והגנת הסייבר לצורך מתן שירותים ללקוחות. זאת, לשם השמירה על עניינם של הלקוחות, הגנה על פרטיותם ובכדי לוודא אבטחת המידע שבידי מיופה הכוח בתמורה באופן אשר ימזער את הסיכון לחשיפה או להעברת המידע לגורמים שאינם מורשים.
- 1.3. מיופי כוח בתמורה נבדלים ביניהם באופן ההתאגדות (כיחיד או כחברה), בשירותים המוצעים על ידם, במורכבות המערכת הטכנולוגית המופעלת על ידם, במספר בעלי ההרשאה, במספר הלקוחות ועוד. נוכח השונות הקיימת בין מיופי הכוח בתמורה השונים, ועל מנת להבטיח את פעילותם התקינה, נקבעו דרישות רגולטוריות מדורגות בנושאי אבטחת מידע, הגנת הסייבר והגנת הפרטיות עבור מיופי כוח בתמורה השונים, התואמות את אופי ואת היקף פעילותם ואת מורכבותה. הדרישות כאמור נקבעו בהתאם למדרג רגולטורי, הכולל שלוש רמות יישום, בהתאם להיקף פעילותם של מיופי הכוח בתמורה ומורכבותה כאמור.
- 1.4. מובהר כי אין בהוראה זו בכדי לגרוע מהוראות הדין, לרבות חוק הגנת הפרטיות, תקנות הגנת הפרטיות (אבטחת מידע) או כל דין רלוונטי אחר.

### 2. תחולה

- 2.1. הוראה זו חלה על מיופה כוח בתמורה במסגרת מתן שירות על ידו לפי החוק.
- 2.2. הממונה רשאי לפטור מיופה כוח בתמורה מסוים מקיום סעיפים מסוימים בהוראה זו, או לקבוע הוראות מסוימות שונות מאלו המפורטות להלן אשר יחולו על מיופה כוח בתמורה מסוים. זאת, במקרים חריגים לאחר שבחן את בקשתו ונימוקיו אשר נמסרו לו בכתב, ורשאי הממונה לקבוע כי הפטור או ההוראות השונות יחולו לתקופה קצובה, כפי שתיקבע על ידו.



406 עמ' 4

הממונה על שיתוף בנתוני אשראי : הוראה למיופה כוח בתמורה  
ניהול סיכוני אבטחת מידע והגנת הסייבר (12/22)

נתוני אשראי  
הקרדיט שמגיע לך



3.

### הגדרות

בהוראה זו -

- **"אבטחת מידע"** אבטחה והגנה על סודיות, שלמות או זמינות של מידע, לרבות אבטחה והגנה מפני תקיפת מערכות המידע ;
- **"בעל הרשאה"** כהגדרתו בתקנות הגנת הפרטיות (אבטחת מידע) ;
- **"הנהלה"** הנהלת מיופה כוח בתמורה, ובמקרה שבו מדובר במיופה כוח בתמורה שהוא יחיד - היחיד עצמו ;
- **"חוק הגנת הפרטיות"** חוק הגנת הפרטיות, תשמ"א-1981, כפי שיתעדכן מעת לעת ;
- **"כללי נתוני אשראי (הוראות שונות)"** כללי נתוני אשראי (הוראות שונות), התשע"ז-2017 ;
- **"יום עסקים"** ימים א'-ה', למעט : ימי שבתון, שני ימי ראש השנה, ערב יום כיפור ויום כיפור, ראשון של סוכות ושמיני עצרת, פורים, ראשון ושביעי של פסח, יום העצמאות, חג השבועות ותשעה באב ;
- **"מאגר מידע"** כהגדרתו בחוק הגנת הפרטיות ;
- **"לקוח"** אדם שיש למיופה הכוח בתמורה מידע אודותיו, שמקורו ממאגר נתוני אשראי, אשר התקבל מלשכות האשראי, או מאותו אדם ישירות.
- **"מידע רגיש"** כהגדרתו בחוק הגנת הפרטיות, וכל מידע אחר אשר סווג על ידי מיופה כוח בתמורה כמידע רגיש לעניין הוראה זו ;
- **"מערכות מידע"** המערכות הטכנולוגיות 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, כלי פיתוח ואמצעי אבטחה ;
- **"נכסי מידע"** מאגר נתונים, התקן, או רכיב של סביבה התומך בפעילויות הקשורות במידע (לרבות תשתיות), חומרה, תוכנה ומידע ;



- "נתיב בקרה"**
- תיעוד פעולות המתבצעות במערכות מידע, אשר מקשר את הפעולה לנתונים, כגון : שם מבצע הפעולה, המועד, הפעולה עצמה ועוד לצורך זיהוי האלמנטים שהשתנו ;
- "ספק מהותי"**
- גורם חיצוני הנכלל בשרשרת האספקה של מיופה הכוח בתמורה המספק שירותים מהותיים לפעילותו בתחומים הקשורים לטכנולוגיית המידע או החושפים אותו לסיכוני אבטחת מידע פוטנציאליים בהיבטי סודיות המידע, שלמות המידע או זמינותו ;
- "פלטפורמה דיגיטלית"**
- פלטפורמה למתן שירותים ללקוחות באמצעות אינטרנט או רשת סלולרית (לדוגמה, אפליקציה), לרבות תוך שימוש בכלים טכנולוגיים לצורך עיבוד הנתונים והצגתם ;
- "קוד עיון"**
- קוד המושתל על ידי משתמש זדוני ועשוי לגרום לביצוע פעולות לא רצויות, פגיעה במערכות, ודלף מידע רגיש לגורמים לא מורשים ;
- תהליך הליך Multi-Factor Authentication (MFA)**
- תהליך אימות המורכב משני גורמי אימות לפחות מ-2 קטגוריות שונות. לעניין זה, גורם אימות הנו אחד מאלה :
    - (1) פריט הנמצא ברשות המשתמש (לדוגמה : סיסמה חד-פעמית זמנית (OTP-One Time Password) הנוצרת על ידי רכיב חומרה הנמצא בידי המשתמש ומקושר לחשבון שלו, סיסמה חד פעמית זמנית הנוצרת על ידי נתן השירות ומועברת ללקוח על ידי מסרון ולעניין זה לרבות מסרון קולי, או תעודה דיגיטלית הנשמרת בכרטיס חכם או רכיב אחר אשר ברשות המשתמש) ;
    - (2) פריט הידוע רק למשתמש (לדוגמה : סיסמה קבועה) ;
    - (3) פריט שהוא המשתמש, לרבות מאפיין ביומטרי, כגון : זיהוי קולי, טביעת אצבע וזיהוי פנים.
- "תעודה דיגיטלית"**
- אישור אלקטרוני שמקשר את הזהות של בעל התעודה לצמד מפתחות הצפנה (אחד פרטי ואחד ציבורי) שבאמצעותם ניתן להצפין ולחתום דיגיטלית מידע ;
- תקנות הגנת הפרטיות (אבטחת מידע)**
- תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017.



406 עמ' 6

הממונה על שיתוף בנתוני אשראי: הוראה למיופה כוח בתמורה  
ניהול סיכונים אבטחת מידע והגנת הסייבר (12/22)



## פרק ב' – סיווג לקבוצות, שירות חדש, עריכת ביקורות

### 4. סיווג לקבוצות ורמות יישום, ושינוי סיווג

4.1. מיופה כוח בתמורה יישם הוראה זו, בהתאם לקבוצה אליה הוא מסווג על פי הכללים שלהלן. בעבור כל אחת מהקבוצות הוגדרה בהוראה רמת יישום שונה של דרישות בתחום ניהול המידע, אבטחת המידע והגנת הסייבר, בהתאם למספר בעלי ההרשאה, מספר הלקוחות ומהות השירותים המסופקים על ידי מיופה הכוח בתמורה, וכן בהתאם למספר דוחות ריכוז נתונים שנמשכו על ידו במהלך כל אחד מתוך ארבעת הרבעונים הקלנדריים האחרונים, והכל כמפורט להלן:

4.1.1. קבוצה 1 (רמת יישום בסיסית): בקבוצה זה ייכלל מיופה כוח בתמורה שמתקיימים לגביו כל התנאים המפורטים להלן (ככל שאחד התנאים לא מתקיים נדרש לבחון שיוך לקבוצה הבאה):

(א) מספר בעלי ההרשאה בו אינו עולה על 10.

(ב) מספר לקוחותיו אינו עולה על 300.

(ג) מספר דוחות ריכוז הנתונים שמשך מיופה הכוח בתמורה במהלך כל אחד מתוך ארבעת הרבעונים הקלנדריים האחרונים, אינו עולה על 1,000.

(ד) מיופה הכוח בתמורה אינו מספק שירות ללקוחותיו באמצעות פלטפורמה דיגיטלית. על מיופה כוח בתמורה שנכלל בקבוצה זו, יחולו הוראות פרקים א, ב, ג, ד, ז, ח'.

4.1.2. קבוצה 2 (רמת יישום בינונית): בקבוצה זה ייכלל מיופה כוח בתמורה שאינו נכלל בקבוצה 1 ומתקיימים לגביו כל התנאים המפורטים להלן (ככל שאחד התנאים לא מתקיים, מיופה הכוח בתמורה ייכלל בקבוצה 3):

(א) מספר בעלי ההרשאה בו אינו עולה על 100.

(ב) מספר לקוחותיו אינו עולה על 10,000.

(ג) מספר דוחות ריכוז הנתונים שמשך מיופה הכוח בתמורה במהלך כל אחד מתוך ארבעת הרבעונים הקלנדריים האחרונים, אינו עולה על 10,000.

(ד) מיופה הכוח בתמורה אינו מספק שירות ללקוחותיו באמצעות פלטפורמה דיגיטלית. על מיופה כוח בתמורה שנכלל בקבוצה זו, יחולו הוראות פרקים א, ב, ג, ה, ז, ח'.

4.1.3. קבוצה 3 (רמת יישום גבוהה): בקבוצה זה ייכלל מיופה כוח בתמורה שמתקיימים לגביו אחד או יותר מהתנאים הבאים:

(א) מספר בעלי ההרשאה בו עולה על 100.

(ב) מספר לקוחותיו עולה על 10,000.

(ג) מספר דוחות ריכוז נתונים שמשך מיופה הכוח בתמורה במהלך כל אחד מתוך ארבעת הרבעונים הקלנדריים האחרונים, עולה על 10,000.

(ד) מיופה כוח בתמורה מספק שירות ללקוחותיו באמצעות פלטפורמה דיגיטלית. על מיופה כוח בתמורה שנכלל בקבוצה זו, יחולו הוראות פרקים א, ב, ג, ה, ו, ז, ח'.



406 עמ' 7

הממונה על שיתוף בנתוני אשראי: הוראה למיופה כוח בתמורה  
ניהול סיכונים אבטחת מידע והגנת הסייבר (12/22)

נתוני אשראי  
הקרדיט שמגיע לך



- 4.2. הסיווג לקבוצה הרלוונטית יבחן על ידי מיופה כוח בתמורה באופן שוטף. מיופה כוח בתמורה יתעד את הבחינה שבוצעה על ידו בנוגע לסיווג לקבוצה הרלוונטית, לפחות אחת לחודש, וישמור אותה ואת המסמכים ששימשו להכנתה, למשך תקופה של 36 חודש לכל הפחות.
- 4.3. בעת שינוי סיווג מקבוצה אחת לקבוצה אחרת, שחלות עליה דרישות מחמירות יותר, מיופה כוח בתמורה יעביר דיווח לממונה כמפורט בסעיף 8.1, ותחול לגבי מיופה כוח בתמורה כאמור תקופת מעבר ליישום הדרישות הנוספות כמפורט להלן:
- 4.3.1. בעת מעבר מקבוצה 1 לקבוצה 2 או 3, תחול תקופת מעבר של 6 חודשים.
- 4.3.2. בעת מעבר מקבוצה 2 ל-3, תחול תקופת מעבר של 3 חודשים.

## 5. עריכת ביקורת

- 5.1. אחת ל-18 חודשים לפחות, תיערך ביקורת על ידי מבקר לפי כללים מקובלים, על פעילות מיופה הכוח בתמורה בהתאם למפורט להלן:
- 5.1.1. לגבי מיופה כוח בתמורה הנכלל בקבוצה 1 – תיערך ביקורת בהתאם לסעיף 11. ביקורת ראשונה תבצע לא יאוחר מ-3 חודשים ממועד רישומו של מיופה הכוח בתמורה במרשם הממונה, ולאחר מכן, כל 18 חודשים לפחות.
- 5.1.2. לגבי מיופה כוח בתמורה הנכלל בקבוצה 2 או 3 – תיערך ביקורת בהתאם לסעיפים 97 עד 99. ביקורת ראשונה תבצע לא יאוחר מתום חצי השנה הראשונה ממועד רישומו של מיופה הכוח בתמורה במרשם הממונה, ולאחר מכן, כל 18 חודשים לפחות.
- במקרה בו חל שינוי סיווג לקבוצה עם דרישות מחמירות יותר, בהתאם לסעיף 4, השלמת ביקורת ראשונה תיערך במהלך השנה הראשונה לאחר מועד שינוי הסיווג כאמור.
- 5.2. "מבקר" בהוראה זו הינו מי שמתקיימים בו כל אלו:
- 5.2.1. יחיד בעל ניסיון של לפחות 3 שנים בביצוע ביקורות טכנולוגיות;
- 5.2.2. אינו מצוי בניגוד עניינים או תלות בקשר עם עריכת הביקורת, למעט קבלת שכר עבור עבודתו; היה המבקר עובד או שותף בתאגיד – לא יהיה ניגוד עניינים או תלות בקשר גם בין התאגיד לבין עריכת הביקורת;
- 5.2.3. תושב ישראל;
- 5.2.4. בעל תואר אקדמי רלוונטי ממוסד להשכלה גבוהה בישראל המוכר על ידי המועצה להשכלה גבוהה;
- 5.2.5. בעל הסמכה בביקורת מערכות מידע או באבטחת מערכות מידע שהיא כדוגמת אחת מבין ההסמכות הבאות: CRISC; CISA; או רואה חשבון מוסמך בישראל בעל התמחות במערכות מידע.
- 5.3. דוח הביקורת והמסמכים ששימשו להכנתו יישמרו אצל מיופה הכוח בתמורה למשך תקופה של 7 שנים, לכל הפחות.



## 6. הפעלת שירות חדש באמצעות פלטפורמה דיגיטלית

- 6.1. מיופה כוח בתמורה ידווח לממונה על הפעלת שירות חדש באמצעות פלטפורמה דיגיטלית לפחות 90 יום מראש, בהתאם לסעיף 8.4, ויהיה רשאי להפעילו ובלבד שהממונה לא התנגד לכך בתקופה זו. מיופה הכוח בתמורה יודא עמידתו בהוראות נוספות של הממונה בנוגע לשירות החדש, ככל שקיימות. לעניין זה, "שירות חדש" – שירות ייעוץ פיננסי בתחום האשראי, בהתאם לסעיף 13(ב) בכללי נתוני אשראי (הוראות שונות), לרבות פעילות או שירות חדש וכן שינויים משמעותיים או הרחבה משמעותית של פעילות או שירות קיימים.
- 6.2. דירקטוריון מיופה כוח בתמורה וכן ההנהלה, יקיימו דיון במסגרתו יבחן השירות החדש, לרבות תוצאות סקר הסיכונים כמפורט בסעיף 6.3, ויאשרו את השירות החדש בטרם יועבר דיווח כאמור על ידי מיופה הכוח בתמורה לממונה.
- 6.3. טרם אישור השירות החדש בהתאם להוראות סעיף 6.2, יערוך מיופה הכוח בתמורה סקר סיכונים אשר ימפה את כלל הסיכונים הכרוכים בפעילות, תוך מתן דגש לסיכוני אבטחת מידע והגנת הפרטיות, ויקבע את הכלים, האמצעים והתהליכים לניטור ובקרה במטרה לצמצם.
- 6.4. בתום השנה הראשונה להפעלת השירות החדש, יתקיים תהליך להערכת הסיכונים ונאותות השירות, ביחס להערכות המוקדמות שנעשו בעת אישור השירות, ויבוצעו התאמות בתהליכי ניהול הסיכונים במידת הצורך.

## פרק ג' – דיווחים לממונה

### 7. דיווחים שנתיים לממונה

#### 7.1. מידע על היקפי הפעילות, וסיווג קבוצה

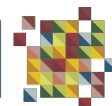
- לא יאוחר מ-30 ימים מתום כל שנה קלנדרית, מיופה כוח בתמורה יעביר לממונה דיווח לגבי:
- 7.1.1. מספר בעלי ההרשאה.
- 7.1.2. מספר לקוחותיו.
- 7.1.3. מספר דוחות ריכוז הנתונים שנמשכו על ידי מיופה הכוח בתמורה בכל אחד מהרבעונים בשנת הדיווח הקלנדרית.
- 7.1.4. הקבוצה אליה משתייך מיופה הכוח בתמורה לפי סעיף 4.1 לעיל.
- הדיווח יועבר בהתאם למתכונת הדיווח **בנספח א'**.

### 8. דיווחים מיידיים/שוטפים לממונה

#### 8.1. דיווח על שינוי סיווג קבוצה

- מיופה כוח בתמורה יעביר לממונה דיווח על שינוי סיווג מקבוצה אחת לקבוצה אחרת, שחלות עליה דרישות מחמירות יותר בהתאם לסעיף 4.3, לא יאוחר מ-30 ימים מהמועד בו נדרש שינוי הסיווג, ויפרט את הסיבה לשינוי סיווג הקבוצה.
- הדיווח יועבר בהתאם למתכונת הדיווח **בנספח ב'**.





## 8.2. דיווח על אירוע משמעותי שהתרחש או כמעט והתרחש בתחום ניהול המידע והגנתו

8.2.1. מיופה כוח בתמורה יעביר דיווח לממונה במקרים הבאים, הקשורים לפעילותו כמיופה כוח בתמורה:

- 8.2.1.1. אירוע הכולל פגיעה בשלמות המידע.
- 8.2.1.2. אירוע שנעשה בו שימוש במידע או גישה למידע או העברת מידע בלא הרשאה או בחריגה מהרשאה.
- 8.2.1.3. אירוע שבמסגרתו נפגעו או הושבתו מערכות מידע בסביבת הייצור המכילות מידע רגיש ליותר מ-3 שעות, למעט השבתה יזומה; ואולם חובת הדיווח במקרה זה לא תחול על מיופה כוח בתמורה השייך לקבוצה 1.
- 8.2.1.4. קיימת אינדיקציה לכך שמידע רגיש אודות לקוחות נחשף או דלף אל מחוץ לחצרות מיופה הכוח בתמורה.
- 8.2.1.5. התממשות אירוע חריג אחר, לרבות ניסיונות מהותיים של חדירה ותקיפה, חדירה בפועל למערכות מידע, קריסה של מערכות מידע מרכזיות, הפעלת תכנית להתמודדות עם אירועים חריגים.
- 8.2.1.6. אירוע אשר הטיפול בו דורש מעורבות משמעותית של הגורם האמון על אבטחת מידע או ממונה אבטחת מידע, לפי העניין, ואשר הטיפול בו לא הסתיים תוך שעתיים ממועד זיהויו לראשונה.
- 8.2.1.7. אירוע שהינו בעל מאפייני תקיפה חדשים או רמת מורכבות גבוהה.
- 8.2.1.8. הונאה אצל מיופה הכוח בתמורה.
- 8.2.1.9. אירוע משמעותי אחר שהתרחש ויש לו השפעה מהותית על ניהול המידע והגנתו.
- 8.2.1.10. כל אירוע כמפורט לעיל שכמעט והתרחש.
- 8.2.1.11. סיום או הפסקת פעילות.

8.2.2. דיווח על אירוע משמעותי שהתרחש יועבר לממונה טלפונית או בכתב תוך שעתיים ממועד הזיהוי הראשוני של האירוע כמחייב דיווח (להלן – **דיווח ראשוני**). השלמת הדיווח תתבצע בכתב בתוך 8 שעות ממועד הדיווח הראשוני (להלן – **דיווח משלים**). אם מועד הדרישה להשלמת הדיווח בכתב חל שלא בשעות העבודה המקובלות (שעות עבודה מקובלות הינם ימים א'-ה' שהינם ימי עסקים, בין השעות 08:00 ל-18:00) הוא יועבר בכתב עם תחילת שעות העבודה המקובלות של היום העוקב. הדיווח הראשוני והדיווח המשלים כאמור, יכללו את הפרטים הידועים נכון למועד מסירת הדיווח.  
ככל שתהיינה התפתחויות מהותיות במהלך האירוע, על מיופה הכוח בתמורה לעדכן את הממונה על התפתחויות אלו.

כמו כן, מיופה כוח בתמורה יעדכן את הממונה על סיום האירוע.

8.2.3. דיווח בכתב על אירוע שכמעט והתרחש יועבר לממונה תוך 7 ימים ממועד הזיהוי הראשוני של האירוע.



- 8.2.4. מיופה הכוח בתמורה ידווח לממונה על תוצאות התחקיר שבוצע בעקבות המקרים המפורטים בסעיף 8.2.1, ועל הלקחים והפעולות שבוצעו בעקבותיהם ככל שנדרש. דיווח כאמור יועבר תוך 45 ימים מהמועד שהאירוע הסתיים או תוך 60 יום ממועד הזיהוי הראשוני, לפי המוקדם מביניהם.
- 8.2.5. למען הסר ספק, דיווח לממונה בקרות אירוע אבטחת מידע אינו גורע מחובת הדיווח לגורמים שנדרש לדווח להם בהתאם להוראות הדין, לרבות דיווח לרשות להגנת הפרטיות בהתאם לתקנות הגנת הפרטיות (אבטחת מידע). בנוסף, הממונה רשאי להורות למיופה הכוח בתמורה להודיע לגורמים נוספים על אירוע האבטחה בהתאם לנסיבות.
- הדיווחים יועברו בהתאם למתכונת הדיווח **בנספח ג'**.
- 8.3. דיווח על אירוע צפוי בעל השפעה מהותית על ניהול המידע והגנתו**
- מיופה כוח בתמורה יעביר לממונה, מראש ולא יאוחר מ-30 ימים טרם האירוע, דיווחים לגבי אירוע צפוי בעל השפעה מהותית על ניהול המידע והגנתו, לדוגמה:
- 8.3.1. שינויים מהותיים צפויים במדיניות או בנהלי אבטחת המידע.
- 8.3.2. הסבה מהותית של מערכות מידע או שינוי מהותי במערכות המידע.
- 8.3.3. שינוי מהותי בערוצי התקשורת.
- 8.3.4. כל נושא אחר בעל השפעה מהותית על ניהול המידע והגנתו.
- הדיווח יועבר בהתאם למתכונת הדיווח **בנספח ד'**.
- 8.4. דיווח על הפעלת שירות חדש באמצעות פלטפורמה דיגיטלית**
- מיופה כוח בתמורה יעביר לממונה לפחות 90 יום מראש, דיווח על שירות חדש שבכוונתו להפעיל באמצעות פלטפורמה דיגיטלית, בהתאם לאמור בסעיף 6, תוך פירוט הנושאים הבאים:
- 8.4.1. מהות השירות החדש.
- 8.4.2. תיעוד הדיון בהנהלה ובדירקטוריון, לגבי השירות החדש ואישור הדירקטוריון לשירות החדש.
- 8.4.3. סקר סיכונים הגלומים בשירות החדש והמענה שניתן להם, כמפורט בסעיף 6.3.
- 8.4.4. ככל שרלוונטי - עיקרי השינויים הצפויים בעקבות יישום דרישות נוספות לאור שינוי הסיווג לקבוצה מחמירה יותר, ותכנית עבודה לעמידה בדרישות.
- הדיווח יועבר בהתאם למתכונת הדיווח **בנספח ה'**.
- 9. דיווח נוסף שיחול על מיופה כוח בתמורה המסווג לקבוצה 1**
- מיופה כוח בתמורה המסווג לקבוצה 1 יעביר לממונה **אישור מבקר**, בדבר עמידתו בדרישות תקנות הגנת הפרטיות (אבטחת מידע) על מאגר שחלה עליו רמת אבטחה בסיסית לכל הפחות, בהתאם למפורט בסעיף 11 לפרק ד'.
- אישור המבקר יועבר לממונה לראשונה לא יאוחר מ-3 חודשים מיום רישומו של מיופה הכוח בתמורה במרשם הממונה, ולאחר מכן, כל 18 חודשים לפחות.



## פרק ד' - דרישות שיחולו על מיופה כוח בתמורה הנכלל בקבוצה 1

### מיופה כוח בתמורה הנכלל בקבוצה 1 יישם את הדרישות שלהלן:

10. יעמוד בכל עת בדרישות הקבועות בתקנות הגנת הפרטיות (אבטחת מידע) לעניין מאגר שחלה עליו רמת האבטחה הבסיסית, לכל הפחות.
11. תיערך ביקורת על ידי מבקר, בהתאם למפורט בסעיף 5 לפרק ב' בדבר עמידת מיופה הכוח בתמורה בהוראות תקנות הגנת הפרטיות (אבטחת מידע) לעניין מאגר שחלה עליו רמת האבטחה הבסיסית, לכל הפחות. לדוח הביקורת יצורף אישור המבקר בדבר עמידה בתקנות כאמור. האישור יועבר לממונה בהתאם למפורט בסעיף 9.
12. בנוסף, מיופה כוח בתמורה יודא באופן שוטף עמידתו בדרישות הנוספות הכלולות בהוראה זו, ויתעד בדיקתו זו אחת לתקופה.

## פרק ה' - דרישות שיחולו על מיופה כוח בתמורה הנכלל בקבוצה 2

### מיופה כוח בתמורה הנכלל בקבוצה 2 יישם את הדרישות שלהלן:

#### 13. אחריות ההנהלה

- ההנהלה תפעל לקידום וחיזוק מערך אבטחת המידע המשמש את פעילות מיופה הכוח בתמורה, בין היתר באמצעות:
- 13.1. מינוי גורם ייעודי שיהיה אמון על תחום אבטחת המידע. יובהר כי הגורם כאמור אינו חייב להיות עובד של מיופה הכוח בתמורה.
  - 13.2. הגדרת מדיניות ונהלי עבודה לניהול סיכונים אבטחת מידע.
  - 13.3. הקצאת משאבים הולמים לצורך מתן מענה לדרישות אבטחת מידע.
  - 13.4. הגדרת תכנית עבודה שנתית, לרבות יעדים לביצוע בהיבטי אבטחת מידע.
  - 13.5. פיקוח ואכיפת היישום של המדיניות והנהלים, תכניות העבודה והנחיות ההנהלה בנושאי אבטחת מידע.
14. מסמך המדיניות כאמור בסעיף 13.2 יכלול, בין היתר, התייחסות לנושאים הבאים:
- 14.1. תיאור כללי של פעולות האיסוף והשימוש במידע ושל מטרות השימוש במידע.
  - 14.2. סוגי המידע השונים הכלולים במאגר המידע.
  - 14.3. הסיכונים העיקריים לפגיעה באבטחת המידע והגנת הסייבר, אופן קביעתם ואופן ההתמודדות עמם.
  - 14.4. נושאים שהוגדרו על ידי בעל מאגר מידע במסמך "הגדרות המאגר" כמפורט בסעיפים 2(א) ו-4(א), 2(א) ו-7(א) בתקנות הגנת הפרטיות (אבטחת מידע).
15. הנהלים כאמור בסעיף 13.2 יכללו, בין היתר, התייחסות לנושאים הבאים כמפורט להלן:
    - 15.1. כלל הגורמים מורשי הגישה למערכות המידע, לרבות גורמים הפועלים במיקור חוץ.
    - 15.2. אבטחה פיזית וסביבתית.
    - 15.3. ניהול הרשאות גישה.
    - 15.4. אמצעי הגנה על מערכות המידע והרשת הארגונית.



- 15.5. הנחיות לבעלי ההרשאה בהיבטי אבטחת מידע והגנת הפרטיות.
- 15.6. אופן התמודדות עם אירועי אבטחת מידע.
- 15.7. הוצאת מידע רגיש באופן מאובטח.
- 15.8. מחיקת נתונים.
- 15.9. ניהול שינויים ופיתוחים באופן מאובטח, לרבות הנחיות תיעוד רלוונטיות וגישת אנשי פיתוח לנתונים במאגר.
- 15.10. תהליכי בקרה וניטור ותיעוד הגישה למערכות המידע.
- 15.11. עריכת ביקורת תקופתית.
- 15.12. דרישות הגנת מידע בהתייחס לסיכונים מיקור חוץ ואבטחת שרשרת אספקה.
- 15.13. אמצעי הזיהוי והאימות לגישה למאגר ולמערכות המידע, לרבות תוך התייחסות לנושאים הבאים :
- 15.13.1. מתן גישה מרחוק.
- 15.13.2. מדיניות הסיסמאות.
- 15.13.3. ניתוק החיבור למערכות מידע לאחר חוסר פעילות זמני.
- 15.13.4. אופן הטיפול בתקלות הקשורות באימות זהות.
- 15.14. הוראות לגבי גיבויים ושחזורים, ובכלל זה :
- 15.14.1. גיבוי נתונים באופן תקופתי.
- 15.14.2. שחזור נתונים באישור הנהלת מיופה הכוח בתמורה.
- 15.14.3. תיעוד הליכי שחזור המידע במסגרת אירוע אבטחה, לרבות זהות הגורם שביצע את השחזור ופרטי המידע ששוחזר.
- 15.15. הוראות לשימוש נאות בהתקנים ניידים, ככל שרלוונטי.
16. ההנהלה תדון בעדכון מסמך המדיניות והנהלים ותאשר אותם :
- 16.1. לפחות אחת לשנה.
- 16.2. בעת ביצוע שינוי מהותי במערכות המידע או בתהליכי העבודה.
- 16.3. כאשר נודע על חשיפה לסיכונים טכנולוגיים חדשים הנוגעים למערכות המידע.
- 16.4. לאחר אירוע אבטחת מידע משמעותי.
17. לפחות אחת לשנה, ההנהלה תבחן האם אין המידע שנשמר במאגר רב מהנדרש לצורך עמידה במטרות המאגר ודרישות החוק.
18. מיופה הכוח בתמורה יחזיק מסמך מעודכן של מבנה מאגרי המידע, רשימת מערכות המידע, ארכיטקטורת השירותים והשרתים, ותרשים הרשת.
19. פרטים מהמדיניות, מהנהלים, ממסמך מבנה מאגרי המידע ומערכות המידע כאמור, ימסרו רק לגורמים בעלי ההרשאות המתאימות, בהיקף הנדרש לצורך ביצוע תפקידיהם.
20. הגורם מטעם ההנהלה שאמון על תחום אבטחת המידע, יכין תכנית לבקרה שוטפת, יבצע אותה ויודיע להנהלה על ממצאיו.



21. ככל שבמיופה הכוח בתמורה קיים דירקטוריון, חובות ההנהלה שבסעיפים לעיל, ייושמו על ידי הדירקטוריון בהתאמות הנדרשות.

### בקרה וניטור

22. עבור כל הפעולות המתבצעות במערכות המידע ובתשתיות, שתומכות באופן ישיר או עקיף במאגר המידע ומנהלות מידע רגיש על לקוחות, ובמערכות מידע שרמת החשיפה שלהן לביצוע פעילות בלתי מורשית הינה גבוהה, לרבות פעולות המבוצעות בעת גישה מרחוק, מיופה כוח בתמורה יישם מנגנון תיעוד אוטומטי.
23. מיופה כוח בתמורה יידע את בעלי ההרשאות הרלוונטיים בדבר קיומו של מנגנון כאמור.
24. המנגנון יפיק נתיב בקרה (AUDIT LOG) שיוגן מפני שינויים בלתי מורשים ויאתר ניסיונות לביצוע שינויים בלתי מורשים כאמור. נתיב הבקרה ישמר ל-24 חודשים לפחות ויתייחס לנושאים הבאים:
- 24.1. חשבון המשתמש ושם העובד.
- 24.2. תאריך ושעה של ניסיון הגישה למאגר המידע ולמערכות המידע.
- 24.3. רכיב המערכת אליו בוצע ניסיון הגישה (שם המערכת, השרת שאליו בוצעה הגישה וכיו"ב).
- 24.4. סוג הגישה שבוצעה – צפייה במאגר המידע, עדכון, מחיקת או העתקת נתונים.
- 24.5. היקף הגישה, והאם הגישה אושרה או נדחתה.
25. יופעל מערך לניטור מערכות המידע (להלן - "מערך SIEM"), הכולל קבלת דיווחים בזמן אמת ממערכות המידע השונות אודות חשש לאירועים חריגים הנוגעים לאיומים על המידע בגין פעולות שמקורן מחוץ לחצרות מיופה הכוח בתמורה או בתוכן. מערך ה-SIEM יופעל על ידי מיופה הכוח בתמורה באופן עצמאי, או באמצעות קבלת שירות על ידי ספק חיצוני בעל ניסיון ויכולת, בתנאי שהספק עומד בדרישות מיופה הכוח בתמורה לביצוע ניטור ומתריע מוקדם ככל האפשר על אירועים חריגים.
26. מערך ה-SIEM יאפשר בקרה על הגישה למערכות המידע ולתשתיות, ועל פעולות המעלות חשש לפגיעה בשלמות המידע, שימוש בו ללא הרשאה או חריגה מההרשאה.
27. ככל שיתקיים ניסיון לעדכון או מחיקת נתיב בקרה, תופק על כך התראה בתפוצה רחבה לידי גורמים רלוונטיים.
28. מיופה כוח בתמורה יישם תהליך שוטף של סקירת נתיבי הבקרה באופן ידני או ממוכן ועריכת דוח לגבי הבעיות שהתגלו.

### אבטחת רשת וגישה מרחוק

29. מיופה כוח בתמורה יגדיר כלים המסדירים תעבורת רשת (יוצאת ונכנסת), בכפוף לחוקים והגדרות אשר מותאמים לאופי פעילותו ומאפייני התעבורה (לרבות התקנת חומת אש - Firewall ותחזוקתה באופן שוטף).
30. מיופה כוח בתמורה יטמיע אמצעי אבטחה (לרבות אנטי וירוס) לזיהוי ומניעת קוד עוין במערכות המידע. אמצעי האבטחה האמורים יכללו מספר שכבות אבטחה כגון: סינון תקשורת וקבצים נכנסים, הגנה בזמן אמת על שרתים או תחנות קצה, ומערכות ניטור ומניעה ייעודיות. מיופה כוח בתמורה יעדכן בתדירות גבוהה את גרסאות אמצעי האבטחה האמורים לעיל.



31. ככלל, מיופה כוח בתמורה יחסום אפשרות לחיבור התקן זיכרון חיצוני (לרבות USB, DISC ON KEY) למחשבים. במקרים בהם יוחלט כי קיימת הצדקה עסקית לשימוש בהתקן זיכרון חיצוני, יש לקיים מנגנוני הגנה ובקורות אפקטיביים שימנעו דלף מידע או החדרת קוד עיון, בשים לב לסיכונים המיוחדים הקשורים לשימוש בהתקן זיכרון חיצוני באותם מחשבים, ובכלל זאת:
- 31.1. ניהול "רשימה לבנה" מרכזית של אמצעים מורשים לחיבור.
- 31.2. שימוש בהתקן זיכרון חיצוני שנרכש על ידי מיופה הכוח בתמורה בלבד, והכולל טכנולוגיית הצפנת מדיה נתיקה.
- 31.3. שימוש בעמדת הלבנת קבצים טרם חיבור התקן זיכרון חיצוני למחשבים ולאחר כל שימוש בו.
- 31.4. ניטור והתראה על חיבור או ניסיון חיבור של התקן זיכרון חיצוני למחשבים.
- 31.5. איסור להעסקת נתוני אשראי ממחשב של מיופה הכוח בתמורה להתקן זיכרון חיצוני.
32. מיופה כוח בתמורה יודא באופן תדיר כי ננקטים אמצעים לצמצום החשיפה לסיכוני אבטחת מידע והגנת הסייבר במערכות המידע ובתשתיות, ובכלל זאת:
- 32.1. חסימת ערוצי תקשורת (פורטים) שאינם נחוצים לביצוע הפעילות השוטפת.
- 32.2. כיבוי שרתים/ נטרול תהליכים שאינם נחוצים או לא בשימוש.
- 32.3. הסרה או חסימה של חשבונות משתמש אורח, לרבות חשבונות ברירת מחדל, ושל חשבונות משתמש של עובדים שעזבו.
- 32.4. שימוש בפרוטוקולי תקשורת מאובטחים.
- 32.5. חסימת האפשרות להתקנת תוכנות (אפליקציות) על ידי משתמשים שאינם מורשים בתחנות קצה.
33. בדיקה כי ננקטו אמצעים לצמצום החשיפה לסיכוני אבטחת מידע והגנת הסייבר תבצע על ידי הגורם האמון על אבטחת המידע במיופה הכוח בתמורה, או לחילופין, ניתן להיעזר בספק המחשוב האמון על שירותי המחשוב אצל מיופה הכוח בתמורה ולקבל הצהרה חוזית המעידה על ביצוע הבדיקות הרלוונטיות.
34. לצורך גישה למערכות מידע שהוערכו כבעלות סיכון גבוה, ובמקרים שבהם מבוצעת התחברות מרוחק למערך טכנולוגיות המידע, תבוצע הזדהות תוך שימוש בתהליך Multi-Factor Authentication (MFA).
35. מיופה כוח בתמורה יקפיד על ניהול ותפעול תקין של מערכות המאגר.

#### אבטחת מערכות ועדכון

36. מיופה כוח בתמורה יבחן באופן שוטף את עדכניות מערכות המידע, לרבות כלי אבטחה שונים, תוך הקפדה על יישום עדכוני אבטחה שוטפים לצורך עמידה במדיניות יצרן המערכת, וזאת על מנת להבטיח כי מערכת המידע הינה בתוקף ונתמכת על ידי היצרן. לא יעשה שימוש במערכות שהיצרן לא תומך בהיבטי אבטחה שלהן, אלא אם כן ניתן מענה אבטחתי מתאים.
37. לצורך בחינה של עדכניות מערכות המידע, ניתן להיעזר בגורם האמון על תחום אבטחת מידע אצל מיופה הכוח בתמורה. לחילופין, ניתן להיעזר בספק המחשוב האמון על שירותי המחשוב אצל מיופה הכוח בתמורה ולקבל הצהרה חוזית המעידה על ביצוע הבדיקות הרלוונטיות.



38. בעת ביצוע שינויים מהותיים במערכות המידע, יבוצע סקר לאיתור כשלי אבטחת מידע בארכיטקטורת הרשת, החוקים ואופן ההגדרה של רכיבי הרשת והתקשורת השונים, ככל שרלוונטי, וזאת על ידי גורם בלתי תלוי בעל מומחיות.

39. מיופה כוח בתמורה יטמיע חוקים יעודיים במערכות ההגנה, הבקרה והניטור. אחת לשנה וכן בעת ביצוע שינויים מהותיים ברשתות ובמערכות המידע, מיופה כוח בתמורה יערוך תהליך טיוב של החוקים שהוגדרו כאמור, ובמסגרת זו יוודא בין היתר התאמת החוקים לשינויים טכנולוגיים, רגולטוריים ועסקיים, לרבות היקפי פעילות משתנים.

לעניין סעיפים 38 ו-39, "שינויים מהותיים" - לרבות הוספת ממשקים, הוספה או גריעה של בקרת אבטחה ברשת, החלפת טכנולוגיות חומרה או תוכנה, מעבר אל שירותי הוסטינג או מהם, העברת התמיכה והשירות ברשת וברכיבי ליבה לספק חיצוני, שינויי קונפיגורציה מהותיים הנוגעים לאבטחת רשת/מערכת, פריצה או חשד לפריצה לרשת/מערכת וכדומה.

#### הפרדה בין סביבות

40. סביבת הייצור תופרד מסביבות אחרות ככל שקיימות, כגון פיתוח ובדיקות. כל גישה מסביבת הייצור תסונן על ידי מערכת חומת אש (Firewall), או אמצעי סינון תעבורה דומה.

41. הפרדת הסביבות תתייחס גם לתשתיות עזר תומכות סביבת התקשוב, ככל שקיימות.

#### אימות פרטי הגורם אליו מועבר מידע

42. מיופה כוח בתמורה יוודא שהגורם אליו הוא מעביר את המידע הנוגע למתן שירות ללקוח הוא הלקוח, או גורם אחר שהלקוח ביקש במפורש שהנתונים יועברו אליו, בהתאם להוראות סעיף 13(א) לכללי נתוני אשראי (הוראות שונות).

#### גישה למסמכים, הצפנה

43. גישה למסמכים המכילים מידע רגיש (לרבות נתוני אשראי) תתאפשר בהתאם לפרק "ניהול הרשאות ובקרת גישה, וניהול סיסמאות" שלהלן.

44. מיופה כוח בתמורה יצפין תעבורה בתווך בהתאם להערכת סיכונים, ולכל הפחות בתקשורת מחוץ לחצרותיו (Data In-Transit).

45. מיופה כוח בתמורה יצפין נתוני אשראי במנוחה (Data At-Rest), לרבות בבסיסי הנתונים ובקלטות גיבוי. הצפנה כאמור בבסיס הנתונים תבוצע עם כניסת המידע לבסיס הנתונים.

46. ההצפנה תיושם באמצעות טכניקות הצפנה מוכרות שהוכחו כיעילות, ותתוקף האפקטיביות שלהן באופן תקופתי.

#### ניהול הרשאות ובקרת גישה, וניהול סיסמאות

47. הליך מתן הרשאות גישה למשתמשים יבוצע בהתאם לתפקיד, על ידי שיוך לפרופיל הרשאות או באופן פרטני ברמה אישית.



48. מתן הרשאות גישה לעובדים יצומצם למינימום ההכרחי הדרוש לצורך ביצוע התפקיד (לדוגמה, מתן הרשאות באמצעות שיוך לפרופיל משתמש המותאם לתפקיד העובד).
49. יוגדר תהליך למעבר עובד לתפקיד חדש, לרבות : הסרת ההרשאות ששימשו את העובד בתפקידו הקודם, והענקת הרשאות חדשות הדרושות למילוי תפקידו החדש של העובד.
50. משתמשים בעלי הרשאות חזקות יבצעו הזדהות באמצעות Multi-Factor Authentication (MFA) בטרם גישה למערכות המידע ולתשתיות.
51. יתועד תהליך ניהול והענקת הרשאות למשתמשים (וכן הסרת הרשאות למשתמשים), לרבות רשימת תפקידים, הרשאות גישה שניתנו להם, בעלי ההרשאות הממלאים תפקידים אלו, מערכות המידע הרלוונטיות ואישורים של הגורמים הרלוונטיים (להלן : "רשימת ההרשאות").
52. תוגדר רשימה של חשבונות משתמשים תוך חלוקה בין "חשבון מנהל" לבין "חשבון משתמש" לרבות פירוט של סוגי הרשאות המשויכות לכל חשבון.
53. ככלל, יעשה שימוש בחשבונות משתמש אישיים לצורך אימות המשתמשים באופן חד ערכי. 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 ההזדהות של החשבון, להגבלת השימוש בו ככל הניתן, ויוגדר גורם האחראי על חשבון המשתמש.
54. אחת לשנה, תבוצע בחינה של הרשאות המשתמשים המורשים למערכות ולתשתיות, שמטרתה לוודא כי הגישה הקיימת לכל משתמש הינה בהתאם לצורך והכרחית למילוי תפקידו. עבור חשבונות משתמשים חזקים, ספקים חיצוניים, עובדי מיקור חוץ ועובדים זמניים הבחינה תבוצע בתדירות גבוהה יותר. תהליכי הסקירה יבוצעו בהתאם לסוג ההרשאה שניתנה ומידת מורכבותה.
55. מיופה כוח בתמורה יודא כי הגישה למאגר היא לבעלי הרשאה המורשים לכך בלבד על פי רשימת ההרשאות.
56. מיופה כוח בתמורה יישם מדיניות סיסמאות בקרב המשתמשים בהתאם לסטנדרטים מקובלים. מדיניות הסיסמאות תכלול התייחסות לאלה : אורך תווים מינימלי, תדירות החלפת סיסמאות (שלא תעלה על תקופה של 90 ימים), מורכבות סיסמא מינימלית וחסירת גישת משתמש לאחר מספר ניסיונות גישה כושלים.
57. מיופה כוח בתמורה יגדיר נהלים המתייחסים לשמירה על סודיות הסיסמה ולהחלפת סיסמה ראשונית על ידי המשתמש.
58. יש לאמת את זהות המשתמש כאשר נמסרת לו סיסמה ראשונית למערכת. המשתמש יחויב לשנותה בהתחברות הראשונה למערכת. תוקף הסיסמה הראשונית ייקבע למינימום זמן האפשרי, בהתאם לאופי השימוש בחשבון, ולא יעלה על 14 ימים.
59. סיסמאות או אמצעי הזדהות אחרים לא יישמרו באופן גלוי (Clear Text), או באופן הניתן לשחזור, ברשומות, בזיכרון או במאגרי מידע.
60. לאחר חוסר פעילות זמני של משתמש, ינותק החיבור לרשת ולמערכות המידע, כך שלא תתאפשר המשכיות החיבור עד להזדהות ואימות חוזר של המשתמש.





61. חשבון משתמש שאין בו צורך יותר יועבר למצב Disable או ימחק. בחשבון משתמש שהועבר למצב Disable יוסרו כלל ההרשאות והוא ימחק לאחר פרק זמן קצוב שיקבע בנהלים.
62. מיד עם סיום תפקידו של בעל הרשאה, מיופה כוח בתמורה יפעל, ככל הניתן, לשינוי סיסמאות למאגר ולמערכות המאגר שבעל הרשאה עשוי היה לדעת.

### תכנית היערכות לניהול אירועי אבטחת מידע

63. ההנהלה תגדיר תכנית היערכות לניהול אירועי אבטחת מידע הכוללת התייחסות לאופן התמודדות עם אירועי אבטחת מידע לפי חומרת האירוע ומידת רגישות המידע, לרבות:
- 63.1. דרכי תגובה ופעולה, לרבות ביטול הרשאות וצעדים אחרים נדרשים, בהתייחס לתרחישי איום שונים, והגורמים האחראים על הפעלתן.
- 63.2. ערוץ תקשורת לעובדים לצורך דיווח להנהלה על אירועי אבטחת מידע או על חשד לאירועים כאמור.
- 63.3. דרכי התקשרות והעברת מסרים עם גורמים פנימיים וחיצוניים, ובכללם לקוחות, בהתאם לתרחישים שונים.
- 63.4. תיעוד אופן הטיפול באירוע.
- 63.5. מתכונת ותדירות הדיווח על האירועים, גורם מדווח, נמען הדיווח וזמן תגובה לדיווח, לרבות דיווח לממונה ולגורמים נוספים על פי דין או על פי הנחיות הממונה.
64. ההנהלה תדון בתכנית ההיערכות לניהול אירועי אבטחת מידע לכל הפחות אחת לשנה, ובכל עת שנעשה שינוי מהותי במערכות המידע או בתהליכי העבודה או שינוי ארגוני משמעותי, וכן בעקבות אירועי אבטחת מידע שהתרחשו, לרבות הסקת מסקנות עיקריות, ותבחן את צורך בעדכון התוכנית לטיפול באירועי אבטחת מידע והנהלים, לרבות התייחסות לעובדים חדשים ולמיקור חוץ, וכן תקיים, לכל הפחות, אחת לשנה תרגול של כלל המערכים הרלוונטיים שמטרתו להכין אותו להפעלת התוכנית לטיפול באירועי אבטחת מידע ולשיפורה בהתאם ללקחי התרגול.

### אבטחת שרשרת אספקה ומיקור חוץ

65. מיופה כוח בתמורה לא יעביר פעילות מהותית הקשורה למתן שירות ללקוח, למיקור חוץ.
66. מיופה כוח בתמורה אשר מקבל שירותים במיקור חוץ מספק חיצוני (להלן - "הספק"), נדרש לבחון, לפני ביצוע ההתקשרות, את סיכוני אבטחת המידע הכרוכים בהתקשרות עם הספק וכן לכלול לכל הפחות התייחסות להיבטים הבאים בהסכם התקשרות כתוב בינו לבין הספק:
- 66.1. המידע שהספק רשאי לעבד, מטרות השימוש המותרות בו לצרכי ההתקשרות וסוג העיבוד או הפעולה שהספק החיצוני רשאי לעשות.
- 66.2. מערכות המאגר שהספק רשאי לגשת אליהן.
- 66.3. משך ההתקשרות, אופן השבת המידע בסיום ההתקשרות, השמדתו מרשותו של הספק ודיווח על כך למיופה הכוח בתמורה.
- 66.4. אופן יישום החובות בתחום אבטחת המידע על ידי הספק בהתאם לתקנות הגנת הפרטיות, להוראה זו ולהנחיות נוספות שנקבעו על ידי מיופה הכוח בתמורה, ככל שרלוונטי.



- 66.5. הגדרת תחומי אחריות של כל אחד מהצדדים להסכם לרבות גורמים נוספים (כגון קבלני משנה), ככל שרלוונטי.
- 66.6. הגדרת רמת שרות (SLA).
- 66.7. הצהרת הספק לפיה הוא:
- 66.7.1. מתחייב לעמוד בדרישות הוראה זו, תקנות הגנת הפרטיות וכן הנחיות נוספות ליישום אמצעי אבטחת מידע שנקבעו על ידי מיופה הכוח בתמורה, ככל שרלוונטי.
- 66.7.2. מתחייב לשמור על סודיות המידע ולהשתמש בו רק על פי האמור בהסכם.
- 66.8. חובתו של הספק לדווח למיופה הכוח בתמורה, בתדירות של אחת לשנה לפחות, על אופן ביצוע חובותיו לפי פרק זה והסכם ההתקשרות ולהודיע למיופה הכוח בתמורה במקרה של אירוע אבטחה.
- 66.9. ככל שהספק מספק את השירות באמצעות גורם נוסף – חובתו של הספק לכלול בהסכם עם הגורם הנוסף את כל ההיבטים המפורטים בסעיף זה.
- 66.10. הסדרים להפסקת הסכם וליישוב מחלוקות.
- 66.11. איסור על הספק להעביר לצד שלישי מידע שקיבל במסגרת ההתקשרות, או להשתמש במידע שאליו נחשף אגב ביצוע ההתקשרות, לכל מטרה אחרת שלא קשורה לביצוע ההתקשרות.
- 66.12. הגבלת הגישה והחשיפה לנתוני אשראי למינימום האפשרי, לרבות ביצוע תהליך גישה מבוקרת לנתונים פרטניים בעת הצורך להעברת נתונים, ככל שרלוונטי, ולא שכפול כלל בסיס הנתונים.
- 66.13. ככל שהשירותים הניתנים על ידי הספק כוללים שירותי פיתוח – התחייבות הספק לבצע פיתוח באופן מאובטח.
- 66.14. עיגון חובת הספק להעביר מידע, ידיעות ומסמכים לממונה לפי דרישתו של הממונה, והתחייבותו לאפשר ביצוע ביקורת של הממונה אצל הספק בנוגע לפעילותו.
67. אין בהנחיות לגבי מיקור חוץ כדי לגרוע מאחריותו של מיופה כוח בתמורה לכל פעולה הנעשית מטעמו או בהסכמתו על ידי ספק מיקור החוץ.
68. מיופה כוח בתמורה ינקוט אמצעי בקרה ופיקוח על עמידת הספק בהנחיות הסכם ההתקשרות והוראה זו, בהיקף הנדרש ובשים לב לחשיפה לסיכונים.
69. מיופה כוח בתמורה יישם הזדהות באמצעות MFA לצורך כל גישה מרחוק של ספק מיקור חוץ. אימות ספק מיקור חוץ יערך באמצעות חשבון משתמש אישי.

### מחשוב ענן

70. שירותי מחשוב ענן יחשבו מיקור חוץ ובהתאם לכך יחולו עליהם הנחיות הוראה זו לעניין אבטחת שרשרת אספקה ומיקור חוץ.
71. בטרם שימוש במחשוב ענן, מיופה כוח בתמורה יבצע הערכת סיכונים שתתייחס, בין היתר, לסיכונים תפעוליים, עסקיים, סיכונים אבטחת מידע, הגנת הסייבר והמשכיות עסקית, סיכונים טכנולוגיים, סיכונים משפטיים, לרבות היבטי סודיות המידע והבעלות על המידע וסיכונים ציית. מיופה כוח בתמורה יבחן את הצורך בעדכון הערכת הסיכונים במהלך תקופת ההתקשרות בהתאם לשינויים בפעילותו ובפעילות ספק שירותי הענן.



72. מיופה כוח בתמורה יגדיר מדיניות לשימוש במחשוב ענן אשר תתייחס בין היתר לסוגי היישומים והשירותים במחשוב ענן, סמכויות ואחריות, בקורות, היבטים משפטיים, פיתוח, תחזוקה, אבטחת מידע וכיו"ב.
73. מיופה כוח בתמורה רשאי לאחסן מידע רגיש לרבות נתוני אשראי מחוץ לגבולות מדינת ישראל, רק לאחר שווידא שספק שירותי הענן מקיים את רמת ההגנה בהתאם לרגולציית הגנת המידע של האיחוד האירופי (GDPR - General Data Protection Regulation) או רגולציה מקבילה אחרת.
74. גישה לנתונים בענן תבוצע באמצעות דרכי גישה מאובטחות, כגון: כתובות מורשות בלבד, שימוש ב-MFA, הצפנה וכיו"ב.
75. על הנתונים המאוחסנים בענן ייושמו בקורות כגון הצפנה, מיסוך נתונים או טוקניזציה, במטרה למנוע חשיפת מידע רגיש, לרבות נתוני אשראי לגורמים שאינם מורשים.
76. מיופה כוח בתמורה יודא שיש לו אפשרות לבצע ניטור אירועי אבטחת מידע המתרחשים בענן.
77. מיופה כוח בתמורה יודא כי עבור כלל ערוצי הגישה מספק מחשוב הענן ואליו, קיימים אמצעים להגנת הסייבר ואבטחת מידע, שיאפשרו לצמצם, ככל שניתן, את השימוש בערוצים אלו לתקיפה.
78. מיופה כוח בתמורה יכלול בהסכם ההתקשרות עם ספק מחשוב הענן אפשרות חד-צדדית של מיופה הכוח בתמורה להפסקת השימוש בשירותי ספק מחשוב הענן, תוך מחיקת המידע ממערכותיו והתחייבותו שלא ניתן לאחזר מידע זה במערכותיו.

#### מסירת מידע באמצעים דיגיטליים

79. כל הודעה הנשלחת באמצעים דיגיטליים תישא כותרת המשקפת את תוכנה.
80. דוח ריכוז נתונים הנשלח ללקוח באמצעים דיגיטליים יוגן בסיסמה.

#### אבטחה פיזית וסביבתית

81. מיופה כוח בתמורה יבטיח כי תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע יישמרו במקום מוגן, המונע חדירה וכניסה אליו בלא הרשאה, והתואם את אופי פעילות המאגר ורגישות המידע שבו.
82. מיופה כוח בתמורה יבצע השמדה של רכיבי מידע המכילים נתוני אשראי לצמיתות (הן מידע השמור פיזית והן מידע האגור במדיה מגנטית).
83. ככל שנעשה שימוש בספק חיצוני האמון על השמדת מדיה (למשל, ניירת ומדיה מגנטית), נדרש לקבל אישור בכתב מצד הספק החיצוני בנוגע לנאותות השמדת המידע.
84. תבוצע אכיפה בעת מתן גישה פיזית למתחם מיופה הכוח בתמורה תוך הקפדה על נעילת דלתות. התרת הגישה תבוצע לאחר ביצוע תהליך זיהוי באמצעות כרטיס עובד, הזנת קוד אישי או אמצעים דומים אחרים.
85. מיופה כוח בתמורה יישם מערך הגנה מקיף הכולל אמצעי אבטחה אשר יכללו בקורות מונעות ובקורות מגלות, כגון: מצלמות אבטחה ומערכות אזעקה, תוך שימת דגש על מתחמים רגישים והקפדה על תחזוקה שוטפת של מערך ההגנה כאמור.



86. מיופה כוח בתמורה ישמור נתיבי בקרה המתעדים כניסה פיזית למתחם בו מאוחסנים מערכות, תשתיות, חדר מחשב מרכזי, ארונות תקשורת וכדומה.
87. מיופה כוח יבדוק, יזהה וירשום ספקים חיצוניים ומבקרים במתחמיו, וכן יקפיד על איסור כניסה לאזורים רגישים (כגון חדר מחשוב וחדר תקשורת), תוך הקפדה על תיעוד וניטור אחר הגישה לאזורים אלו. ככל שנשכר מתחם חיצוני שבו מאוחסנים שרתי מיופה הכוח בתמורה, המנוהל ומתופעל במיקור חוץ, יכללו בהסכם דרישות המתייחסות לאבטחה הפיזית והסביבתית של המתחם.
88. מיופה כוח בתמורה יסקור באופן שוטף את רשימת מורשי הגישה למתחמיו ויקפיד על הסרת הרשאות גישה עודפות.
89. מיופה כוח בתמורה יבקר וינטר גישה למתחמיו ולאזורים הרגישים, בין היתר שלא בשעות העבודה המקובלות או בימים שאינם מוגדרים כימי עבודה.

#### משאבי אנוש והדרכה

90. ההנהלה תגדיר תהליך מיון וגיוס מועמדים בטרם העסקתם, וכן בטרם שינוי היקף הרשאות גישה לעובדים קיימים (לדוגמה, ביצוע ראיונות וביצוע מבדקי אמינות עבור משרות שהוגדרו כרגישות). מטרת התהליך לוודא כי העובדים מתאימים לקבלת גישה לסוג המידע הנדרש בשים לב לרגישות המידע, היקף הרשאות הגישה והתפקיד שמיועד לעובד.
91. מיופה כוח בתמורה יגדיר כללי התנהגות ונהלים לעובדים בהיבטי אבטחת מידע והגנת הפרטיות בהתייחס למערכות המידע, תחומי אחריות ושימוש נאות במערכות, תוך שימת דגש על מערכות רגישות.
92. מיופה כוח בתמורה יודא כי עובדים חדשים ועובדים קיימים חתומים על נספח אבטחת מידע ומסמך הצהרה על שמירה על סודיות, שיכללו, בין היתר, התייחסות להיבטים הבאים:
- 92.1. כללי התנהגות ונהלים נדרשים ומקובלים, תוך מתן דגש על שימוש במערכות המידע, לרבות שימוש נאות במשאבים הטכנולוגיים אצל מיופה הכוח בתמורה.
- 92.2. הצהרת העובד כי הוא יפעל בהתאם לדרישות אבטחת המידע המופיעות בנוהל אבטחת המידע הארגוני.
- 92.3. התחייבות העובד לשמירה על סודיות מידע רגיש אליו נחשף במסגרת תפקידו, תוך מתן דגש על נתוני אשראי.
- 92.4. התחייבות העובד להימנע ממצבים בהם הוא מצוי בניגוד עניינים במסגרת תפקידו השוטף.
93. התחייבות העובד לעמידה בכללים ונהלים והגבלות שיקבעו על ידי ההנהלה המתייחסים לשימוש ברשתות החברתיות.
94. לפחות אחת לשנה, העובדים יעברו הדרכה בנושא שימוש נאות במידע, דרישות אבטחת מידע, איומים פנימיים וחיצוניים וסימני מזהים עבור איומים אלו.
95. עובד חדש, או עובד ששוננו לגביו היקפי הרשאה, יתוודך בטרם כניסתו לתפקיד או ביצוע השינוי על ידי הגורם האמון על נושא אבטחת המידע אצל מיופה הכוח בתמורה, וכן בזמן מעבר מתפקיד לתפקיד, אם קיימת משמעות אבטחתית למעבר. ההדרכה תתייחס, בין היתר, לחובות העובד בגין חוק הגנת הפרטיות ותקנותיו, והנהלים הפנימיים בנושאי אבטחת מידע.
96. מיופה כוח בתמורה יודא כי בסיום העסקה לא יישארו נכסי מידע בידי העובד.



### עריכת ביקורת תקופתית

97. תיערך ביקורת על ידי מבקר, בהתאם למפורט בסעיף 5 לפרק ג', בדבר עמידת מיופה הכוח בתמורה בדרישות הוראה זו.
98. דוח הביקורת יועבר להנהלה ולדירקטוריון ככל שקיים והם ידונו בדוח הביקורת, יפעלו ליישום ההמלצות, ויבחנו את הצורך בעדכון המדיניות או נהלי אבטחת המידע.
99. ככל שזוהו ליקויים בדוח הביקורת, תיקבע תכנית עבודה שתכלול לוח זמנים לטיפול בליקויים. לוח הזמנים יביא בחשבון את רמת הסיכון של הממצאים, ובכלל זה את מידת החשיפה לאירועי אבטחת מידע והפגיעה בפרטיות הלקוחות.

### שמירה, גיבוי ושחזור של נתונים ומידע

100. מיופה כוח בתמורה ישמור באופן מאובטח את הנתונים הבאים :
- 100.1. נתיבי בקרה כנדרש בהוראה זו.
- 100.2. בקרות ותהליכי עבודה שביצע לצורך עמידה בדרישות הוראה זו.
- 100.3. נתוני אירועי אבטחת מידע ותקלות שמעלות חשד לאירועי אבטחת מידע.
- 100.4. מסמכים הקשורים לפעילותו דוגמת מסמכי מדיניות ונהלים, תכנית היערכות לניהול אירועי אבטחת מידע ואופן הטיפול באירועי אבטחת מידע, הערכות סיכונים, דוחות ביקורת ותכניות עבודה לטיפול בליקויים שזוהו בדוחות הביקורת.
101. הנתונים כאמור בסעיפים 100.1-100.3 ישמרו לתקופה שלא תפחת מ-24 חודשים, והנתונים כאמור בסעיף 100.4 ישמרו לתקופה שלא תפחת מ-7 שנים.
- הנתונים כאמור בסעיפים 100.1-100.4 יגובו באופן שיאפשר, בכל עת, שחזור שלהם למצבם המקורי.

### **פרק ו' - דרישות נוספות שיחולו על מיופה כוח בתמורה הנכלל בקבוצה 3**

מיופה כוח בתמורה הנכלל בקבוצה 3 יישם את הדרישות המפורטות בפרק ה', ובנוסף יישם את הדרישות שלהלן:

#### חובת התאגדות כחברה

102. מיופה כוח בתמורה הנכלל בקבוצה 3 יפעל כחברה, כהגדרתה בחוק החברות, תשנ"ט-1999.

#### אחריות הדירקטוריון

103. מיופה כוח בתמורה יקבע מדיניות לניהול המידע והגנתו שתידון בדירקטוריון ותאושר על ידו. המדיניות תכלול התייחסות לכלל הנושאים שפורטו בפרק ה' וכן לתפיסת הגנת המידע - אבטחת המידע, כפי שהוגדרה על ידו.
104. הדירקטוריון ידון, לפחות אחת לשנה ובעת ביצוע שינוי מהותי, בחשיפות לסיכונים הנובעים מניהול המידע והגנתו כפי שהם מוצגים בסקרי הסיכונים ומבחני החדירה ובעקבות ממצאי דוחות הביקורת בנושא, וכן ידון בתוכנית שנקבעה על ידי ההנהלה להפחתת הסיכונים שזוהו.



105. לפחות אחת לשנה יידון הדירקטוריון באירועי אבטחת מידע מהותיים שהתרחשו, בהחלטות ובפעולות שבוצעו.
106. מסמך המדיניות ונהלי העבודה יעודכנו על ידי ההנהלה, ויאושרו על ידי הדירקטוריון בתדירות הנדרשת בסעיף 16.

### אחריות ההנהלה

107. על אף האמור בסעיף 13.1, ההנהלה תמנה ממונה על אבטחת המידע והגנת הסייבר שיפעל בכפיפות ישירה להחלטות ההנהלה, וזו תקצה לו משאבים מתאימים. הממונה על אבטחת המידע:
- 107.1. יהיה אמון על מדיניות אבטחת המידע.
  - 107.2. יפעל לקידום וחיזוק מערך אבטחת המידע.
  - 107.3. יכין תכנית לבקרה שוטפת, יבצע אותה ויודיע להנהלה על ממצאיו.
108. הממונה על אבטחת המידע והגנת הסייבר יהיה בעל הכשרה וניסיון מתאימים, שיש לו הסמכה כדוגמת אחת או יותר מההסמכות הבאות:
- 108.1. CISSP.
  - 108.2. CCSA.
  - 108.3. CCNA.
  - 108.4. CISO.
  - 108.5. CISA.
  - 108.6. CISM.
- 108.7. בודקי ספקים שעמדו בהצלחה בבחינות הסיום לקורס בודקי תאימות סייבר לשרשרת אספקה ארגונית, מגופים המוכרים על ידי מערך הסייבר הלאומי.
109. הממונה על אבטחת המידע והגנת הסייבר לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגודי עניינים בביצוע תפקידו כממונה על אבטחת המידע והגנת הסייבר. בנוסף, ככל שיוקצו לממונה על אבטחת המידע משימות נוספות, אלו יוגדרו על ידי ההנהלה באופן ברור. יובהר כי הממונה על אבטחת המידע והגנת הסייבר אינו חייב להיות עובד של מיופה הכוח בתמורה.
110. ההנהלה, באמצעות הממונה על אבטחת המידע והגנת הסייבר, תבחן באופן שוטף את מגוון הסיכונים בהיבטי אבטחת מידע וסייבר, תעקוב אחר איומי סייבר משמעותיים בישראל ובעולם ותאסוף ותנתח מידע רלוונטי ממקורות פנימיים וחיצוניים (לרבות פרסומים שונים של מערך הסייבר הלאומי והרשות להגנת הפרטיות, בין היתר, בכל הנוגע להתראות, פגיעויות, עדכוני אבטחה והמלצות). בהתאם לכך, ההנהלה תפיק לקחים, תיישם מסקנות רלוונטיות ותפעל לצמצום החשיפות לאיומים.
111. ההנהלה תדון, לפחות אחת לשנה ובעת ביצוע שינוי מהותי, בחשיפות לסיכונים הנובעים מניהול המידע והגנתו כפי שהם מוצגים בסקרי סיכוני אבטחת מידע ומבחני החדירה, ובעקבות ממצאי דוחות הביקורת בנושא. בנוסף, ההנהלה תקבע תכנית להפחתת הסיכונים שזוהו ותעמיד משאבים נאותים לצורך כך, ותעקוב לכל הפחות ברמה רבעונית אחר יישומה.



### סקר סיכוני אבטחת מידע ומבחני חדירה

112. מיופה כוח בתמורה נדרש לבצע סקר סיכונים בהיבטי אבטחת מידע וסייבר על ידי גורם בלתי תלוי בעל הסמכה וניסיון בנושא.
113. מיופה כוח בתמורה נדרש להגדיר תכנית עבודה לטיפול בממצאים העולים מסקר הסיכונים, הכוללת ביצוע מעקב וניטור אחר אופן הטיפול בממצאים אלה.
114. מיופה כוח בתמורה נדרש לבצע מבחני חדירה על ידי גורם חיצוני בלתי תלוי בעל הסמכה וניסיון בנושא, תוך הקפדה על טיפול ותיקון הממצאים.
115. סקר הסיכונים ומבחני החדירה (להלן יחד: "הסקרים") יערכו לפי פרקטיקה מקובלת, יבוצעו בתדירות שלא תפחת מ-18 חודשים, יתייחסו לכלל מאגרי המידע ומערכות המידע המהותיות הרלוונטיות לפעילות, ויבחנו את התאמת כל מערכות המידע והתהליכים העסקיים למדיניות ולנוהלי אבטחת המידע של מיופה הכוח בתמורה, לרבות ברמת בדיקת קיום ואפקטיביות הבקורות להגנה על המידע בפני סיכונים פנימיים וחיצוניים. על אף האמור לעיל, יש לבצע סקרים טרם הטמעת שינוי משמעותי במערכת מידע, או בסביבתה הטכנולוגית, או טרם יישום של שירות חדש.
116. מבחני החדירה יכללו מבחן המדמה ניסיון תקיפה מרשתות חיצוניות (כגון רשת האינטרנט, חיבור לספקים או שותפים עסקיים), בדיקות הנדסה חברתית, התחזות ופשינג, ותקיפה מתוך הרשת. במסגרת ביצוע מבחני החדירה יש לפעול הן כמשתמש קיים והן ללא חשבון קיים.

### תהליכי פיתוח ותחזוקה

117. תהליכי פיתוח יתבצעו בהתאם לפרקטיקה מקובלת לביצוע תהליכי פיתוח באופן מאובטח (SSDLC).
118. בשלב יזום ואפיון מערכות מידע, יבוצע הליך הערכת סיכונים בהיבטי אבטחת מידע של הפרויקט והמוצר, לרבות הגדרת הדרישות.
119. בשלב הפיתוח, מיופה כוח בתמורה יישם ויממש את דרישות האבטחה אשר הוגדרו בשלב אפיון המערכת, ויקפיד על הטמעתן באופן מלא ברמת התשתיות, האפליקציה והלוגיקה העסקית המיושמת במערכת.
120. יבוצע הליך לבדיקת המערכת בטרם הטמעתה תוך הקפדה, בין היתר, על:
- 120.1. בדיקות ברמת הקוד בהיבטי אבטחת מידע.
- 120.2. פונקציונליות המערכת.
- 120.3. יישום בדיקות על ידי גורם שאינו מעורב בתהליך הפיתוח.
121. תבוצע הטמעת מערכת לאחר קבלת אישורים על ידי הגורמים הרלוונטיים, לרבות הממונה על אבטחת המידע.
122. שלבים אלו יבוצעו גם בפעילות תחזוקה או ניהול שינויים במערכות המידע, בהתאם לרלוונטיות.

### אבטחת רשת

123. מיופה כוח בתמורה יישם 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 המידע.



124. מיופה כוח בתמורה יגדיר וינהל כלים לזיהוי נזקות בסביבת הרשת הארגונית ובתחנות קצה.

#### **אבטחת מערכות ועדכון**

125. הטמעת עדכוני אבטחת מידע תתבצע תוך התייחסות למקוריות קבצי העדכון, בדיקת עדכונים בטרם יישומם, ושמירה על יציבות מערכות המידע בתהליך העדכון. מיופה כוח יתעד את תהליך העדכון המבוצע בהתאם לדרישות סעיף זה, ויגבש תכנית גיבוי המאפשרת שחזור בטוח וחזרה למצב לפני העדכון במקרה של השפעות בלתי צפויות כתוצאה מעדכון.

126. מיופה כוח בתמורה נדרש לנקוט באמצעים הולמים לצורך צמצום החשיפה לסיכוני אבטחת מידע במערכות המידע ובתשתיות.

127. יוטמעו כלים אוטומטיים לסריקת חולשות אבטחה במערכות ובתשתיות, תוך הקפדה על עדכונים שוטפים והפקת התראות בזמן אמת לגורמים הרלוונטיים אצל מיופה הכוח בתמורה. סריקת חולשות אבטחה כאמור יכולה להתבצע באמצעות ספק חיצוני בעל ידע וניסיון רלוונטי.

#### **הפרדה בין סביבות**

128. הסביבה בה ינוהלו נתוני אשראי של לקוחות פרטיים, תופרד באופן מוחלט ממערכות מידע וסביבות אחרות, לרבות מסביבות התומכות בפעילות עסקית אחרת של מיופה הכוח בתמורה. גישה לנתוני האשראי של לקוחות פרטיים תתבצע תחת בקרה וסינון.

129. הרשאות משתמשים לסביבות ייצור תנוהלנה בנפרד מההרשאות לסביבות האחרות.

130. העברת נתונים מסביבת ייצור לסביבה אחרת תתבצע באישור הממונה על אבטחת המידע, או מי מטעמו.

#### **ניהול הרשאות ובקרת גישה**

131. מיופה כוח בתמורה יגביל את מספר החיבורים המותרים בו זמנית של משתמש בודד.

132. מיופה כוח בתמורה יגדיר הליך תקופתי לטיוב פרופילי הרשאות המשוויכים לתפקיד תוך הקפדה על תחומי אחריות, קיום הרשאות בהתאם לעקרון "הצורך לדעת", ומתן דגש על קיום הרשאות מינימליות לביצוע התפקיד.

133. מיופה כוח בתמורה נדרש להגדיר מנגנון אשר מזהה חשבונות משתמשים אשר לא קיימת בהם פעילות לאורך פרק זמן ממושך. גישה לחשבונות אלו תיחסם באופן אוטומטי.

134. מיופה כוח בתמורה יישם מנגנון לנטרול וחסמת חשבונות זמניים באופן אוטומטי לאחר פרק זמן מוגדר.

135. הפרדת סמכויות תיושם בפרופילי הרשאות המשתמשים, לרבות מניעת גישה כך שלעובד פיתוח לא תהיה גישה לסביבת הייצור, למעט הרשאות צפייה.

136. מיופה כוח בתמורה יישם מנגנון לניטור והקלטת פעולות המבוצעות במערכות המידע על ידי משתמשים חזקים וספקי מיקור חוץ.





### מניעת דלף מידע ואובדן מידע

137. מיופה כוח בתמורה יערוך מיפוי של תהליך זרימת מידע רגיש, לרבות נתוני אשראי, בהתאם לערוצי התקשורת ולפעילות העסקית. בהתאם למיפוי, מיופה כוח בתמורה יישם מנגנונים ובקורות למניעת דלף מידע ואובדן מידע, לדוגמה, הטמעת התראות או חסימות על ניסיונות להעברת או הוצאת מידע רגיש על ידי גורמים שאינם מורשים, או בניגוד למדיניות ולנהלים. לעניין זה, "דלף מידע" - חשיפת מידע לגורמים שאינם מורשים מחוץ לחצרות מיופה הכוח בתמורה (Data Leakage), "אובדן מידע" - פגיעה בשלמות המידע (Data Loss), לרבות במצב מנוחה (אחסון), שימוש (פעולות בנקודות קצה) ותנועה (תעבורת רשת).

### שימוש בתעודה דיגיטלית

138. מיופה כוח בתמורה הפועל באמצעות פלטפורמה דיגיטלית, שמאפשרת הוצאת נתוני אשראי, יבצע שימוש בתעודה דיגיטלית, שתונפק על ידי גוף מוכר הפועל לפי תקנים מקובלים, להעברת המידע, כמפורט להלן:

- 138.1. עבור משתמשי קצה – מיופה כוח בתמורה נדרש לעשות שימוש בתעודה דיגיטלית חד-כיוונית.
- 138.2. בתקשורת בין מיופה הכוח לספקים וגורמים חיצוניים שאינם משתמשי קצה – מיופה כוח בתמורה נדרש לעשות שימוש בתעודה דיגיטלית דו-כיוונית.

### ניהול משתמשים

139. מיופה כוח בתמורה יתעד, ינטר ויבצע בקרה אחר משתמשים באופן שוטף ויחקור אנומליות או חריגות.
140. בכל הנוגע לניהול חשבונות משתמשים בעלי הרשאות חזקות (לדוגמה - Privileged User Accounts, Service Accounts, Domain Administrative Accounts, Active Directory/Domain Service Accounts, Application Accounts with admin permissions), מיופה כוח בתמורה יפעל בהתאם להנחיות המפורטות להלן:
  - 140.1. נדרש לזהות את כלל חשבונות המשתמשים בעלי הרשאות חזקות, לרבות המשתמשים החזקים המנהלים יישומים שנרכשו מגורם צד שלישי, ולנהל את חשבונות המשתמשים באופן מרוכז, לדוגמה באמצעות מערכות המיישמות טכנולוגיית Privileged Access Management (PAM);
  - 140.2. ערוצי התקשורת ינוטרו;
  - 140.3. סיסמאות, שמות משתמשים ומפתחות הצפנה בחשבונות של משתמשים אפליקטיביים חזקים (Privilege Application Accounts) יוחלפו בתדירות של אחת ל-90 יום לפחות;
  - 140.4. עבור משתמש שאינו זקוק להרשאות חזקות באופן קבוע, הפעילות בחשבון תבוצע לאחר קבלת אישור מראש ותהיה מוגבלת בזמן.

### תכנית היערכות לניהול אירועי אבטחת מידע

141. מיופה הכוח בתמורה יגדיר תכנית היערכות לניהול אירועי אבטחת מידע (להלן – תכנית ההיערכות), בהתאם להערכת סיכונים ולניתוח תרחישי איום (כגון: גישה לא מורשית לנכסי המידע, דלף מידע, התחזות, נזקות, הונאה, מניעת שירות וכדומה) אשר תתייחס לשלבי האירוע הבאים:



406 עמ' 26

הממונה על שיתוף בנתוני אשראי: הוראה למיופה כוח בתמורה  
ניהול סיכוני אבטחת מידע והגנת הסייבר (12/22)

נתוני אשראי  
הקרדיט שמגיע לך



- 141.1. גילוי – גילוי וזיהוי השלב בו נמצא האירוע תוך פירוט שלבי הפעולה (בידוד, חקירה, איסוף ראיות, הסקת מסקנות וכדומה).
- 141.2. הערכת מצב – בירור וניתוח האירוע ובחינת דרכי פעולה להתמודדות, לרבות הפסקת פעילות באופן זמני באירועים בחומרה גבוהה.
- 141.3. הכלה – השגת שליטה על האירוע.
- 141.4. בלימה – עצירת החמרה של האירוע.
- 141.5. התאוששות – הכרעת האירוע תוך מזעור הנזקים שנגרם.
- 141.6. חזרה לשגרה – חזרה לפעילות מלאה לאחר תיקון כל נזק שנגרם.
142. במקום האמור בסעיף 64, לגבי תדירות הדיון בתכנית ההיערכות לניהול אירועי אבטחת מידע, יערך דיון כאמור לכל הפחות אחת לרבעון. יתר הוראות סעיף 64 יחולו בהתאמות הנדרשות.
143. מיופה כוח בתמורה יקים צוות תגובה להתמודדות עם אירועי אבטחת מידע.

#### **אבטחת שרשרת אספקה ומיקור חוץ**

144. מיופה כוח בתמורה יבצע הליך שוטף ומחזורי למיפוי כלל הספקים, לרבות ספקים מהותיים. בין היתר, ההליך יכלול בחינת הסיכונים הנגזרים מאופי הפעילות של ספקים אלו והבקורות הננקטות לצמצום הסיכונים, ובחינת הסכס ההתקשרות מולם.
145. מיופה כוח בתמורה יבצע ביקורות בחצרות ספקים מהותיים, לצורך בחינת אפקטיביות מערך ההגנה ואבטחת המידע המיושם על ידם או שיוודא את עמידתם בתקני אבטחת מידע מקובלים והסמכות חיצוניות באמצעות קבלת מידע הנוגע למבדקים וביקורות שבוצעו לגביהם.
146. מיופה כוח בתמורה יישם מנגנון בקרה וניטור אחר פעולות המבוצעות על ידי ספק, באמצעות קבלת גישה פיזית או גישה מרחוק למשאבי המחשוב, תוך הקפדה על תיעוד הניטור והמעקב אחר פעולות הספק.

#### **מחשוב ענן**

147. בטרם התקשרות עם ספק שירותי ענן המוגדר כספק מהותי, מיופה כוח בתמורה:
- 147.1. יוודא את חוסנו הכלכלי והתפעולי, יכולתו המקצועית וניסיונו לספק שירותים דומים. מיופה כוח בתמורה יבצע בדיקה כאמור גם באופן תקופתי במהלך ההתקשרות.
- 147.2. יוודא את עמידתו בתקני אבטחת מידע מקובלים והסמכות חיצוניות באמצעות קבלת מידע הנוגע למבדקים וביקורות שבוצעו לגבי ספק שירותי הענן.

#### **שימוש במכשירים ניידים**

148. שימוש במכשירים ניידים (לרבות מחשבים ניידים, טלפונים ניידים, טאבלטים וכיו"ב) יהיה כפוף להנחיות שלהלן:
- 148.1. מיופה כוח בתמורה יגבש מדיניות ארגונית לשימוש במכשירים ניידים, המתייחסת בין היתר, להגדרות אבטחה, עדכניות המערכות, אופן הגישה ליישומים ארגוניים, מחיקת נתונים מרחוק, ותהליכים מובנים לטיפול באובדן מכשיר. על המדיניות הארגונית להיבחן אחת לשנה ובמקרים של שינויים מהותיים.



406 עמ' 27

הממונה על שיתוף בנתוני אשראי: הוראה למיופה כוח בתמורה  
ניהול סיכונים אבטחת מידע והגנת הסייבר (12/22)

נתוני אשראי  
הקרדיט שמגיע לך



- 148.2. במקרה שבו מתאפשרת גישה למידע רגיש כחלק מהשימוש במכשירים ניידים שאינם מוגדרים ברשת הארגונית, לרבות גישה למידע רגיש בתיבות דואר אלקטרוני, מיופה כוח בתמורה יטמיע תהליך לניהול מכשירים ניידים.
- במסגרת תהליך זה, יוגדר כיצד תיושם המדיניות הארגונית, בין השאר באמצעות הקשחות ומנגנוני הגנה ובקרה על מכשירים ניידים שאינם מוגדרים ברשת הארגונית (כגון: מניעת דלף מידע, הצפנת תווך, הצפנת מידע רגיש לרבות מידע צרכני ועסקי במטרה למזער את הסיכון של חשיפת מידע רגיש, שימוש בסיסמא, נעילה אוטומטית לאחר פרק זמן, התקנת עדכוני תוכנה, בחינה תקופתית של הרשאות גישה שניתנו לאפליקציות הארגוניות).
- יובהר כי על מכשירים ניידים המוגדרים ברשת הארגונית יחולו כל דרישות הוראה זו.
- 148.3. מיופה כוח בתמורה יטמיע חוקים ייעודיים והתראות במערכת ה-SIEM עבור מכשירים ניידים שאינם מוגדרים ברשת הארגונית.
- 148.4. לא יתאפשר מתן שירות ללקוחות באמצעות מכשירים ניידים שאינם מוגדרים ברשת הארגונית.

#### מסירת מידע באמצעים דיגיטליים

149. מתן שירותים והעברת מסרים ממיופה כוח בתמורה אל לקוחותיו יכולה להתבצע באמצעים דיגיטליים בכפוף להוראות הבאות:
- 149.1. זיהוי מבקש המידע וקבלת הסכמתו להעברת מסרים;
- 149.2. בדיקה כי מבקש המידע רשאי לקבל את המידע;
- 149.3. בקשת מבקש המידע תתועד;
- 149.4. מתן אפשרות למבקש המידע לחזור בו מהסכמתו להעברת המסרים בכל עת.
150. מיופה כוח בתמורה ישמור כל מידע תפעולי לצורכי בקרה, ניהול ומעקב אחר קיום תנאי שליחת מידע באמצעים דיגיטליים.
151. יוטמעו חוקים ייעודיים והתראות במערכות ההגנה למניעת דלף מידע באמצעים לא מורשים.
152. מיופה כוח בתמורה יספק ללקוחותיו הנחיות המסייעות לנקיטת אמצעי זהירות לשמירה על פרטיות המידע, לרבות הנחיות המפרטות כיצד יש לנהוג במקרה של חשד לאירועי אבטחת מידע.

#### ניהול סיסמאות לקוח

153. מיופה כוח בתמורה יגדיר נהלים לוודוא חוזק סיסמה, שמירה על סודיותה, החלפת סיסמה ראשונית על ידי המשתמש ותוקף הסיסמה הראשונית.
154. סיסמה ראשונית, לרבות כזו הניתנת ללקוח בעת שחרור סיסמה, תימסר ללקוח באמצעות ערוץ תקשורת מאושר ע"י הלקוח כשהיא חסויה אף מהמוסר.
155. מיופה כוח בתמורה יזום החלפת סיסמה ראשונית ללקוח מיד לאחר ההתקשרות הראשונה וכן עדכון סיסמה אחת לתקופה.
156. מיופה כוח בתמורה ינקוט אמצעים 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.



157. מיזופה כוח בתמורה יבטל את הסיסמה, שנמסרה ללקוח, במקרים הבאים:  
157.1. הסיסמה הראשונית לא הופעלה תוך 7 ימים מהנפקתה.  
157.2. לבקשת הלקוח או אם קיים חשד שנעשה שימוש לא מורשה בסיסמה.  
157.3. לאחר מספר מסוים של ניסיונות כניסה כושלים, אשר בכל מקרה לא יעלה על חמישה ניסיונות כושלים רצופים.

#### משאבי אנוש והדרכה

158. במסגרת התהליך שתגדיר ההנהלה למיון וגיוס מועמדים בטרם העסקתם, יוגדרו עבור כל תפקיד הקיים בחברה רמות הסיווג הנדרשות ובדיקות הרקע שיש לבצע בעת הגיוס, תוך הקפדה על תיעוד תהליך הגיוס באופן נאות.
159. במקום הדרישות המופיעות בסעיף 92 לעניין תכנית הדרכה לעובדים, יחולו הדרישות שלהלן:  
מיזופה כוח בתמורה יגדיר ויישם תכנית הדרכה עבור כלל העובדים, בנושא אבטחת מידע אשר תותאם לאופי הפעילות של בעלי התפקידים השונים, ותכלול לוחות זמנים לביצוע ההדרכות. בין היתר, במסגרת תכנית ההדרכה יוגדר כי כלל העובדים נדרשים לעבור הדרכה בנושא אבטחת מידע לכל הפחות בתדירות שנתית, ואשר תתייחס, בין היתר, לנושאים הבאים:  
159.1. שימוש נאות במידע.  
159.2. כללי אבטחת מידע.  
159.3. איומים פנימיים וחיצוניים וסימנים מזהים עבור איומים אלו.
160. מיזופה כוח בתמורה יבצע הדרכות ייעודיות בהיבטי אבטחת מידע לבעלי תפקידים ספציפיים:  
160.1. גורמים בעלי גישה למשאבים רגישים.  
160.2. גורמים האמונים על זיהוי, טיפול ודיווח בעת אירוע אבטחה.
161. מיזופה כוח בתמורה יבצע קמפינים להעלאת המודעות בקרב העובדים בנושא הנדסה חברתית.

#### שמירה, גיבוי ושחזור של נתונים ומידע

162. מיזופה כוח בתמורה ישמור עותק גיבוי של הנתונים כאמור בסעיפים 100.1-100.4, באופן שיבטיח את שלמות המידע ואת אפשרות שחזור המידע במקרה של אובדן או הרס, למשל באמצעות שמירת הגיבוי באתר פיזי אחר.

#### **פרק ז – תחילה**

163. תחילתה של הוראה זו ביום פרסומה באתר מערכת נתוני אשראי בבנק ישראל (להלן - יום התחילה); ואולם, מיזופה כוח בתמורה אשר היה רשום במרשם הממונה ביום התחילה (להלן - מיזופה כוח בתמורה רשום), רשאי ליישמה לא יאוחר מ-3 חודשים מיום התחילה.
164. על אף האמור בסעיף 163, תחילתו של פרק ג' להוראה (דיווחים לממונה) ביום 5.9.2023.
165. על אף האמור בסעיפים 163 ו-164, תחילתו של סעיף 8.2 (דיווח על אירוע משמעותי שהתרחש או כמעט והתרחש בתחום ניהול המידע והגנתו) ביום התחילה גם לגבי מיזופה כוח בתמורה רשום.



## פרק ח' – מתכונת דיווחים לממונה

### הנחיות כלליות לדיווחים :

1. תאריך הדיווח - התאריך בו העביר מיופה הכוח את הדיווח לממונה.
2. פרטי ממלא הדוח בפועל – שם פרטי, שם משפחה ותפקיד של ממלא הדוח.
3. שם מיופה הכוח בתמורה – בהתאם למרשם מיופי הכוח בתמורה.
4. מזהה מיופה הכוח בתמורה - בהתאם למרשם מיופי הכוח בתמורה.
5. העברת הדיווח תתבצע באמצעות ממשק דיגיטלי באזור העסקי של מיופה הכוח בתמורה, בהתאם להנחיות שיינתנו על ידי הממונה בטרם מועד התחילה של הדיווחים, למעט הדיווח הנדרש לפי נספח ג' (דיווח על אירוע משמעותי שהתרחש או כמעט והתרחש, שיש לו השפעה על ניהול המידע והגנתו) שמועד תחילתו הינו עם פרסום ההוראה, ולפיכך יועבר לממונה על פי המפורט בסעיף ההבהרות של נספח ג', ורק בהמשך, יועבר באמצעות הממשק הדיגיטלי באזור העסקי בהתאם להנחיות שיינתנו כמפורט לעיל.

### נספח א' – מתכונת דיווח על סיווג לקבוצה

קבוצת סיווג				
DD/MM/YYYY				תאריך הדיווח
				שם מיופה הכוח בתמורה
				מזהה מיופה כוח בתמורה במרשם מיופי הכוח בתמורה
				פרטי ממלא הדוח בפועל
				מספר בעלי הרשאה
				מספר לקוחות
רבעון 4	רבעון 3	רבעון 2	רבעון 1	מספר דוחות שנמשכו בכל רבעון בשנה הקלנדרית
				נכלל בקבוצה (בהתאם לסעיף 4.1 בהוראה)



**נספח ב' – מתכונת דיווח על שינוי קבוצת סיווג**

שינוי קבוצת סיווג	
DD/MM/YYYY	תאריך הדיווח
	שם מיופה הכוח בתמורה
	מזהה מיופה כוח בתמורה במרשם מיופי הכוח בתמורה
	פרטי ממלא הדוח בפועל
	תאריך השינוי
לפני השינוי	
	מספר בעלי הרשאה
	מספר לקוחות
	מספר דוחות ריכוז נתונים שנמשכו ברבעון הקלנדרי הקודם
	נכלל בקבוצה (על פי סעיף 4.1 בהוראה)
לאחר השינוי	
	מספר בעלי הרשאה
	מספר לקוחות
	מספר דוחות ריכוז נתונים שנמשכו ברבעון הקלנדרי האחרון
	נכלל בקבוצה (על פי סעיף 4.1 בהוראה)



406 עמי 31

הממונה על שיתוף בנתוני אשראי: הוראה למיופה כוח בתמורה  
ניהול סיכוני אבטחת מידע והגנת הסייבר (12/22)

נתוני אשראי  
הקרדיט שמגיע לך



**נספח ג' - מתכונת דיווח על אירוע משמעותי שהתרחש או כמעט והתרחש, שיש לו השפעה על ניהול המידע**

**והגנתו**

אירוע בתחום ניהול המידע והגנתו	
DD/MM/YYYY	תאריך הדיווח
	שם מיופה הכוח בתמורה
	מזהה מיופה כוח בתמורה במרשם מיופי הכוח בתמורה
שם פרטי ושם משפחה: _____ דוא"ל: _____ מס' טלפון: _____	פרטי ממלא הדוח בפועל
יש לסמן את סוג הדיווח: <input type="checkbox"/> דיווח ראשוני <input type="checkbox"/> דיווח משלים <input type="checkbox"/> דיווח על התפתחויות מהותיות במהלך האירוע <input type="checkbox"/> דיווח על סיום האירוע <input type="checkbox"/> דיווח על אירוע שכמעט והתרחש דוח הפקת לקחים והמלצות ליישום	סוג הדיווח
מלל חופשי	תיאור האירוע (לרבות פירוט פגיעה במידע/ תהליכים/ מערכות/לקוחות/ נזק אחר כולל כספי, ככל שרלוונטי)
DD/MM/YYYY שעה: _____	מועד זיהוי האירוע
DD/MM/YYYY שעה: _____	מועד משוער של תחילת האירוע
DD/MM/YYYY שעה: _____	מועד סיום האירוע (בהתאם לקביעת ההנהלה)
מלל חופשי	הפערים שאפשרו את התרחשות האירוע
מלל חופשי	התפתחויות מהותיות, ככל שאירעו
מלל חופשי	אופן הטיפול באירוע
מלל חופשי (יש לצרף דוח)	הפקת לקחים מהאירוע והמלצות ליישום
שם הרשות / המאסדר: _____ הגורם אליו הועבר הדיווח: _____ תאריך העברת הדיווח: DD/MM/YYYY	האם האירוע דווח לרשות להגנת הפרטיות או לרשות אכיפה או למאסדר אחר של נתן השירות

**הבהרות:**

- 1 - **דיווחים בכתב** יש להעביר באמצעי מאובטח קיים בין מיופה הכוח לממונה או לדוא"ל: [Pbcd@boi.org.il](mailto:Pbcd@boi.org.il), תוך סגירת קובץ הדיווח בסיסמה שתימסר טלפונית לנציגי הממונה.
- 2 - **דיווח ראשוני** יימסר תוך שעתיים ממועד זיהוי האירוע כמחייב דיווח. ככל שהדיווח הראשוני יימסר טלפונית הוא יועבר על פי פרטי הקשר שנמסרו למיופה הכוח בתמורה. ככל שהדיווח הראשוני יימסר בכתב הוא יועבר בהתאם למפורט בסעיף 1 לעיל, תוך מילוי הפרטים הידועים בעת מסירת הדיווח. בנוסף, יש לוודא קבלתו ע"י נציגי הממונה בסמוך לאחר שליחתו.
- 3 - **דיווח משלים** יימסר תוך 8 שעות ממועד הדיווח הראשוני, תוך מילוי הפרטים הידועים בעת מסירת הדיווח.

**נספח ד' - מתכונת דיווח על אירוע צפוי בעל השפעה מהותית על ניהול המידע והגנתו**



הממונה על שיתוף בנתוני אשראי : הוראה למיופה כוח בתמורה  
ניהול סיכוני אבטחת מידע והגנת הסייבר (12/22)

**נתוני אשראי**  
הקרדיט שמגיע לך



אירוע צפוי בעל השפעה מהותית על ניהול המידע והגנתו	
DD/MM/YYYY	תאריך הדיווח
	שם מיופה הכוח בתמורה
	מזהה מיופה כוח בתמורה במרשם מיופי הכוח בתמורה
	פרטי ממלא הדוח בפועל
מלל חופשי	נושא האירוע
מלל חופשי	תיאור האירוע והשפעתו
DD/MM/YYYY	צפי למימוש





**נספח ה' – מתכונת דיווח על שירות טכנולוגי חדש**

שירות חדש	
DD/MM/YYYY	תאריך הדיווח
	שם מיופה הכוח בתמורה
	מזהה מיופה כוח בתמורה במרשם מיופי הכוח בתמורה
	פרטי ממלא הדוח בפועל
	שם השירות החדש
מלל חופשי	תיאור השירות
טרם אושר/ אושר חלקית/ אושר במלואו/ יעוץ משפטי/ממונה אבטחת מידע/ הנהלה/ דירקטוריון תאריך האישור	סטטוס אישורים והגורם המאשר
יש לצרף	תכנית עבודה לעמידה בדרישות נוספות שיחולו בעקבות שינוי סיווג, ככל שרלוונטי
יש לצרף	סקר סיכונים הממפה את כלל הסיכונים הכרוכים בפעילות, והכלים האמצעים והתהליכים לניטור ובקרה במטרה לצמצם