משרד הביטחון

יחידת "רב-מגן" | תוה"ג

תקן רב-מגן ❷

הגנה בסייבר למידע ביטחוני

בראי חברה/ספק בשרשרת האספקה של תעשיות וספקים ביטחוניים

DoD High Assessment & NIST SP 800-171 Compatible

גרסה

גרסה 05

תאריך תוקף

16 אוגוסט, 2022

תאריך עדכון

28 ספטמבר, 2023

רמה

-	2	-	-	-

רמה 2 – בינונית

תואמת CMMC

- המסמך אינו מסווג UNCLASSIFIED -

אודות המסמך

כותרת	**תקן רב-מגן 2 – הגנה בסייבר למידע ביטחוני**
	בראי חברה/ספק ביטחוני בשרשרת האספקה של מערכת הביטחון
מחברים	עמית ר., גלית ב. – משרד הביטחון
מס' גרסה (מהדורה)	05
נגזרת רמה	רמה 2 – בינונית, תואמת DoD High Assessment & NIST SP 800-171
סטאטוס	גרסא פומבית – לתיקוף, הערות ומשובים
סיווג	לא מסווג – בלמ"ס – UNCLASSIFIED
שם קובץ	RAV-MAGEN-L2-Vxx.pdf (xx = מספר הגרסה)
מס' עמודים	79
סימון	RM-2

היסטוריה 5 גרסאות אחרונות

גרסה	תאריך	רשימת שינויים
05	18/10/2023	גרסה פומבית לאתר רב-מגן
04	28/09/2023	גרסה לתיקוף
03	23/02/2023	טיוטה שנייה – Draft
02	16/08/2022	טיוטה שנייה – Draft

מסמך זה נכתב ע"י הממונה על ההגנה בסייבר במשרד הביטחון כחלק מן התכנית להגנה על מידע ביטחוני של מערכת הביטחון במדינת ישראל. כל הזכויות שמורות למשרד הביטחון.

יש להשתמש בגרסה המקורית, המלאה והעדכנית של מסמך זה כפי שמופיע בפרסומים. הנוסח המופיע במסמך זה הוא הקובע. אין לבצע שינויים בכיתוב או בנוסח הוראות תקן זה. אין להעביר לגורם אחר חלקים מתקן זה, משמעות התקן בשלמותו.

מסמך זה מהווה תקן המבוסס על תכנית ההגנה על הרכש ושרשרת האספקה של משרד ההגנה ארה"ב תחת מסגרות DFARS, CMMC ו-NIST ובהרשאתם.

משרד הביטחון לא ישא באחריות לכל נזק ישיר ו/או עקיף, תוצאתי, מיוחד ו/או עונשי שייגרם לכל ארגון, לשותפיו, לעובדיו ו/או לצדדים שלישיים, לרבות הפסד כספי, אובדן נתונים, אובדן זמן מחשב, שחזור תוכנות, רכישות מוצרים ו/או צורך בקבלת שירותים חלופיים (כגון: עלות כיסוי), עלויות זמן השבתה וכל נזק אחר כתוצאה משימוש בתקן זה.

התייחסויות לתוכן המסמך ניתן להעביר באימייל ל- **ravmagen@mod.gov.il**

תוכן עניינים

1 הקדמה 5

1.1 סקירה כללית 5

1.2 קהל היעד 6

1.3 מטרת התקן 7

1.4 היבטים לזכויות השימוש בתקן 7

1.5 סקירת רמות התקינה 7

2 מידע ביטחוני 9

2.1 מטרה 9

2.2 סמכות 9

2.3 הגדרה ותבחינים 9

3 תהליך השימוש בתקן 13

3.1 הצגת התהליך 13

3.2 תכנון והכנה למבדק תאימות 13

3.3 ביצוע מבדק תאימות פנימי 15

3.4 ביצוע מבדק תאימות ע"י בודק המוסמך 17

3.5 דיווח תוצאות המבדק 22

3.6 הסמכה 23

4 תיחום 25

4.1 הקדמה 25

4.2 קטגוריות לתיחום נכסים 25

4.3 הגדרת רמת הבדיקה 26

4.4 התוצר הנדרש 27

5 אופן ביצוע מבדק התאימות 28

5.1 מטרה 28

5.2 שיטות 28

5.3 תבחינים להערכת מידת ההתאמה של המענה מול הדרישה 29

5.4 אותנטיות המימצאים 29

5.5 סיכום מימצאים כרמת התאמה 30

5.6 דוח מסכם 30

6 רשימת הדרישות 31

7 ניקוד וציון ההתאמה הכללי 71

7.1 אופן חישוב הניקוד מול סעיף דרישה 71

7.2 חישוב ציון ההתאמה הכללי 72

7.3 טבלת ניקוד 72

8 **הגדרות ומונחים** 77
8.1 טבלת ראשי תיבות בשימוש 77

1 הקדמה

1.1 סקירה כללית

יחידת "רב-מגן" במשרד הביטחון הינה גוף האחראי בין היתר על אבטחת המידע וההגנה בסייבר על משרד הביטחון, על יחידות הסמך ועל התעשיות הביטחוניות הישראליות (שייקראו להלן: "גופי הביטחון"). בתוך כך, היחידה פועלת לממש את אחריותה להגנת המידע הביטחוני המצוי בארגונים אלו, זאת באמצעות קביעת מדיניות, מתן הנחיות אופרטיביות וביצוע שגרת פיקוח ובקרה על הגופים הביטחוניים.

גופי הביטחון מתקשרים בהסכמים עם חברות צד-שלישי רבות המספקות עבורן מוצרים ושירותים שונים. חברות אלו הינן ספקיות המרכיבות את שרשרת האספקה של גופי הביטחון (להלן: "שרשרת האספקה"). לצורך אספקת המוצרים והשירותים על פי דרישות גופי הביטחון, על פי רוב, הספקים עושים שימוש במידע ביטחוני.

עבודת גופי הביטחון מול חברות שרשרת האספקה מגדילה את מרחב סיכוני הסייבר עבורן – סיכונים העלולים להתרחש למשל כתוצאה מרמת אבטחת מידע שאינה מספקת בחצרות הספק. בשנים האחרונות אף חל גידול משמעותי במספר תקיפות הסייבר על ארגונים שהינם ספקים של ארגונים אחרים, תוך ניצול האמון שהארגון נותן לספק שלו, ומכאן לבצע חדירה אל ארגון היעד. לצורך צמצום הסיכונים מסוג זה, גופי הביטחון נדרשים להשלים את מעטפת ההגנה בארגונם ולהחיל אותה גם על החברות בשרשרת האספקה שלהם.

כלל החברות והספקים בשרשרת האספקה של גופי הביטחון לרבות קבלני המשנה שלהם, מהווים אם כן גורם בעל חשיבות רבה למערכת הביטחון. ההצלחה של ארגונים אלו להגן בצורה אפקטיבית על המידע הביטחוני ועל תוצריו משפיעה בצורה ישירה על הפחתת רמת סיכוני הסייבר הכללית של מערכת הביטחון.

מכאן, ספקים וחברות בשרשרת האספקה של מערכת הביטחון נדרשים להגן על המידע הביטחוני אשר הועבר, מוחזק, מעובד בתשתיותיהם, לרבות להגן על התוצרים אשר פותחו באמצעות המידע הביטחוני, לדרוש ולהציב את התנאים לשימור רצף ההגנה גם בשרשרת האספקה שלהם – אצל נותני השירותים וקבלני המשנה שלהם עצמם.

תקן "רב־מגן" פותח לטובת העלאת רמת ההגנה בסייבר על סביבות מיחשוביות המטפלות באופן ישיר או עקיף במידע ביטחוני וזאת באמצעות הצבת דרישות למיסוד תהליכים ואמצעים לאבטחת מידע המותאמים לארגונים וחברות בשרשרת האספקה. התקן הותאם למספר רמות הגנה במדרג עולה.

התקנות למימוש אבטחת המידע וההגנה בסייבר באמצעות תשתית תקינה זו יחולו על מערך הגופים המונחים של משרד הביטחון, כאשר אלו נדרשים לאכוף את מימוש התקינה בשרשרת האספקה שלהם באמצעות קשירת הסכמים וחוזים מול החברות והספקים אשר יקבלו על עצמם כפיפות חוזית ליישום דרישות תקן זה בארגונם.

תקן זה משמש כסטנדרט המקצועי לאבטחת מידע והגנה בסייבר על מידע ביטחוני בארגון, אשר נדרש להגן בצורה נאותה ואפקטיבית על המידע והתוצרים הביטחוניים במסגרת פעילותו המבוצעת עבור גופי הביטחון מזמיני העבודה.

דרישות ההגנה המופיעות בתקן מיועדות להגנה על מידע ביטחוני בתצורתו הפיזית או הדיגיטאלית, הנדרש בהגנה כאשר הוא מוחזק, מאוחסן, מעובד, מועבר ו/או משודר על גבי או בין רכיבים מחשוביים, במערכות תקשוביות ובתהליכים ארגוניים. התקן מגדיר את מרחב היישום של מטעפת ההגנה לכלול את המערכות והסביבות הכרוכות בטיפול במידע ביטחוני.

התקן מכיל חלוקה לחמש רמות תקינה ובסדר עולה של רמת ההגנה. שלוש רמות ראשונות; בסיסית, בינונית וגבוהה, הינן רמות אשר דרישותיהן אינן מסווגות ולפיכך יופיעו בפרסומים גלויים. שתי רמות הגנה גבוהות יותר; רמה מתקדמת ורמה אקטיבית, הינן רמות הכוללות דרישות הגנה מתקדמות יותר המיועדות להתמודדות מול איומים, תרחישים ויכולות בסדר גודל של מדינה. רמות הגנה אלו לא מופיעות בפרסומים גלויים ומועברות על פי הצורך למורשים בלבד.

רמת ההגנה הנדרשת עבור הספק תוגדר לו כחלק מחוזה תכולת העבודה.

1.2 קהל היעד

תקן זה מיועד לשימוש בארגונים אשר הינם גופי ביטחון, חברות בשרשרת האספקה של גופי הביטחון, חברות המעוניינות להיות ספק של משרד הביטחון, חברות המבקשות להיות ספק בשרשרת האספקה של גוף ביטחוני זר בעל הסכם ביטחון מול משרד הביטחון, או עבור כל חברה אחרת אשר קיבלה דרישה לעמידה בדרישות תקן זה.

יישום אבטחת המידע בארגון, לרבות יישום דרישות תקן מסוג זה, מבוצע בארגון על ידי בעלי התפקיד הייעודיים לנושא אבטחת מידע, אלו מגיעים מן הארגון עצמו, או בשילוב מומחי תוכן חיצוניים.

התקן מותאם ככלי מקצועי לשימוש עבור קהל היעד המקצועי ובעלי התפקיד, להלן –

- הממונה על אבטחת המידע / הגנה בסייבר בארגון – על פי רוב CISO.
- בודק תאימות סייבר.
- סוקר / מעריך.

בעלי עניין אחרים השותפים לפעילות ההגנה בסייבר –

- מנהלי אבטחת מידע והגנת סייבר.
- מנהלי מערכות מידע.
- מנהלי מערכי הגנה בסייבר: ארכיטקטים, מיישמים, מגינים, בודקים, אנליסטים, חוקרים וכד'.
- מנהלי מערכות מחשב IT, אדמיניסטרטורים.
- מנהלי סיכונים, רגולציה, פיקוח וביקורת.
- מנהלי רכש או קניינים.
- קב"טים (קציני ביטחון).

בעלי תפקיד אחרים אצל שותפים וספקי שירותים מחוץ לארגון –

- בודקי תאימות הגנה בסייבר, סוקרים ומעריכים.
- ספקי שירותי ייעוץ והגנה בסייבר לארגון – לדוג' MSSPs.
- ספקי שירותי IT לארגון.
- ספקי תשתיות, פלטפורמות ושירותים אפליקטיביים בענן.

גורמים אחרים – כל גורם נוסף בעל עניין במידע המוגדר בתקן זה, ולכל מטרה; בקרה, לימוד, מחקר, או אחרת.

1.3 מטרת התקן

הגדרת סטנדרט מקצועי אחיד להגנה בסייבר על מידע ביטחוני עבור חברות אשר הינן חלק משרשרת האספקה של גופי הביטחון.

הוראות התקן נועדו לתת כלים למזער ככל הניתן את הסיכונים לגרימת נזק ביטחוני הכרוך בדלף של מידע ביטחוני, שיבושו, או יצירת פגיעה בתהליכים טכנולוגיים, במערכות ממוחשבות או בתוצרים המיועדים בהמשך הדרך להשתלב אל מערכות הביטחון.

תקן זה מכתיב הנחיות ודרישות מקצועיות הנוגעות לביצוע מבדק תאימות להגנה בסייבר על מערכות ממוחשבות להן יש קשר ישיר או עקיף למידע ביטחוני.

1.4 היבטים לזכויות השימוש בתקן

להלן היבטים שונים לנושא זכויות השימוש בתקן זה –

- מסגרת התכנית להגנה על מידע ביטחוני בגופי הביטחון ובשרשרת האספקה מותאמת ככל האפשר לתקינות אזרחיות/בינלאומיות נפוצות תוך שילוב ידע קיים בתצורתו כ- Best Practices. בכך מושגת תמיכה רחבה לתקן המשלבת גופים מסחריים רבים.
- בין השאר, התקן מותאם לתכנית ההגנה על הרכש ושרשרת האספקה של משרד ההגנה ארה"ב תחת מסגרות DFARS, CMMC ו-NIST ובהרשאתם.
- אין לעשות שימוש בהוראות תקן זה כדי לסתור תקינה אחרת או הנחיות רגולציה אחרות.
- משרד הביטחון מתיר ומעודד את השימוש בתקן זה על בסיס התנדבותי עבור כל ארגון המבקש להגן על המידע הקנייני שלו, גם במצב בו לא קיימת עבורו כל כפיפות לרגולציה ביטחונית. מוטב להשתמש בגרסת התקן השלמה והעדכנית ולא להשתמש בשכתובים או בנגזרות מתוכו.
- גורמי עניין מוזמנים לעיין בטיוטות הפרסומים במהלך שלב ההערות הציבוריות ולספק משוב למחברים.

1.5 סקירת רמות התקינה

תקן "רב-מגן" מכיל חמש רמות של תקינה. סולם רמות התקינה נבנה עבור פרופילים שונים של ארגונים בעלי רגישות ביטחונית או אופי שימוש במידע ביטחוני שונה, ועוד. הרמות מוגדרות בסדר עולה על פי רמת ההגנה אותה היא מיועדת להשיג. כל רמה מכילה את תכולת הדרישות של הרמות תחתיה.

הרמה המיוחסת לביצוע תיקבע על ידי הגוף הביטחוני המזמין לבין הספק כחלק מהתנאים הביטחוניים אשר יופיעו בהסכם ההתקשרות בין הצדדים, ובכפוף להנחיות משרד הביטחון.

שים לב כי חוברת תקן זו, הינה בלתי מסווגת, מפורסמת פומבי, מכילה את נגזרת הדרישות המתאימות לרמה 2, ואינה מכילה את הסט הדרישות השלם.

להלן סקירה כללית של כלל רמות ההגנה הקיימות בתקן "רב-מגן":

רמה	שם	ייעוד ומאפיינים עיקריים	חשיפה
רמה 1	בסיסית	הגנה בסיסית על תשתיות רשת ארגונית מוגדרת, תחת העקרונות של הקשחת אמצעים מיחשוביים ויצירת חסימות באמצעים ושיטות מומלצות, עם הפעלת אמצעי הגנה באופן פרטני וממוקד, זאת כנגד איומים של גישה לא מורשית, ותקיפות בלתי ממוקדות במתווים נפוצים תחת רמת מורכבות בסיסית. רמה זו אינה מיועדת להגנה על רשתות או מידע מסווג.	פומבית; בלתי מסווג
רמה 2	בינונית	הגנה על מידע ביטחוני אשר נשמר, מעובד, ומועבר על גבי תשתיות ארגוניות המתאפיינות באמצעים דיגיטאליים תקשוביים נפוצים ושגורים, עם השימוש במערכות הגנה מסחריות נפוצות, כאשר לארגון עובדים וגבולות רשת מוגדרים, זאת בהתאמה מול איומים של דלף מידע (בהיקף ובמיקום מוגדר), כנגד מתקפות בתרחישים נפוצים, תקיפות בלתי ממוקדות בעלות חתימה, אשר מקור נגישותן הוא מרשת האינטרנט או מנגישות פנימית. רמה זו אינה מיועדת להגנה על רשתות או מידע מסווג. רמה זו תואמת לתקן CMMC Level 2.	פומבית; בלתי מסווג
רמה 3	גבוהה	הרחבת הטיפול ההגנתי לכלול משטחי תקיפה רחבים יותר, בשילוב עם מערכי הגנה מרכזיים, רציפים, רחבים, המפיקים תובנות ומתאימים את פעילותם לצמצום האיומים, ולאיתור מתקפות מורכבות ומשתנות, לרבות מתקפות ממוקדות מהסוג APT. המערך מופעל ע"י גורמים מקצועיים מאומתים. הרחבת הטיפול לכלול מתארים להשבתת הרציפות התפקודית. רמה זו אינה מיועדת להגנה על רשתות או מידע מסווג.	פומבית; בלתי מסווג
רמה 4	מתקדמת	העלאת רמת הטיפול ההגנתי הנדרש עבור רשתות מסווגות ומבודלות, יצירת מומחיות בהגנה הכוללת שימוש באמצעים ושיטות קנייניות, מיטביות, תוך הרחבת סט האיומים לכלול ריגול תעשייתי, שיבוש מידע, השבתת שירותים רגישים והגנה בפני יצירת נזק ביטחוני עבור תוצרי הפעילות הארגונית מן הסוגים למשל: רכיבים פיסיים, רכיבי תוכנה או רכיבים רגישים אחרים.	מוגבלת; מסווג כשמור
רמה 5	אקטיבית	הרחבת הטיפול ההגנתי לכלול אמצעים ושיטות פרו-אקטיביות, אוטומטיות וחשאיות, לאיתור פעילות עוינת קיימת ברמת מורכבות של מדינה ומעלה.	מוגבלת; מסווג כשמור

תקינה מסווגת תועבר, על פי הצורך, תחת מעטפת ביטחונית רלוונטית לחברות וספקים ביטחוניים.

2 מידע ביטחוני

2.1 מטרה

פרק זה סוקר ומגדיר מהו "מידע ביטחוני מפוקח" ומהו המידע הנדרש בהגנה. כל מידע אחר אשר אינו עומד בתבחינים של "מידע מפוקח" (לדוגמא סוד מסחרי, מידע פרטי, מידע ציבורי, וכד') אינו נדרש בהגנה על פי המוגדר בתקן זה.

בכל מקום בו מופיע בתקן זה המונח "מידע ביטחוני" או בתצורות דומות כ- "מידע מפוקח" או בהרחבה "מידע ביטחוני מפוקח" – יש להתייחס למונח ע"פ ההגדרה המופיעה בפרק זה.

2.2 סמכות

מידע ביטחוני, בעליו הינה מדינת ישראל. משרד הביטחון מחזיק בסמכות הבלעדית לקביעה והגדרה מהו מידע ביטחוני מפוקח – כזה הנדרש בהגנה. משרד הביטחון האציל סמכותו לביצוע הגדרות סיווג למידע ביטחוני למספר גופים מונחים, כאשר הגדרה זו מבוצעת בגופים אלו באמצעות קציני ביטחון מוסמכים – ממוני ביטחון של משרד הביטחון.

אין בסמכותו של אף גורם לשנות הגדרה של מידע ביטחוני או לשנות את קביעת סיווגו של מידע אשר סומן או הוגדר קודם לכן על ידי קצין ביטחון מוסמך. בסמכותו של קצין ביטחון מוסמך לקבוע מחדש או לשנות סיווג של מידע ביטחוני.

ככל שהתקבל בארגון מידע כלשהו ממקור ביטחוני, לגביו קיימת סבירות כי הוא מידע ביטחוני, הגם שלא סומן כך, יש להחשיבו כמידע ביטחוני, לשמרו תחת מעטפת הגנה, ולהפנות את המקרה לטיפול קצין הביטחון בהקדם.

מידע ביטחוני אשר בעליו היא מדינה זרה המטופל תחת הסכם ביטחון עם משרד הביטחון, יטופל במסגרת הביטחונית הקיימת ועל פי סימון סיווגו כאילו היה מידע ביטחוני ישראלי.

2.3 הגדרה ותבחינים

פרק זה מגדיר את המונח "מידע ביטחוני" ואת רשימת התבחינים על פי הם יוגדר מידע כ- "מידע ביטחוני" הנדרש בהגנה על פי תקן זה.

נבדיל בין "מידע עסקי", הוא מידע קנייני של הארגון, מידע אזרחי שאינו ביטחוני, לבין "מידע ביטחוני" אשר התקבל מגוף ביטחוני ומסומן בסיווג מרמת "בלמ"ס" ועד ל"סודי ביותר". אבחנת רמת הסיווג נקבעת על פי רמת הנזק העלול להיגרם לביטחון המדינה במקרה של חשיפת המידע לגורם שאינו מורשה.

מידע ביטחוני נדרש תמיד להיות תחת פיקוח ביטחוני משום הינו תמיד מוגבל בחשיפתו בו אין לחשפו לגורמים לא מורשים. כל זה לרבות מידע המוגדר כ"בלמ"ס" (מוגבל), כאשר גם במקרה זה נדרש להגן עליו מפני חשיפה לבלתי מורשים.

יוצא דופן הוא מידע בלמ"ס פומבי, המוגדר כמיועד לחשיפה לציבור, כך שלא ניתן להגביל תפוצתו ומותר הוא בחשיפה לכל גורם, ומשכך גם לא ניתן לבצע עליו פיקוח ביטחוני ולא נדרש בעבורו יישום של מעטפת הגנה. מידע בלמ"ס פומבי אינו מפוקח ביטחונית.

> ***מידע ביטחוני מפוקח*** – מידע אשר גוף ביטחוני הינו בעליו או כזה אשר נקבע והוגדר כמידע ביטחוני אותו אין לחשוף לגורם שאינו מורשה, משום שחשיפת המידע עלולה לפגוע בארגון אשר המידע הוא בבעלותו ו/או בביטחון המדינה.

ראה בתרשים להלן –

כאשר פריט המידע מוגדר כ"מפוקח ביטחונית" הינו נדרש בהגנה מפני חשיפה שלא לצורך, ו/או הגנה מפני פגיעה בשלמותו או זמינותו. הטיפול הביטחוני כרוך ביישום מעטפת הגנה ארגונית נאותה להגנת המידע בתשתיות הארגון המצריך הרכבת אמצעים ומערכות ייעודיות להגנה בסייבר.

מידע ביטחוני מפוקח יוגדר ככזה עבור כל פריט מידע אשר מקורו ממערכת הביטחון, או תצורתו הנוכחית הינה נגזרת של מידע ממקור זה, בתצורתו הפיזית או הדיגיטלית, מידע האגור או המשולב ברכיב מיחשובי, עבורו קיימת תאימות מלאה או חלקית <u>לאחד או יותר מן התבחינים</u> המופיעים בטבלה להלן –

טבלת תבחינים למידע ביטחוני מפוקח	
#	**התבחין** (כולל את ההקשר הביטחוני)
א.	המידע מוגדר במפורש על ידי משרד הביטחון ו/או שבעליו הינו גוף ביטחוני במערכת הביטחון, מזמין העבודה כ"מידע ביטחוני מפוקח" או מידע המסומן כ- "<u>בלמ"ס</u>", עימו נרשם עוד "מוגבל" או "רגיש" או "מפוקח".
ב.	המידע <u>מסווג</u> וכולל את הגדרת הסיווג <u>הביטחוני</u> ביחס אליו, ומסומן כ- "שמור", "סודי" או "סודי ביותר".
ג.	מידע אשר תוכנו נדרש להיות ברמת אמינות גבוהה (Integrity), שלמות

	מלאה וללא שיבוש/שינוי עוין, אשר ישולב בהמשך הדרך בהפקת תוצרים ביטחוניים.
ד.	רכיב, תוצר או מוצר המופק, מעובד, מפותח, או מיוצר כתוצאה משימוש במידע מסווג אשר מכיל נגזרת של המידע המסווג.
ה.	מידע המאפשר "הרכבת תמונה" או הפקת משמעויות ביטחונית המבוקשות להסתרה.
ו.	מידע הכולל אגד רשומות (מסד נתונים) של פרטים אישיים, פרטי התקשרות, תמונות, כשירות ביטחונית, מידע תעסוקתי או אחר אשר עלול לחשוף עובדים בגופים ביטחוניים, תפקידם או את הקשרים ביניהם לפרויקטים ביטחוניים.
ז.	מידע הכולל רשומות רכש, רשומות BOM (Bill of Materials), רשומות ספקים ותשלומים, אבני דרך וכד', אשר עלולות לחשוף את קשרי הגומלין בשרשרת האספקה, לוחות זמנים ו/או כל מידע הרלוונטי לתוצרים ביטחוניים.
ח.	מידע מסווג מסוג תכן הנדסי הכולל, בין השאר, תרשימים טכניים, קוד תוכנה, קונפיגורציות, מפרטים שונים, המשמשים לפיתוח וייצור של רכיבים המיועדים להיות משולבים בתוצרים ביטחוניים.
ט.	מידע תקשובי IT ו/או מידע אודות מערך הגנה בסייבר הארגוני אשר עצם חשיפתם תוביל לפגיעה במערכי ההגנה האמונים על הגנת המידע הביטחוני.
י.	מידע בבעלות משרד ההגנה האמריקאי (DoD) שאינו לפרסום ציבורי, או המסופק על ידו, או הנוצר עבורו, אשר מוגדר על ידי בעליו ומסומן כמידע ביטחוני אמריקאי באחת מן ההגדרות הבאות - א. CUI (Controlled Unclassified Information) – הגדרת ממשל אמריקאית למידע בלמ"ס המפוקח ביטחונית – מידע רגיש הנקשר למידע אישי, מידע עסקי חסוי, מידע טכני, ועוד. ב. FCI (Federal Contract Information) – מידע מפוקח הנקשר לחוזים, הצעות, תהליכי מכרז והתכתבויות בהקשרים אלו. ג. CDI (Covered Defense Information) / UCTI (Unclassified Controlled Technical Information) – מידע ביטחוני תחת הגדרות משרד ההגנה האמריקאי ותקנות רכש DFARS. • DoD – U.S. Department of Defense • DFARS – U.S. Defense Federal Acquisition Regulation Supplement
י"א.	מידע מגורם זר (גוף ביטחוני זר בעל הסכם ביטחוני עם מדינת ישראל) אשר מוגדר על ידי בעליו ומסומן בהגדרות סיווג ביטחוניות, למשל – - OFFICIAL SENSITIVE – הגדרות סיווג למידע ביטחוני בריטי.

	- FOUO (For Official Use Only) - RESTRICTED – הגדרת סיווג למידע בחלק ממדינות נאט"ו (גרמניה, קנדה, ועוד)
י"ב.	מידע המוגבל בייצוא מישראל תחת הנחיות משרד הביטחון וחוק הפיקוח על הייצוא.

3 תהליך השימוש בתקן

3.1 הצגת התהליך

ארגון המעוניין לעמוד בתקן זה, נדרש להראות ולהוכיח כי הוא מתנהל על פי הדרישות המפורטות בתקן והינו מיישם את מערך הדרישות ברמת תאימות מספקת.

בסופו של התהליך, בודק מוסמך, אשר רשאי להמליץ לגוף המסמיך, יבצע מבדק תאימות אשר יוודא כי קיימת תאימות מספקת בין דרישות התקן לבין התנהלות הארגון, ועל כך ייתן המלצתו.

תעודת הסמכה ניתנת לארגון לאחר שהארגון נבדק והומלץ על ידי הבודק המוסמך כי הוא מתאים ומקיים את דרישות התקן.

פרק זה סוקר את התהליכים הנדרשים לביצוע תחת הנחיות תקן זה. התהליך השלם עד להשגת ההסמכה כולל חמישה שלבים –

- שלב 1: תכנון והכנה למבדק תאימות
- שלב 2: ביצוע מבדק תאימות פנימי
- שלב 3: ביצוע מבדק תאימות ע"י בודק מוסמך
- שלב 4: דיווח תוצאות מבדק התאימות
- שלב 5: הסמכה

3.2 תכנון והכנה למבדק תאימות

תהליך מבדק התאימות נכון ויעיל אשר יניב תרומה ביטחונית לארגון נדרש להתחיל בתכנון מאורגן היטב. שלב התכנון וההכנה הוא הבסיס הקריטי להצלחת התהליך כולו. שלב זה, על כל פעילויותיו המוגדרות, נדרש בהשלמה כדי להבטיח את הביצוע הנכון והעקבי של מבדק התאימות לטובת קבלת ההסמכה בהמשך. להלן השלבים והתוצרים הנדרשים לשלב זה –

3.2.1 בניין הכוח בארגון

תהליך מבדק התאימות דורש מעורבות ושיתוף פעולה של גורמים שונים בארגון. כאשר בשלב ראשון נדרש הארגון להגדיר את בעלי התפקיד הרלוונטים, להגדיר להם את אחריותם, לתת להם סמכויות, להקצותם עבור המשימות בתכנית העבודה, להקצות עבורם את המשאבים הנדרשים, ולגבש כצוות עבודה שיוביל את המשימה הכוללת.

בתהליך זה ניתן להיעזר בגורמים מקצועיים חיצוניים אשר הינם בעלי ניסיון מוכח בתהליכי הסמכה לתקינה טכנולוגית.

להלן דגשים לתפקידים אותם יש להגדיר ולאייש במסגרת צוות העבודה: (אין מניעה כי אותו האדם ימלא יותר מתפקיד אחד)

א. **מוביל מבדק התאימות** – הנציג הבכיר ביותר שהינו עובד הארגון אשר באחריותו להוביל את מבדק התאימות מתחילתו ועד הסמכת הארגון, והוא מבצע זאת באמצעות סמכויותיו לקבל החלטות עבור הארגון בכל הדרוש לעמידה בדרישות תקן זה, כגון: תכנון והנעה של תהליכים, הקצאת משאבים, רכישה והטמעה של מערכות, מציאת פתרונות וכדומה.

ב. **מוביל אבטחת מידע / הגנה בסייבר** – איש אבטחת מידע / הגנה בסייבר בעל ידע וניסיון מתאימים אשר אחראי להבטיח את דיוק התהליך ונכונות התיעוד המופק ממנו. בעל סמכות לבצע בדיקות מסוגים שונים בעזרת אנשי הארגון בתפקידים השונים עד להגעה למיצוי החלטתו המקצועית. נותן את חתימתו על המבדק תאימות הפנימי. הנציג פועל בשם הארגון אך אינו חייב להיות עובד הארגון.

ג. **חבר/י צוות בודקי תאימות** – אנשי מקצועה בהגנת הסייבר המבצעים את תהליך מבדק התאימות באמצעות תשאול, צפייה במידע ובדיקות תוך איסוף ראיות רלוונטיות וניתוח כלל המידע שנאסף לטובת גיבוש רמות ההתאמה ומיפוי הפערים מול דרישות התקן.

ד. **נציג IT** – נציג בכיר מטעם מחלקת ה- IT (תשתיות מיחשוביות ויישומים ארגוניים) בארגון, האחראי על שיתוף הפעולה, התיווך, והנגשת הידע הטכנולוגי אודות מערכות הארגון לצוות התאימות על פי בקשותיו.

ה. **מנהל ארגוני בכיר** – מנהל בכיר בארגון אשר מייצג את אינטרס הנהלת הארגון לייצר תאימות או הסמכה מול תקן זה, האחראי לבניין הכוח של הצוות, הקצאת הסמכויות והמשאבים, מולו יש לדווח על שלבי התקדמות הביצוע של התכנית ועד להשלמתה.

תוצר נדרש	א'	**תכנית אב** מסמך המתעד את חברי צוות העבודה, אחריות וסמכות, הקצאת המשאבים ולו"ז מתוכנן.

3.2.2 ארגון מסמכי התקינה ותבניות העזר

אסוף וארגן את סט המסמכים והמידע הנדרש לצורך הפקת אומדן להיקף העבודה הנדרשת בארגונך לצורך ביצוע מבדק התאימות.

א. **תקן רב-מגן** – גרסת התקן האחרונה. הרמה הנדרשת בתקן תהיה בהתאם לרמה אשר הוגדרה למידע הביטחוני המפוקח הנדרש לתהליך התאימות.

ב. **כלים ועזרים** – הורד את סט מסמכי טבלאות העזר הזמינים בפורטל ניהול התכנית (שלד תוכנית הגנה ארגונית SSP, טבלת נכסים ארגונית לטובת תיחום, אקסל לחישוב ניקוד, ועוד).

3.2.3 תיחום הפעילות

הארגון אחראי תחילה להגדיר את היקף הנכסים והרשתות הכלולים במסגרת התאימות (ראה בפרטים בפרק הגדרות התיחום). תיחום זה יאומת בהמשך הדרך על ידי הבודק המוסמך. לצורך כך **מוביל מבדק התאימות** יבצע את ההכנות הבאות –

א. הגדר את הזהות התאגידית של הארגון שבו מבוצע מבדק תאימות – האם זהו הארגון והמטה הכללי, האם חברת בת, סניף מרוחק, או יחידה/חטיבה עסקית נפקדת.

ב. הגדרה והקצאת משאבים למבדק ובהם מקום ביצוע המבדק, בעלי תפקיד וזמינותם, לוחות זמנים וכן ציוד, אם נדרש.

ג. הכנת חומרים – מסמכים ותיעוד אשר יסייעו בהכנה וביצוע המבדק ובהם: סכימת הרשת, דיאגרמות זרימת מידע ועיבוד, הנחיות ביטחון ותכנית אבטחת המערכת, מסמכי מדיניות ונהלים ארגוניים. מסמכי אפיון ותחזוקה .

ד. בקש מן היצרנים, ספקי תשתיות, ספקי מיחשוב בענן (בארץ או בחו"ל), ספקי שירותים מנוהלים של הארגון תעודות המעידות על הסמכה של מוצריהם או שירותיהם בהם הארגון עושה שימוש.

ה. אמוד את היקף העבודה הנדרשת לצורך ביצוע מבדק התאימות עד לסיומו, או עד להרכשת הסמכה ככל שנדרשת. לצורך הפקת אומדנים ראשוניים, מומלץ להיעזר באנשי מקצוע בעלי ניסיון קודם בעריכת מבדקי תאימות טכנולוגיים מסוגים אלו.

3.3 ביצוע מבדק תאימות פנימי

מטרת שלב זה היא להגדיר את אופן ביצוע מבדק התאימות. צוות בודקי התאימות יעריך את רמת יישום דרישות התקן בארגון, יאמת את הלימות המענים מול הדרישות על בסיס אסמכתאות וראיות שיאספו. צוות בודקי התאימות יקבע האם המענים עמדו בדרישות, יזהה, יתאר ויתעד פערים כלשהם אשר התגלו במהלך התהליך. הפעילויות המוגדרות בשלב זה אינטרקטיביות במהותן מול הארגון. לצורך השלמת המבדק הפרק כולל את הגדרת התוצרים הנדרשים להשגה בסופו –

3.3.1 מפת משאבי התקשו"ב בארגון

הכן והצג רישום של כלל נכסי הארגון הלוגיים, הפיזיים והעינניים באמצעות רשימה המפרטת את המערכות, התוכנות, ציוד המחשוב, שרתים, מחשבים, התקנים, יישומים, אפליקציות וכל פלטפורמה המכילה מידע ארגוני.

תוצר נדרש	ב'	**מפת נכסים ארגונית** תיעוד רשימת כלל המשאבים התקשוביים של הארגון.

3.3.2 זיהוי ומיפוי נכסי המידע הביטחוניים

מתוך מפת המשאבים התקשוביים, יש לזהות ולסמן את הנכסים העונים על ההגדרה של "נכסים ביטחוניים" על פי ההגדרה בפרק "תיחום מבדק התאימות". נכסים ביטחוניים אלו נדרשים להיכלל בתכולת המבדק.

3.3.3 סיווג נכסים ביטחוניים ע"פ קטגוריות לתיחום

עבור על רשימת כלל המשאבים התקשוביים של הארגון ושייך משאב לנכס ביטחוני בהתאם לקטגוריה המתאימה לו על פי המאפיינים המופיעים בפרק "תיחום מבדק התאימות" בטבלת "קטגוריות לתיחום".

סווג כל משאב לנכס בקטגוריה המתאימה מחמשת הקטגוריות A ועד E –

א. נכסים בקטגוריה **A** – נכסי מחשוב המטפלים ישירות במידע ביטחוני.

ב. נכסים בקטגוריה **B** – נכסי מחשוב במערכות ורכיבי הגנה / הגנה.

ג. נכסים בקטגוריה **C** – נכסים אשר ייעודם אינו לטפל במידע ביטחוני, אך קיים חשש כי ייחשפו אליו.

ד. נכסים בקטגוריה **D** – נכסים מיוחדים אשר אינם נושאים ביכולת שיוריות למידע.

ה. נכסים בקטגוריה **E** – נכסים המופרדים טכנולוגית באופן מובהק מן המידע הביטחוני. נכסים אלו אינם נכללים במבדק התאימות.

3.3.4 הגדרת רמת הבדיקה לנכס הביטחוני

עבור כל הנכסים הביטחוניים אשר סווגו לקטגוריות התיחום A ועד E יש להתאים רמת בדיקה ע"פ טבלת "רמות הבדיקה" בפרק "תיחום מבדק התאימות" – מלאה, חלקית, בסיסית או לא נדרשת.

3.3.5 הכנת מסמך התיחום

יש להכין "מסמך תיחום" הנדרש כמסמך בסיס לטובת ביצוע בדיקת התאימות כפי המתואר בטבלה להלן .

מסמך התיחום מהווה את המלצת הארגון לתיחום המבדק כפי שיוגש לבודק התאימות המוסמך.

תוצר נדרש	ג'	**מסמך התיחום** רשימת הנכסים המטפלים במידע ביטחוני ע"פ הגדרות תקן זה והינם כלולים במבדק, ע"פ הקטגוריה, והגדרת רמת הבדיקה הנדרשת עבורם.

3.3.6 ניתוח פערים

בשלב זה יבוצע ניתוח הפערים (Gap Analysis) – תהליך הכולל בחינה מפורטת של מצב קיום המענים מול הדרישות, בחינה אשר באמצעותה נזהה את היכולות, התהליכים, הכישורים, הטכנולוגיות והאמצעים שאינם אופטימליים או חסרים. ולאחר מכן, יגובשו המלצות לצעדים הנדרשים אשר יצמצמו את הפערים שאותרו למתן מענה כולל טוב יותר לדרישות התקן.

המטרה, בשלב זה, היא לייצר ולהציג עבור בעלי העניין בארגון את תמונת המצב של ההתאמת הארגון מול התקן לטובת קבלת החלטה על אופן צמצום הפערים ושיפור ההתאמה.

א. יש לעבור על דרישות התקן, ולזהות מול כל דרישה את הנכסים אשר הינם רלוונטים לגביה, כלומר הנכס מכיל משטחי תקיפה אשר הדרישה מתייחסת אליהם.

ב. יש להעריך האם המצב המתואר בדרישה מתקיים אל מול הנכס, ובאיזה מידה – מהם האמצעים הקיימים אשר מסכלים את ניצול משטחי התקיפה מפני פגיעה בנכס או במידע הביטחוני הקשור אליו. יש להעריך את מידת ההתאמה על פי הסולם המתואר בפרק התאימות.

ג. היה והדרישה אינה מתקיימת במלואה, יש לתעד את הפער ברשימת הפערים תוך מתן התייחסות לנכס/למערכת ולסעיף הדרישה בתקן.

תוצר נדרש	ד'	**רשימת פערים.** מסמך הכולל את רשימת הפערים אשר התגלו מול הנכנסים הנמצאים בתיחום, הכולל את שם הכנס, מידת ההתאמה, תיאור הפער, והתייחסות מול סעיף הדרישה בתקן.

3.3.7 סגירת הפערים

שלב זה כולל את הקמת תכנית פעולה אופרטיבית לצמצום הפערים, הפעלתה, ועדכון טבלת הפערים (Gap Analysis) כדי להציג את המצב המשופר החדש.

א. **תכנית לצמצום פערים** – יש לאפיין עבור כל פער את דרך הפעולה המיטבית לצמצומו ושיפור ההתאמה. דרך הפעולה תוגדר באופן עקרוני ע"י מוביל אבטחת המידע. אפיון דרכי הפעולה יוגדר לאחר בחינה של מספר אפשרויות למשל:

1) התקנה/שדרוג של אמצעי הגנה
2) שינוי קונפיגורציה של מערכות ותשתיות
3) הצבת נהלים
4) הוצאת הנכס מחוץ לתיחום הביטחוני
5) שיפור הגורם האנושי (יכולת הפעלה, כישורים, מודעות)
6) שינוי בארכיטקטורת או בתהליכים.

7) השארת המצב על כנו.

ב. **הכנת תכנית עבודה** – עבור כל טיפול בפער תוגדר תכנית עבודה המפרטת את אופן יישום הפתרון בצורה מעשית ומפורטת, משלב התכנון ועד לשלב ההצלחה בבדיקות הקבלה (Acceptance Test). התכנית תובל על ידי מוביל הגנת מידע בשילוב עם מומחי תוכן ארגוניים או חיצוניים). התכנית תכלול התייחסות מפורטת עבור על פריט –

1) הנכס/ים עבורם מבוצע הטיפול
2) התייחסות לדרישה בתקן
3) אופן הטיפול המפורט המבוצע
4) אחראים
5) הגדרת זמני טיפול העומדים במסגרת זמן מבדק התאימות או לאחריו.
6) תיאור שלבי ביצוע – אבני דרך, משאבים, תאריכים (התחלה, סיום)
7) אופן השיפור בהתאמה

ג. **ביצוע התוכנית** – הארגון יפעל בכדי לממש את תוכנית העבודה כפי שהוגדרה תוך השלמת יישומה בפרק הזמן שהוגדר.

ד. **מבדק התאמה פנימי** – הארגון יבצע אומדן מחודש מול הפערים/נכסים ויעריך מחדש את ציון ההתאמה על פי המצב החדש שנוצר. מכאן, יהיה אלו תוצאות המבדק אשר ידווחו לבודק המוסמך כמצב הקיים.

ה. **תכנית פעולה להמשך** – ככל שלא יושלמו כלל הפעילויות בתכנית הפעולה עד למועד הסקירה של הבודק המוסמך או מועד ההסמכה, יש לגזור את תכנית ההשלמה (מה שנותר לביצוע) ולשמרה לטובת בחינת התאימות. תכנית זו תוצג ותהיה מעתה – תכנית הפעולה לצמצום פערים, כפי שנותרו.

תוצר נדרש	ה'	**תכנית פעולה לצמצום פערים (POA&M).** מסמך הכולל את הצגת התוכנית המעשית המפורטת לביצוע יישום של אמצעים לטובת תיקון ליקויים או סגירת פערים. ראה לעיל, על פי סעיף "תכנית העבודה".

3.4 ביצוע מבדק תאימות ע"י בודק המוסמך

פרק זה סוקר את שלבי העבודה הנדרשים לביצוע מבדק תאימות ע"י בודק מוסמך. המבוצעת מול הארגון על ידי גורם שהוסמך לבצע מבדק תאימות ע"פ דרישות תקן זה והינו מוסמך, להמליץ לגוף המסמיך על מתן אישור או הסמכה רשמיים שהארגון מקיים את דרישות התקן.

מבדק התאימות מצריך הובלה של מומחה תוכן ייעודי לתחום זה, אדם בעל ידע מקצועי אשר הוסמך לתפקיד זה על ידי הגוף הביטחוני – יקרא להלן "הבודק המוסמך". גורם זה יהיה האחראי להוביל תהליך בדיקת התאימות והבדיקה של ההתאמה של הארגון מול דרישות התקן ולקבוע את ציון ההתאמה.

להלן שלבי העבודה –

3.4.1 בחירה והתקשרות עם בודק מוסמך

יש לבחור בודק תאימות מוסמך מתוך רשימת הבודקים המוסמכים. יש לוודא כי לא קיימים ניגודי עניינים וניגודי אינטרסים בין הארגון, בין חברי צוות בודקי התאימות, לבין הבודק המוסמך. יש לסגור את ההתקשרות המסחרית מול הבודק, לרבות על תכולת המבדק.

3.4.2 הכנת מסגרת העבודה

יש להגדיר את מסגרת העבודה ותאריך היעד לטובת ביצוע תהליך הבדיקה. יש להקצות את המשאבים הנדרשים ואת זמינות צוות בודקי התאימות הארגוני ובעלי תפקיד רלוונטיים.

3.4.3 ישיבת התנעה

הבודק המוסמך יכנס פגישת התנעה למבדק. במפגש יוצגו בעלי התפקיד ותחומי אחריות, התהליך המתוכנן אותו הוא יוביל וכן יבוצע תיאום ציפיות. במפגש זה צוות העבודה יתאם את הלוגיסטיקה הדרושה לצורך עבודתו המשותפת; מיקומים, דרכי התקשרות, חומר ומסמכים מקדימים הנדרשים להעברה, אילוצים ועוד.

3.4.4 הצגת תיק המסמכים

הארגון יציג וימסור לבודק המוסמך מידע ומסמכים רלוונטיים לבדיקה ככל שיידרש. סט המסמכים יכלול על פי רוב את תיעוד הנושאים: תשתיות הארגון, רשימות נכסים, תכניות ההגנה, רשימות פערים, תכנית לצמצום פערים, מסמכי מדיניות ונהלים הקשורים לאבטחת מידע והגנה.

להלן רשימת המסמכים והראיות אשר הארגון נדרש להיות מוכן להצגה ומסירה לבודק.

הרשימה אינה ממויינת על פי סדר מסויים. להלן –

#	כותרת המסמך	מקור הדרישה	תיאור
.1	דיאגרמת תשתיות רשתות ותקשורת	כללית	מיפוי ותרשימים הכוללים טופולוגיה פיזית, גיאוגרפית, חיבוריות רשתית, ניתובים, קונפיגורציה לוגית (סגמנטציה, ערוצי תקשורת לוגיים, IP). חיבורים בין רשתות; מעבדות, טלפוניה, אלחוט, ענן, שותפים, אינטרנט.
.2	דיאגרמת זרימת הנתונים	כללית	תרשימי זרימת המידע הביטחוני המציגים היכן מאוחסן, מעובד ומועבר. מאגרי מידע, קבצים ומסדי נתונים. תהליכים אוטומטיים או כאלה המופעלים על ידי משתמשים.
.3	בעלי תפקיד ואחריות	כללית	מיפוי בעלי תפקיד האחראים לביצוע תהליכי הגנה, בקרה, מימוש הדרישות, ומנהלי מערכת בהרשאות חזקות.
.4	חוזי אבטחת מידע נותני שירותים	כללית	תיעוד שירותי אבטחת המידע המסופקים על ידי חברות צד-שלישי, המחוייבים חוזית להגן על מידע ביטחוני, וכיצד.
.5	מדיניות ונהלים ארגוניים	כללית	מיפוי נהלים ארגוניים התומכים באבטחת

			מידע והגנה בסייבר.
6.	תהליכים בהתחייבות	כללית	מסמך המתאר היבטים או תהליכי אבטחת מידע אשר מקורם בתקנות רגולציה, חוק או מקורות אחרים מולם התחייב הארגון.
7.	טיפול במידע ביטחוני	דרישה בתקן	הצגת שיטות העבודה לגבי אופן הזיהוי, הסימון, והטיפול השגור במידע הביטחוני.
8.	תכנית הגנה (SSP)	דרישה בתקן	תכנית אבטחת המערכות המכסה את תיחום המידע הביטחוני, אחת או יותר.
9.	תכנית פעולה לצמצום פערים (POA&M)	דרישה בתקן	מסמך הכולל את הצגת התוכנית המעשית המפורטת לביצוע יישום של אמצעים לטובת תיקון ליקויים או סגירת פערים.
10.	רשימת נכסים	דרישה בתקן	רשימת נכסי ומשאבי המחשוב והרשת הכוללת מערכות, יישומים, שירותים, תהליכים, חדרי שרתים, אחסון וגיבוי, יתירות והתאוששות, מכונות ייצור ובדיקה, מערכות תפעוליות תומכות (אקלים, חשמל, בטיחות, הגנה, בניין), התקנים (עמדות עבודה, טלפוניה, מדפסות וסורקים, התקני USB, מולטימדיה וכו'). רשימת נכסים חיוניים וקריטיים
11.	ציון התאמה	דרישה בתקן	גיליון נתונים של מפרט ציוני ההתאמות מול הדרישות עם הציון הכללי המחושב.
12.	דוחות מבדקי פגיעות וחוסן	דרישה בתקן	דוחות של מבדקי פגיעויות ומבדקי חוסן שבוצעו, הנמצאים בתיחום המידע הביטחוני.
13.	בקרת שינויים	דרישה בתקן	מסמכים המאשרים ביצוע של שינויי תצורה במערכות, אמצעי הגנה, הרשאות, ותהליכים הנוגעים למידע ביטחוני.
14.	מודעות בהגנה בסייבר	דרישה בתקן	הצגת תיעוד הפעילויות והמערכות המשמשות בשגרה להגברת מודעות ואימון עובדים מורשי גישה בנושא הגנה בסייבר.
15.	נוהל תגובה לאירועים (IR)	דרישה בתקן	הצגת תו"ל לניהול אירועים (סייבר או תקלות) ומצבי חירום בארגון – מצבי כוננות, אופני הפעלה, תהליכים, וכו'.
16.	נוהל לחקירת אירוע סייבר	דרישה בתקן	הצגת נוהל לעריכת חקירה לזיהוי סיבת השורש (Root Cause Analysis) לתקלה או מתקפה – חקירת ראיות דיגיטליות (פורנזיקה).
17.	תצורת בסיס של מערכות	דרישה בתקן	מפרט תצורת הבסיס (קונפיגורציית הפעלה) של כל המערכות והפלטפורמות הכרוכות בתיחום המידע הביטחוני. מערכות הפעלה וגרסאות מוצרים.
18.	נוהל טיוב הרשאות	דרישה בתקן	נוהל עבודה לטיוב ביטחוני של הרשאות במערכות השונות – סריקת חשבונות חזקים, צמצום, מעבר תפקידים, וכו'.
19.	ניהול סיכונים	דרישה בתקן	תכנית תקפה ועדכנית של הערכת הסיכונים.
20.	ערוצי התרעות ומודיעין	דרישה בתקן	הצגת החוזים והתוצרים המתקבלים משירותי

	סייבר		מומחה המספקים התרעות ומודיעין סייבר.
21.	מדיניות השמירה על מידע ביטחוני מפוקח	דרישה בתקן	מסמך המתאר את המדיניות התקפה בארגון לרבות פירוט אופני יישום המדיניות בשטח לצורך ההגנה על מידע ביטחוני במערכות טכנולוגיות, בתהליכים ובקרב העובדים.
22.	הסכמי סודיות (NDA)	דרישה בתקן	הסכמי הסודיות הנכרתים מול העובדים ומול נותני שירותים חיצוניים לצורך שמירה על מידע ביטחוני.
23.	לוגים ואיסוף מרכזי	דרישה בתקן	תיעוד תהליכי שמירת התיעוד/לוגים של אירועי אבטחת מידע במערכות והאיסוף המרכזי.
24.	נוהל בדיקות התאמה / הכשר ביטחוני לעובדים	דרישה בתקן	תיעוד הנוהל להפעלת בדיקות התאמה ו/או קבלת הכשר ביטחוני לעובדים טרם חשיפתם למידע ביטחוני.
25.	יומן ביקורי אורחים	דרישה בתקן	הצגת יומן ביקורים של אורחים בארגון וזהות המלווה.
26.	עבודה מהבית	דרישה בתקן	תצורת ההגנה של החיבור המרוחק הניתן לעובדים מרוחקים / מן הבית.
27.	שגרת גיבויים	דרישה בתקן	הצגת מתווה הגיבויים המבוצעים, שגרות, אחסנה, ושמירה על מידע ביטחוני. הצגת תרגילי שיחזור מידע.
28.	נהלי מחזור החיים והטיפול בציוד מחשבים	דרישה בתקן	הצגת מחזור החיים (Lifecycle) ונהלי הטיפול בציוד מחשבים ו- IT משלב הרכש, התקנה, שדרוג, תחזוקה, עד סילוק.
29.	רשימת פערים	דרישה בתקן	רשימת הפערים אשר זוהו בתהליך ניתוח הפערים (Gap Analysis) מול דרישות התקן.
30.	נהלי פיתוח קוד מאובטח	דרישה בתקן	הצגת השיטות, התהליכים והאמצעים השגורים בארגון לפיתוח מאובטח וסריקת קוד בכל הקשור לפיתוח תוכנה פנימי. (ככל שרלוונטי לארגון)
31.	מיפוי מערכות לטיפול בחומרים מסוכנים	כללית	מיפוי תשתיות, חיבורים והתקנים המשמשים מערכות המשלבות חומרים מסוכנים ורעלים.

3.4.5 סמכויות הבודק המוסמך

הבודק המוסמך אשר הארגון ישכור את שירותיו מחוייב להיות הוגן ונאמן מול שני גורמים; הראשון הוא מול הארגון עצמו לו הוא מחוייב בעריכת מבדק מקצועי, יעיל, תחת מסגרת העבודה שהוגדרה, והמשקף נכונה את מצב ההגנה הקיים על מידע ביטחוני מול דרישות התקן. הגורם השני הוא הגורם המזמין את המבדק שמבקש לשקף מולו את המצב ההגנה על מידע ביטחוני באופן המקצועי והנכון ביותר. הבודק המוסמך עבר הכשרה מקצועית ייעודית לעריכת מבדקי תאימות מסוג זה, נבחן, והוסמך, כך שהינו מכיר את מחויבויותיו אלו ויודע להוביל את שני הצדדים נכונה.

לצורך יצירת התיאום והבנות הנדרשות לעבודה משותפת בין הארגון לבין הבודק המוסמך, תחת האחריות המוגדרת בתפקידו, ניתנות לבודק המוסמך הסמכויות להלן –

א. לבקש את הצגה בשטח לצורך התרשמות מקרוב של אמצעים, שגרות, יומנים, מסמכים בארגון.

ב. לבקש לערוך ראיון או תשאול של בעלי תפקיד או עובדים מטעם הארגון.

ג. לקבוע ולהכריע בכל הקשור למסמכים והתיעוד הנדרש בהצגה, ורמת הפירוט/הרחבה הנדרשת.

ד. לקבוע האם ראיה שסופקה על ידי הארגון מהווה אסמכתא נאותה הקבילה לצורך הערכת התאימות.

ה. להעריך על דעתו את מידת ההתאמה של המענה הקיים אל מול הדרישה ולקבוע את ציון ההתאמה.

ו. לתת המלצה לבקרה מפצה אחרת, ולתעד המלצתו בדוח.

ז. לקבוע כי מסגרת העבודה שהוקצתה למבדק אינה מספיקה לצורך השלמת המבדק על פי הדרישות.

ח. לחשב ולקבוע את ציון ההתאמה הכללית של המבדק.

ט. לספק רמת תאימות כללית כתובה אשר תירשם כתוספת בדוח המבדק.

י. לספק המלצות שונות לארגון אשר ירשמו כתוספות בדוח המבדק.

יא. להמליץ על מתן החרגה זמנית ולאפשר לארגון זמן לתיקון פערים.

לבודק המוסמך <u>לא</u> תוקנה הסמכות –

יב. לקבל גישה על שמו למערכות הארגון.

יג. לגשת ולהפעיל מערכות באופן עצמאי – הקלדת פקודות, הפעלת סקריפטים, הפעלת יישומים. (בכל דרישה להוכחת יכולת על גבי המערכות, תבוצע ההדגמה על ידי עובד הארגון ובאחריותו).

יד. להכנסת חומר מכל סוג לרשתות הארגון.

טו. לאסוף ממצאים ועדויות ולהכניסם לתאימות ללא ידיעת הארגון.

טז. לפנות ישירות לנותני השירותים של הארגון ללא תיווך הארגון.

כל הממצאים והראיות שיאספו על ידי הבודק יהיו בתיווך הארגון ובידיעתו.

בכל מקרה של מחלוקת בלתי פתירה מול הבודק המוסמך, יש לפנות למזמין או לגוף הביטחוני הרגולטור על מנת לקבל הנחיות לפתרון הסוגייה.

3.4.6 ביצוע תהליך מבדק התאימות

הבודק המוסמך יוביל ויבצע את התהליך למבדק התאימות של מערכות הארגון מול דרישות התקן בתיחום שהוצע. התהליך יבוצע בשיתוף ובהפעלת צוות בודקי התאימות שהוקם.

אופן הביצוע המפורט של תהליך מבדק התאימות מול דרישות התקן מתואר בפרטים בפרק התאימות בתקן זה.

אופן הביצוע המפורט של תהליך הניקוד, מתואר בפרטים בפרק ניקוד וציון התאמה כללי.

תהליך כללי של מבדק התאימות הביטחונית יכלול על פי רוב את השלבים להלן –

א. **בחינת סט המסמכים** – סקירה וניתוח של המסמכים שהוגשו.

ב. **בדיקת המענה** – ביצוע בדיקה מפורטת מול כל דרישה בתקן – בחינה במסמכים, תשאול, בדיקה בשטח.

ג. **בדיקת הסמכות ספקי שירותים** – אימות ושילוב הסמכות (אם קיימות) של ספקי השירותים של הארגון (שירותי ענן לדוגמא). כיצד בקרות ההגנה של הספק שוות לאלו הנדרשות בתקן.

ד. **הצגת ראיות** – בקשה להצגה/קבלת ראיות תומכות לאופן מימוש המענה ו/או אופן העמידה בדרישה.

ה. **הערכת התאמה** – ביצוע שקלול אופן יישום המענה, היקפו, עומקו, חוסנו, אל מול הדרישה, והפקת ציון ההתאמה פר דרישה. התהליך יהיה אינטרקטיבי – ציונים שגובשו יוצגו לארגון ותינתן לו הזדמנות להרחיב את הצגת הראיות.

ו. **דיון טיוטת הדוח והממצאים** – עריכת דיון מסכם על טיוטת הדוח מול צוות העבודה. קבלת התייחסויות. מתן מענה להתייחסויות שהועברו. במידת הצורך תורחב מסגרת העבודה.

ז. **הפקת דוח מסכם** – הפקת דוח תאימות סופי הכולל את ציון ההתאמה הכללי, גיליון פירוט ציוני התאמה מול על דרישה, הערות לגבי אופן חישוב הציון והפערים, המלצות שונות, וחוות דעת כללית אודות ההתאמה ותהליך המבדק.

ח. **המלצה להסמכה** – ככל שהציון הכללי עומד בתנאים לקבלת הסמכה, יספק הבודק המוסמך את טופס הבקשה חתום לצורך הגשה לגוף הביטחוני.

3.4.7 הצהרת הארגון

הארגון יספק הצהרה כי הוא דוח הבודק המוסמך מסכם נכונה את מצב התאימות של הארגון מול התקן, וכי הארגון עומד בציון ההתאמה כפי שמופיע בדוח. על ההצהרה יחתמו מוביל מבדק התאימות, מוביל אבטחת המידע, ומנהל כללי המוסמך חתימה. מסמך ההצהרה יתווסף לתיק המסמכים להגשה.

3.5 דיווח תוצאות המבדק

פרק זה סוקר את עקרונות ההגשה של תוצאות תהליך מבדק התאימות הסופי לבעלי העניין שלו, אם המזמין או הגוף הביטחוני, אם לצורך מענה למכרז או אם לצורך קבלת הסמכה.

3.5.1 אריזת תיק המסמכים

בשלב זה הארגון יארוז את כלל המסמכים אשר נעשה בהם שימוש בתהליך התאימות; מסמכים אשר הוכנו קודם לתהליך התאימות, מסמכים אשר נוצרו במהלך תהליך התאימות, בעלי תפקיד, נכסים, התיחום הביטחוני, פערים, תכניות עבודה, פרוטוקולי דיונים, מדיניות ונהלים, מבדקים, ראיונות, מסמכי הראיות, הערכות, לרבות דוח התאימות הכללי המסכם – וכל אלו יארזו דיגיטלית לכדי תיק מסמכים אחוד.

תיק המסמכים יכיל בנוסף את פרטי הבודק המוסמך ותיעוד רישיונו.

תיק המסמכים יכיל בנוסף את "תעודת הזהות" של הארגון, כתובת, מנהלי החברה, פרטי צוות התאימות, ודרכי התקשרות.

תיק המסמכים ותכולתו יהיו בבעלות הארגון. באחריות הארגון יהיה לשמור ולגבות לאורך זמן (לפחות 3 שנים) את תיק המסמכים ולהגן עליו מפני חשיפה או אובדן.

3.5.2 הגשה / משלוח

תיק המסמכים נדרש להגשה לגורם המזמין או לגוף ההתעדה, והכל בהתאם להנחיות ההגשה המפורטות במסמכי המכרז של המזמין, או אם לצורך הסמכה, כפי שמופיעות בפורטל תכנית ההסמכה.

הגשת המסמכים תבוצע לא יאוחר מ- 30 יום לאחר סיום וחתימת הדוח המסכם.

הנמען, המזמין, יאשר את קבלת תיק המסמכים והדוח המסכם באמצעות מכתב רשמי לארגון.

3.6 הסמכה

בקשה לקבלת הסמכה מגוף ההתעדה אינה קשורה לתהליך המבוצע מול המזמין. יש למצות ובעדיפות את כל התהליך הנדרש מול המזמין (אם קיים). ההסמכה הינה תהליך המבוצע בנפרד מול גוף ההתעדה לצורך קבלת אישור רשמי על הסמכה לתקינה.

לצורך הגשת בקשה להסמכה, יגיש הארגון את תיק המסמכים (המתואר בסעיף קודם) לגוף ההתעדה על פי הפרטים וההנחיות המופיעות בפורטל תוכנית ההסמכה.

הגשת המסמכים תבוצע לא יאוחר מ- 45 יום לאחר סיום וחתימת הדוח המסכם.

3.6.1 בדיקה להסמכה

גוף ההתעדה יבצע בדיקה למידת התאמת הארגון לתנאי ההסמכה אשר בתוקף. גוף ההתעדה יבצע את הבדיקה בכפוף לסיכום התאימות אשר בוצעה על ידי הבודק המוסמך. גוף ההתעדה יוכל לעיין בתיק המסמכים בכדי לבחון נושאים כאלו ואחרים אשר סבור הוא כי הם נדרשים על מנת לגבש את החלטתו. גוף ההתעדה יהיה רשאי לפנות לארגון ולבקש הבהרות כאלו ואחרות על הנושאים המופיעים בתיק המסמכים.

ככל שמצא גוף ההתעדה כי מתקיימים התנאים להסמכה, לרבות ציון ההתאמה הכללי עומד בסף ההסמכה, יאשר גוף ההתעדה לארגון כי הוא עומד בתנאים.

גוף ההתעדה ינפיק וישלח את תעודת ההסמכה לארגון.

התעודה תישא את תוקף ההתחלה של מועד חתימת הדוח על ידי הבודק המוסמך. התעודה תוקפה יהיה ל- 3 שנים. לאחר מכן נדרש יהיה לחדש את ההסמכה.

גוף ההתעדה ירשום את הארגון במאגר החברות בעלות הסמכה ביטחונית. המאגר יהיה נגיש לגופים ביטחוניים.

גוף ההתעדה ישמור עותק סט המסמכים עד לסיום תוקף ההסמכה.

3.6.2 דחיית הסמכה

ככל שיהיה גוף ההתעדה סבור כי התנאים למתן הסמכה לארגון אינם מתקיימים, ינפיק גוף ההתעדה מענה רשמי לארגון הכולל את הפערים והסיבות לאי מתן ההסמכה. במצב זה, ימליץ גוף ההתעדה לפנות לבודק מוסמך על מנת לעבד את התשובה ולבחון את הפעילויות הנדרשות לצורך סגירת הפערים הנדרשים לקבלת ההסמכה.

3.6.3 שמירת רצף הכשירות

הקמת מערכת ההגנה וההגנה על נכסי הארגון, לרבות תהליך מבדק התאימות, והדיווח דורשים השקעת מאמץ ומשאבים רבים. האינטרס של כל הצדדים הוא כי רמת ההגנה כל מידע ביטחוני אשר הושגה בעמל רב תישמר ברציפות לאורך כל תקופת מסגרת העבודה מול המזמין, לרבות ישמור הארגון את רמת ההגנה לטובתו הוא, וגם לטובת המכרזים/העבודות העתידיות לבוא, כך שלא תתבסס אחיזה של תוקף בין התקופות. לצורך כך נדרש להקדיש לשמירת רצף הכשירות משאבים רציפים בכל שנה. הגנה בסייבר אינו מאמץ חד-פעמי.

לצורך שמירת רצף הכשירות יש לבצע אחת לשנה –

א. טיוב רשימת הנכסים הארגוניים.

ב. טיוב תיחום הנכסים הביטחוניים.

ג. ביצוע מבדקים לגילוי פערים ופגיעויות בחוסן בהתאם לתכנית.

ד. ביצוע פעולות מתקנות מול ליקויים ותקלות שמתגלות.

ה. טיוב מצב התאימות מול דרישות התקינה על ידי תהליך של תאימות עצמית. עדכון הדוח.

ו. תיעוד הפעילויות שבוצעו לשמירת הכשירות.

3.6.4 חידוש ההסמכה

תעודת ההסמכה ניתנת לתוקף של 3 שנים מיום חתימת דוח התאימות על ידי הבודק המוסמך. לאחר תקופה זו פג תוקפה.

ההסמכה ניתנת לחידוש על ידי ביצוע מבדק חדש והגשה של תיק המסמכים בגינו, זאת באותו האופן ע"פ המפורט בפרקים הקודמים.

פעילויות שמירת הכשירות השנתית הינן מהותיות להצלחת חידוש ההסמכה.

4 תיחום

4.1 הקדמה

פרק זה מספק את המידע הנדרש לצורך הכנת **מפרט התיחום** של הנכסים הארגוניים – המפרט הנדרש לצורך ביצוע מבדק התאימות. הפרק מכיל את ההגדרות הנדרשות לצורך הכנת מפרט זה. מפרט התיחום יכיל את הרשימה של הנכסים הכלולים במבדק, ואת הנכסים שאינם כלולים במבדק. מול אלו, המפרט מגדיר את היקף בדיקת התאמה הנדרשת עבור כל סוג של נכס.

פרק זה מספק את ההרחבה הנדרשת עבור המשימה "תיחום נכנסים" אשר מופיעה בפרק קודם כיצד להשתמש בתקן. הארגון נדרש לספק את מפרט התיחום כחלק מתהליך מבדק תאימות.

4.2 קטגוריות לתיחום נכסים

להלן הגדרה של 5 קטגוריות ביטחוניות המיועדות להגדרת הנכסים הארגוניים הביטחוניים. כל נכס ארגוני ישתייך לאחת מן הקטגוריות להלן –

טבלת קטגוריות לתיחום נכסים		
קטגוריה	**מאפיינים**	**דוגמאות**
נכסים אשר נכנסים לתיחום מבדק התאימות		
A נכסי מיחשוב ביטחוני	נכסי מיחשוב המבצעים באופן ישיר פעולות של אחסון, ו/או עיבוד, ו/או העברה של מידע ביטחוני.	▪ עמדות עבודה למשתמשים במידע ביטחוני ▪ מדפסות ▪ שרת קבצים ▪ סגמנט רשת
B נכסי מערכות הגנה	נכסי מיחשוב ברחבי הארגון המספקים פונקציות או יכולת הגנה על נכסי הארגון, ללא רלוונטיות לאופן חשיפתם למידע ביטחוני אם כן או לא.	▪ אנשים – יועצים וספקים להגנה בסייבר, אנשי תחזוקת מערכות הגנה, מנהלי רשת והרשאות. ▪ מע' הגנה – SIEM, VPN, חומת אש. ▪ מתקנים – מרכז בקרה ביטחוני (SOC), Data Center,
C נכסי מיחשוב בסיכון חשיפה	נכסי מיחשוב בעלי היכולת (הפוטנציאלית) לאחסן, ו/או לעבד, ו/או להעביר מידע ביטחוני, אך ייעודן הוגדר שונה, וכך הן מופרדות ממידע ביטחוני באמצעות הגבלות והרשאות של מערכות הגנה, ומגבלות אלו מתועדות במדיניות ובנהלים.	▪ עמדות עבודה למשתמשים שאינם מטפלים במידע ביטחוני ▪ סגמנט רשת ללא מידע ביטחוני
D	נכסים אשר יתכן ויאחסנו, ו/או יעבדו, ו/או	▪ טלוויזיה חכמה, גלאי חירום,

נכסי מיחשוב מיוחדים	יעבירו מידע ביטחוני, אך תצורתם הטכנולוגית מוגבלת ואינה מיועדת לאגירת נתונים, כך שאינם יוצרים חשיפה גבוהה, והם אחד מן הסוגים – א. התקני IoT (סנסורים חכמים, בקרים להפעלת תכונות פיזיות במרחב) ב. מערכות תפעוליות OT (ניהול רצפת ייצור ותעשייה, מעי' בניין) ג. מכשירי מעבדה, קו ייצור, וכלי עזר מיוחדים לבדיקות וסימולציות. ד. ציוד/מכשיר מיוחד שסופק/הושכר מאת המזמין, שאינו תוכנה.	תאורה חכמה ▪ בקרים PLC, מעי' מכונות SCADA/ICS, CNC ▪ צב"ד
נכסים אשר <u>אינם</u> נכנסים לתיחום מבדק התאימות		
E נכסים אחרים (מחוץ לתיחום)	נכסי מיחשוב אשר אינם יכולים לאחסן, לעבד או להעביר מידע ביטחוני, או, נכסים שהם מופרדים פיזית מסביבות/רשתות/התקנים המטפלים במידע ביטחוני.	▪ איזור המופרד בשער, שומר, או דלת, עם כרטיס כניסה. ▪ רשת מרוחקת בסניף ארגוני. ▪ מקרן

נכסים מן הקטגוריה האחרונה (E) אינם נדרשים להיכלל במסגרת התיחום עבור תהליכי מבדק התאימות.

4.3 הגדרת רמת הבדיקה

להלן הגדרה של אופני הבדיקה הנדרשת לביצוע במבדק התאימות, בהתאם לסוג קטגוריית הנכס כפי שהוגדר ע"פ המאפיינים בסעיף הקודם, להלן –

טבלת רמות הבדיקה		
רמת הבדיקה	**עבור קטגוריה**	**אופן הבדיקה**
מלאה	**B ,A**	בדיקה תבוצע באופן מלא מול כל בקרות התקן הרלוונטיות.
חלקית	**C**	במידה והנכס מוכל בתוכנית ההגנה הכללית (ע"פ דרישה 12.4) ואופן ההגנה עבורו מתועד ונאות, אזי הנכס לא נדרש בהערכת תאימות מול דרישות התקן. במידה ואופן ההגנה על הנכס כפי שמתואר בתכנית אינו שלם בעיניי הבודק, יוגדר הפער, והוא בלבד יעמוד להערכת תאימות מול דרישות התקן.
בסיסית	**D**	יש לבצע בדיקה ותאימות ע"פ המופיע בתכנית ההגנה הכללית (ע"פ דרישה 12.4).

לא נדרשת	**E**	לא נדרשת בדיקה.

4.4 התוצר הנדרש

להלן הגדרות התוצר הנדרש ל"מפרט התיחום" –

א. לצורך הכנת תוצר מפרט התיחום, נדרש להכין מראש את רשימת הנכסים הארגוניים הכוללת. הרשימה תהווה את הבסיס לשלב זה.

ב. תוצר שלב הגדרת התיחום הוא מסמך עבודה. המסמך יכיל את טבלת הנכסים הארגוניים מכל הסוגים בתוספת הנתונים הבאים –

- כל נכס יהיה משוייך לקטגוריה אחת, בין A ל- E.
- כל נכס יהיה משוייך לרמת בדיקה אחת, בין מלאה ל-לא נדרשת.

ג. להלן דוגמא טבלאית להמחשת התוצר הנדרש –

מפרט התיחום – חברת ABC – גרסה 1, 10 אוגוסט 2022

#	סוג הנכס / שם המערכת	מיקום	נגישות למידע ביטחוני והפרדות	פירוט מטרת המערכת	קטגורית התיחום	רמת הבדיקה	פירוט תכולת הבדיקה	שם אחראי המערכת
1.	SIEM	ספק MSSP שירות חיצוני בחיבור מרוחק. .	מופרד לוגית וללא מידע ביטחוני	איסוף לוגים ממערכות ומתן התרעות במרכז הניטור SOC.	B	מלאה	מול כל הבקרות בתקן	ישראל ישראלי

5 אופן ביצוע מבדק התאימות

5.1 מטרה

מטרת תהליך מבדק התאימות היא לוודא ולאמת כי הארגון מימש ועמד בדרישות המפורטות בתקינה כראוי. את תהליך התאימות יוביל בודק מיומן, אם מומחה תוכן מטעם הארגון, או אם בודק מוסמך לצורך קבלת הסמכה. במסגרת התהליך נדרש הבודק לוודא את עמידתו של הארגון בבקרות התקן הרלוונטיות, וזאת בהתאם למסגרת התיחום שנקבעה.

היות והארגון יכול לעמוד בדרישות התקינה בדרכים שונות (למשל באמצעות הצבת נהלים, הגדרות תצורת מחשבים, תצורת רשתות, אימון בעלי תפקיד, ועוד), הבודק המוסמך יפעל בדרכים ובטכניקות מגוונות, כולל כל אחת משלוש שיטות התאימות המתוארות בהמשך, לטובת קביעת אומדן ההתאמה מול הדרישה.

פרק זה מכיל את השיטות והאופנים הנדרשים לביצוע ע"י בודק תקינה לצורך תכלול ושיקלול כלל הנתונים לכדי הפקת האומדן האחוד.

5.2 שיטות

להלן שיטות, טכניקות, לאיסוף, ניהול וסקירת עדויות, בכדי לקבוע האם יעדי התאימות מתקיימים –

א. **תיעוד ממצאים מהשטח** – ביצוע סיור מדגמי לאיסוף ותיעוד ממצאים נראים מן השטח – אמצעי נעילה, דלתות/שערים, סנסורים, צמתי תקשורת, התקני קצה, ועוד.

ב. **ראיונות/תשאולים** – ביצוע ראיונות, תשאולים ודיונים מול עובדים וצוותי עבודה, ברמות ארגוניות שונות, בכדי לגבש מסקנה כיצד מיושמים המענים, האם המשאבים נאותים, האם התהליכים ממומשים, האם קיימת הדרכה למשתמשים, והאם קיים תכנון ותחזוקת פרקטיקות המענה. הראיונות משקפים את מה שהעובדים מאמינים שמתקיים בארגון. המפגשים יבוצעו בהסכמה הדדית ובשיתוף פעולה.

ג. **סקירה** – תהליך לסקירה, התבוננות, לימוד או ניתוח של אובייקטים שונים המשקפים את כוונת הארגון לבצע את הבקרה או המעידים כי הינה כבר פועלת; כגון סקירת מסמכים, מנגנונים או פעילויות. מסמכים נדרשים להיות בתצורתם הסופית (טיוטות לא מאושרות אינן קבילות כראיות). מסמכים יכללו; מסמכי מדיניות, תהליכים ונהלים, חומרי הדרכה, תוכניות ומסמכי תכנון, דיאגרמות ברמת מערכת, רמת הרשת או רמת זרימת הנתונים.

ד. **בחינה/הדגמה** – תהליך יזום לביצוע בחינה פיזית של אמצעים, צפייה, הצגת יכולת, בקשה להדגמה, ובקשה כי הארגון יציג כיצד הוא מבצע את הנדרש בבקרה הלכה למעשה בשטח, כך שהבודק יוכל להרשם ממקור ראשון. הבחינה ממחישה ומתארת את הביצוע בפועל של הבקרה – מה נעשה, באיזה היקף, האם בצורה נאותה, ומה לא נעשה.

ה. **מבדקים** – תהליך בו אופן פעולת המערכת נבדקת באופן ייזום תחת סביבת מבחן מוגדרת מראש (Test Plan) – התנאים התפעוליים, התרחיש, התוצאות המצופות, מבחן המעבר – לטובת בדיקה האם המערכת עונה על הדרישה. הפעלת מבדקים תהיה תמיד על ידי עובד הארגון או מפעיל המערכת המורשה בהתאם להגדרות הבדיקה של הבודק. הארגון יהיה אחראי על עריכת הבדיקות ומניעת גרימת נזקים בעקבות הפעלתם. הבודק המוסמך לא יבצע גישה למערכות ולא יבצע כל סוג של בדיקות בעצמו.

5.3 תבחינים להערכת מידת ההתאמה של המענה מול הדרישה

להלן רשימה של תבחיני עזר על פי הם ניתן לאמוד את מידת ההתאמה של המענה אל מול הדרישה, להלן –

א. **בדיקת <u>עצם הקיום</u>/אי הקיום של המענה** – בחינה עקרונית הבודקת האם המענה על מרכיביו העיקריים מספק מענה הרלוונטי לדרישה.

ב. **בדיקת <u>היקף</u> הכיסוי של המענה** – בחינה כמותית הבודקת האם היקף המענה מכסה את מלוא מרחב יחידות המערכת, ותתי המערכות באיזור הכיסוי/התיחום הנדרש. לדוגמא, האם המענה מטפל בכל המשתמשים במערכת, בכל עמדות העבודה, בכל סוגי מערכות ההפעלה, או רק בחלקם.

ג. **בדיקת <u>עומק</u> הכיסוי של המענה** – בחינת מרכיבי המענה לגעת ולטפל בשכבות השונות של המערכות עם היכולת לבצע טיפול גם בשכבות עמוקות. לדוגמא, סינון תכנים המבוצע מרמת התוכן וסכמת הנותונים, ועד לעומק רמת תשדורות ה- IP.

ד. **בדיקת יכולת המענה לפעול <u>ברציפות</u> ולאורך זמן** – בחינת מנגנוני ההפעלה של המענה ויכולתך לפעול באופן רציף, יתיר, עם זמינות מלאה של התפוקה הביטחונית ולאורך זמן ללא תקלות והשבתות.

ה. **בדיקת יכולת המענה <u>לגלות ולזהות</u> אירועים ופערים** – בחינת יכולת המענה לגלות ולזהות את האירועים והפערים הביטחוניים המצופים ממנו ולהפיק במצב זה התרעה בעלת ערך.

ו. **בדיקת יכולת המענה <u>להתמודדות</u> והתגוננות** – בחינת יכולת המענה לפעול בצורה אפקטיבית ואוטומטית כנגד הפער שזוהה תוך מניעת דרדור המצב.

ז. **בדיקת <u>חוסן</u> המענה** – בדיקה של רמת החוסן וקשיחות המענה לעמוד בפני תקיפה ייעודית אשר מטרתה לעקפו, להשביתו או לפגום בתכונותיו.

ח. **בדיקת <u>עדכניות</u> המענה** – בחינת המענה להכיל את אופני הפעולה העדכנים ביותר אשר עומדים עבורו. לדוגמא, האם הותקנו והופעלו עליו הגרסאות תוכנה/חומרה, התכונות האחרונות אשר העמיד אותן היצרן.

ט. **בדיקת <u>מורכבות</u> המענה** – בחינת סיבוכיות המענה והסיכונים להתממשות המקרים בהם השימוש בו יהיה לא נכון עקב מורכבותו. למשל, עקב מורכבות התקנה או הקונפיגורציה, מורכבות ההפעלה למשתמשים, מורכבות הנהלים לשימוש, מורכבות תוצרי המענה.

י. **בדיקת <u>שילוביות</u> המענה בהגנה** – בדיקה לאומדן תרומתו של המענה כרכיב המשולב במערך הגנה רחב.

5.4 אותנטיות המימצאים

הבודק יקבל מסמכים ועדויות אוטנטיות בלבד.

כל המימצאים אשר מסופקים לבודק נדרשים להיות מקוריים, מאומתים, מבוססים, מזוהים (מי חיבר, ועל ידי מי נמסר), חתומים, נאותים, ובהירים.

בסמכות הבודק לפסול בדיקת מסמכים אשר אינם עומדים בהגדרות אלו.

5.5 סיכום מימצאים כרמת התאמה

סיכום מבדק התאימות מול כל דרישה בתקן מביאה לאחד מן ארבעת הממצאים האפשריים – רמת התאמה. להלן הגדרתם בטבלה –

רמת ההתאמה	מאפיינים
התאמה מלאה **MET**	הארגון עומד בהצלחה בדרישה. הארגון סיפק הצהרות, אסמכתאות, מסמכים, ועבר את המבדקים בהצלחה, כך שהעדויות מצביעות על כי המענים הקיימים תואמים את הדרישה בצורה מלאה וללא פערים.
ללא התאמה **NOT MET**	הארגון אינו עומד בדרישה. לא קיימים מענים מול הדרישה, או אלו אינם פועלים כנדרש כך שלא מתקיימת התפוקה הביטחונית, או שלא סופקו הצהרות ואסמכתאות אשר סיפקו את הבודק להשתכנע כי המענה מתקיים, או שמבחן ההוכחה (Test) כשל.
התאמה חלקית **PARTIAL MET**	הארגון יישם מענים אל מול הדרישה, אך אלו נמצאו שאינם עומדים בצורה מלאה מול הדרישה, אינם מספקים את התפוקה הביטחונית המצופה או שסופקו הצהרות ואסמכתאות באופן חלקי אשר אינו מאפשר לבודק להשתכנע בצורה מלאה להתקיימות המענה מול הדרישה, או, שהבדיקה (Test) הצליחה לאמת חלק מן המענה. במקרה זה תוערך באחוזים רמת המענה שהושגה בין 0% ל- 100%.
התאמה לא רלוונטית **NOT APPLICABLE (N/A)**	לא ישים, לא רלוונטי. הדרישה ליישום מענה הגנה אינה יכולה להתקיים במהותה, שכן התשתית בבסיס הדרישה אינה קיימת, זאת באופן שעצם חוסר קיום התשתית אינו יוצר פער, כלומר, משטח התקיפה אינו קיים. יש לספק הצהרה המסבירה מדוע אין הדרישה רלוונטית.

5.6 דוח מסכם

הבודק יתעד את כל בדיקותיו וממצאיו בדוח אחוד. הדוח יכלול התייחסות פרטנית מול כל בקרה רלוונטית. הדוח יכלול את סט הבדיקות שביצע עד שהשתכנע כי הדרישה או חלקה מתקיימים.

6 רשימת הדרישות

בכדי להפחית את הסיכונים להתממשות אירוע סייבר על סביבה המכילה מידע ביטחוני, הארגון נדרש ליישם את המענים לדרישות בתחומים השונים הקשורים לתשתיות המחשוב והסייבר. דרישות אלו כוללות הצבת מענים בצורות של תהליכים, נהלים, קונפיגורציה, מערכות הגנה, טכנולוגיות לחוסן, ועוד.

דרישות אלו מאוגדות על פי 14 קבוצות נושאים –

#	שם קבוצה	מס' הדרישות	שם הקבוצה (English)
1.	**בקרת גישה**	22	Access Control (AC)
2.	**מודעות הגנה והדרכה**	3	Awareness and Training (AT)
3.	**ביקורת ואחריות**	9	Audit and Accountability (AU)
4.	**ניהול תצורה**	9	Configuration Management (CM)
5.	**זיהוי ואימות**	11	Identification and Authentications (IA)
6.	**תגובה לאירועים**	3	Incident Response (IR)
7.	**תחזוקת מערכות**	6	Maintenance (MA)
8.	**הגנה על מדיות**	9	Media Protection (MP)
9.	**אבטחת כוח אדם**	2	Personnel Security (PS)
10.	**הגנה פיזית**	6	Physical Protection (PE)
11.	**ניהול סיכונים**	3	Risk Assessment (RA)
12.	**הערכת רמת ההגנה**	4	Security Assessment (CA)
13.	**הגנה על תקשורת בין מערכות**	16	System and Communications Protection (SC)
14.	**שלמות המידע והמערכות**	7	System and Information Integrity (SI)
	סה"כ דרישות	110	

רשימת הדרישות תואמת לתקנים:

- CMMC 2.0 – רמה 2
- NIST SP 800-171

למרות הערת התאימות לתקינה חיצונית, יש להסתמך על הנוסח המופיע בתקן זה בלבד!

סעיפי הדרישות אינם מופיעים על פי סדר חשיבות אלא ע"פ סדר אלפביתי.

רשימת הדרישות בטבלה להלן –

(בדף הבא)

טבלת דרישות – תקן רב־מגן 2

פרק 1 – בקרת גישה

Access Control (AC)

2.1.1	**גישה מורשית ומזוהה** הארגון יישם וינהל מנגנונים לבקרת הגישה למערכות המידע ולרשת הארגונית עבור משתמשים, תהליכים ושירותים וכן התקנים/מכשירים ממוחשבים, כך שתתאפשר גישה לגורם מורשה המזוהה באופן מהימן בלבד למשאבי הרשת. בתוך כך, כלל הישויות ברשת יהיו מזוהות וכברירת מחדל לא תינתן גישה למשאבי רשת. CMMCv2; AC.L1-3.1.1 – Authorized Access Control
2.1.2	**בקרת פעילויות ותהליכים** הארגון יגביל את גישת המשתמשים והתהליכים המורשים אל משאבי המערכת, אל המתחמים, אל הפעילויות ואל הפונקציונאליות אשר מאושרות להם לבצע במסגרת אחריותם ותפקידם בלבד. הגישה תוגבל, בין השאר, בתקשורת (Firewall), בסוג התוכן המועבר, בגישה ליישומים/תהליכים, שעות פעילות, מקור ביצוע הגישה וכן הגבלת הרשאות; יצירה/קריאה/עדכון/מחיקה/הפעלה. CMMCv2; AC.L1-3.1.2 – Transaction & Function Control
2.1.3	**בקרת זרימת המידע הביטחוני** הארגון יישם מנגנוני בקרה על זרימת המידע הביטחוני ברשת, בין המערכות, ובין התקני הקצה, באופן בו יבוצעו הגבלות וחסימות על תנועת המידע, כך שלא יתאפשר למידע לנוע ולהגיע לנקודות לא מורשות, לא יתאפשר למידע לנוע באופן גלוי (שאינו מוצפן), ולא ינוע במרחבים בעלי נגישות לגורמים לא מורשים / ציבורית. הכוונה למנגנוני בידוק וסינון תשדורות ותוכן בנקודות צומת וגבול, תוך שימוש בעקרונות של סגמנטציה רשתית, ערוצי Tunneling מאובטחים, הצפנה, ערוצים חד-כיווניים, הפרדה ומידור המידע באזורים מוגנים. עבור נתיבים בעלי נקודת קצה ברשת האינטרנט ימומשו, לכל הפחות, שני איזורי הפרדה בידוק וסינון בשרשור. CMMCv2; AC.L2-3.1.3 – Control Data Flow
2.1.4	**הפרדת סמכויות ותפקידים** הארגון ימנע הרשאה לגורם יחיד שתתן אפשרות לבצע תהליך/פעולה/משימה רוחבית שלמה לבדו, ללא התערבות גורם מבקר, זאת לטובת מניעת מצב בו גורם מורשה יחיד יוכל לנצל את ההרשאה שניתנה לו ולבצע פעילות היכולה לסכן מידע ביטחוני, בין אם זו נעשית בטעות או במכוון. יש לסקור ולמפות תפקידים קריטיים הנדרשים להפרדת סמכויות ולוודא כי ההרשאות ליישום סמכויות אלו ניתנות בהתאם עבור משתמשים כדוגמת שילובי תפקידים המאופיינים בניגוד עניינים, תפקידים ספציפיים, או בהרשאות יתר הכרוכות

	בחשיפה לרשומות וקבצים של מידע ביטחוני. תמיכה וניהול מערכות IT כדוגמת משתמשים חזקים, מתן הרשאות ושינויי קונפיגורציה, מפעילי מערכות הגנה בסייבר, מהנדסי פיתוח בעלי גישה למערכות ייצור וכד'. CMMCv2; AC.L2-3.1.4 – Separation of Duties
2.1.5	**מינימום זכויות גישה והרשאות** הארגון יגדיר ויממש את עיקרון "מינימום הרשאות" (Least Privilege) עבור כלל המשתמשים, התהליכים וחשבונות עתירי ההרשאות בכך שיצמצם את: (א') הגישה וההרשאות המוקנות להם רק לרכיבים, למשאבים ולמידע הנדרשים להם לצורך ביצוע הפעולה או התפקיד המוגדר. (ב') הגבלת הגדרות תצורת המערכת אשר המשתמשים יכולים לשנותה. יש להחיל עיקרון זה עבור כלל המשתמשים, הרכיבים,השירותים והתהליכים בכל המערכות, לרבות עבור חשבונות עתירי הרשאות וחשבונות האמונים על ניהול ובקרת מנגנוני ההגנה. יש לבקר ולתעד שינויי הרשאות. CMMCv2; AC.L2-3.1.5 – Least Privilege
2.1.6	**הגבלת השימוש בחשבונות חזקים** הארגון יבטיח כי משתמשים המחזיקים בחשבונות חזקים, עתירי הרשאות לניהול מערכות מידע, אמצעי הגנה, שינוי קונפיגורציה וכן הרשאות עם חשיפה נרחבת למידע. משתמשים אלו יוגבלו ולא יעשו כל שימוש אישי שגרתי אחר בחשבונות חזקים הללו (כדוגמת גלישה באינטרנט, קריאת דוא"ל, עבודה שגרתית שאינה ניהול במערכות ושירותים אחרים בארגון, התחברות מנקודה לא מוגנת), אלא יעשו שימוש ייעודי ומבוקר בחשבון זה רק עבור פונקציות התפקיד המוגדרות לו ובנקודת החיבור המותרת. CMMCv2; AC.L2-3.1.6 – Non-Privileged Account Use
2.1.7	**הבטחת השימוש הנאות בפונקציות משתמש מורשות** הארגון יבטיח כי המשתמשים במערכות המידע יפעילו את הפונקציות המורשות להם באופן בו הן לא יורחבו מעבר למוגדר בתהליכי העבודה, לא יופעלו מעבר למסגרת התפקיד, לא יופעלו ללא הסמכה, לא יועברו לגורם אחר, ולא ינוצלו לשימוש שונה אשר ירחיב את הסיכונים לפגיעה במערכות או במידע הביטחוני. הארגון ייישם אמצעים לגילוי שימוש לא מורשה מסוג זה קרוב ככל האפשר למועד התרחשותו וזאת באמצעות הקמת מנגנוני רישום ומעקב אחר פעולות משתמשים תוך יישום תהליכי בקרה ופיקוח הכוללים ניטור שוטף וחריגות מהנורמה. CMMCv2; AC.L2-3.1.7 – Privileged Functions
2.1.8	**טיפול בניסיונות גישה כושלים** הארגון ייישם אמצעים לזיהוי ניסיונות גישה למערכות/לרשת/לתחנה שלא צלחו, אמצעים אשר מטרתם להתריע ולעכב תקיפות (כדוגמת המבוצעות באמצעים אוטומטיים). אופן הטיפול ואמצעי ההגנה יהיו אוטומטיים ויכללו יישום עקרונות הגנה הכוללים;

	רישום מירב הפרמטרים הידועים (מקום, זמן, כתובת גישה, פרמטרים שסופקו לזיהוי, וכד'), יישום הגנה כנגד רובוטים (לדוג' reCAPTCHA), הגבלת מספר ניסיונות הגישה, נעילה לזמן מוגדר או עד לשחרור בידי בעל תפקיד, אי חשיפת נכונות פרמטרי הזיהוי, אי מתן האפשרות החיצונית לשינוי סיסמא חיצוני שאינו מבוקרם, ניטור והתראה במרכז הניטור הביטחוני. CMMCv2; AC.L2-3.1.8 – Unsuccessful Logon
2.1.9	**הסכמת משתמשים ליישום אכיפת אבטחת מידע** הארגון יוודא כי המשתמשים המורשים הנכנסים למערכות המידע המכילות פוטנציאל נגישות למידע ביטחוני מסכמים על הצבת אמצעים ואכיפת מדיניות אבטחת מידע ופרטיות, הנוגעות לבקרה על אופן שימושם במערכות ע"פ התנאים, לרבות היכרותם את ההשלכות המשפטיות הנוגעות להפרתם. הסכמת המשתמשים תושג בין אם באמצעות אישור דיגיטלי מתועד של תנאי השימוש במערכת בעת הכניסה אליה, או באמצעות חתימה על חומר מודפס. יש לאשרר הסכמות אלו מעת לעת. הארגון ישמור על תיעוד רישום הסכמות המשתמשים לאורך זמן. הארגון יפיק את הסכם השימוש באמצעות יועץ משפטי כאשר הסכם זה יכלול לכל הפחות; המשתמש מכיר כי המערכת מכילה מידע ביטחוני מפוקח, השימוש במערכת הוא לייעודים ספציפיים מורשים המוגדרים מראש, המשתמש מסכים כי השימוש במערכת המידע עשוי להיות מפוקח, מנוטר, מתועד, כפוף לביקורת, וכי אין לבצע שימוש בלתי מורשה במערכת או במידע. שימוש בלתי מורשה כפוף לעונשים פליליים ואזרחיים. CMMCv2; AC.L2-3.1.9 – Privacy & Security Notices
2.1.10	**נעילת Sessions** הארגון יישם נעילת Sessions בתחנות הקצה, ברמת מערכת ההפעלה או ברמת היישום, זאת כדי למנוע גישה או צפייה לא מבוקרת במידע מצד גורמים לא מורשים בסביבת העבודה. מנגנון הנעילה יופעל באופן אוטומטי לאחר משך זמן מוגדר ללא פעילות. בנוסף יפעל המנגנון גם ביזום המשתמש לנעילה. בעת הפעלת מנגנון הנעילה יובטח כי יוסתרו דפוסי פעילות ומידע על המסך וכי לא ניתן יהיה להשתמש מחדש או לשנות את השימוש בעמדה או בהתקניה, אלא אם כן בוצעה הזדהות משתמש מחודשת. CMMCv2; AC.L2-3.1.10 – Session Lock
2.1.11	**ניתוק Session** הארגון יישם אמצעים לניתוק Sessions במערכות, יישומים ותחנות קצה, כאשר במסגרת הניתוק יופסקו כל התהליכים אשר הופעלו על ידי המשתמש בשיוך להתקשרות זו, מלבד תהליכים אשר נוצרו במיוחד לשימוש ללא תלות בהפעלה של ההתקשרות, כאשר מגנון הניתוק יופעל אוטומטית עם התקיימות התנאים; תקופות ארוכות מוגדרות של חוסר בפעילות המשתמש, כניסה למצבים תפעוליים ארגוניים (כניסה לאירוע, חירום, תחזוקה/שדרוג, וכד'), הגבלות שימוש עם סיום שעות עבודה יומיות, סוף שבוע או חופשה, הדפסת כרטיס סיום עבודה, זיהוי הפרת מדיניות השימוש, בקשה מפורשת של מנהל או ממונה הגנה. עבור עמדות עבודה, מנגנון הנעילה יבצע כיבוי של המחשב, אלא אם העמדה מוגדרת לעבודה רצופה.

	CMMCv2; AC.L2-3.1.11 – Session Termination
2.1.12	**בקרת ערוצי הגישה מרחוק** הארגון יבצע פיקוח ובקרה על כל הערוצים המאפשרים גישה מרחוק של משתמשים או תהליכים אל מרחבי המערכת, המידע, הרשת או התקניה, ויוודא כי כל גישה מבוצעת הינה מורשית, מזוהה, מבוקרת ומנוטרת. חיבורים מרחוק כוללים בין השאר גישת משתמשים או תהליכים מרחוק אל רשת הארגון ומערכותיה, דרך רשתות חיצוניות לארגון (למשל אינטרנט, ענן ציבורי או רשת צד ג') בשימוש חיבורים ו- Tunneling מוגן (לדוגמא VPN), כאשר מבוצע לעיתים באמצעות החיבור של התקנים אישיים/פרטיים (טלפונים חכמים, טאבלט, מחשב נייד, וכד'). CMMCv2; AC.L2-3.1.12 – Control Remote Access
2.1.13	**הצפנת ערוצי הגישה מרחוק** הארגון ייישם הצפנה על כל הערוצים המאפשרים גישה מרחוק אל רשת הארגון, באופן בו ערוץ הגישה העובר בתווך ציבורי או חיצוני לרשת יהיה מוצפן ובכך תוגן סודיות המידע העובר על גביו. יש לוודא כי מודל המימוש להצפנה (מוצר החומרה/תוכנה) הינו מאושר לשימוש להגנה על מידע ביטחוני או בעל תאימות מול תקן FIPS 140-1 / 2. CMMCv2; AC.L2-3.1.13 – Control Remote Confidentiality
2.1.14	**ריכוז הפיקוח וההגנה לערוצי הגישה מרחוק** הארגון יצמצם את ערוצי הגישה מרחוק לרשת ויעבירם דרך צמתים בהן ירוכזו מנגנוני ההגנה, הסינון, הבידוק והניטור המיישמים את מדיניות הגישה מרחוק על כל נקודות הגישה המורשות. CMMCv2; AC.L2-3.1.14 – Remote Access Routing
2.1.15	**הגבלת פעולות מהותיות מרחוק** הארגון יגביל את האפשרות לפעולות מהותיות ע"י משתמשים או תהליכים הפועלים מרחוק, לרבות משתמשים חזקים עם יכולת לשינוי הרשאות ותצורה, כך שלא תינתן האפשרות לפעולות העלולות לגרום למעקף מנגנוני ההגנה או ליצירת נזק חמור למידע או למערכות הארגוניות. יש לוודא כי הפעולות אשר יאושרו ינוטרו ויתועדו. CMMCv2; AC.L2-3.1.15 – Privileged Remote Access
2.1.16	**גישה אלחוטית להתקנים מאושרים** הארגון יגביל את האפשרות של התקנים שונים לבצע חיבור אלחוטי לרשתות הארגון באופן בו תבוצע בדיקה אקטיבית מקדימה על ההתקן/החיבור לטובת בחינת היכולת לממש את השליטה על ההתקן/החיבור בהיבטי מנגנוני האימות, התצורה, ההצפנה ומול ההרשאה שהוגדרה טרם הענקת החיבור. יש לוודא כי המנגנון מכיל בין השאר יכולת לבצע בקרה של סוג המכשיר, ציוד

	בבעלות ארגונית או פרטית, דרישות סף לתצורה הנדרשות לחיבור, דרישות לפרוטוקולים ואימות הדדי, ברירות מחדל וכד'. CMMCv2; AC.L2-3.1.16 – Wireless Access Authorization
2.1.17	**הגנת גישה אלחוטית לרשת** הארגון יטמיע מנגנוני הגנה על אפיקי גישה אלחוטית הכוללים אימות זיהוי חד ערכי למשתמש ולהתקן המתחבר ,הצפנה (תאימות מול תקן FIPS 140-1 / 2) ובקרת גישה בתקשורת לרשת לכל הפחות. CMMCv2; AC.L2-3.1.17 – Wireless Access Protection
2.1.18	**חיבור מכשירים ניידים** הארגון יטמיע מנגנוני שליטה ובקרה על אפיקי החיבור עבור מכשירים ניידים המורשים בחיבור אל הרשת הארגונית, מנגנונים הכוללים את המאפיינים הבאים – א. זיהוי המכשיר (חומרה) המבצע את החיבור חד-ערכית. ב. אימות המשתמש המורשה העומד מאחורי החיבור. ג. בדיקת תצורה לרכיב המתחבר – עדכוני תוכנה קריטיים, הפעלת יישומי הגנה מוגדרים, הפעלה בתצורה הממקסמת את מעטפת ההגנה. ד. נטרול/השבתת תכונות מיותרות. ה. וידוא סריקת המכשיר לאיתור קוד זדוני. ו. ניטור ורישום של מכשירים והתחברויות. יש לוודא כי החיבור ניתן למכשירים המאושרים ורשומים מראש במערכת הניהול. יש לוודא כי קיימת מדיניות ארגונית לחיבור מכשירים ניידים, בין אם ארגוניים או פרטיים (BYOD). תחת ההגדרה "מכשירים ניידים" יכללו – כל התקן ממוחשב, ללא חיבור פיזי קבוע (על פי רוב אלחוטי) בעל יכולת חיבוריות ותקשורת – דוגמאות: טלפונים חכמים, טאבלטים, קוראים אלקטרונים, עזרים דיגיטאלים, וכו'. CMMCv2; AC.L2-3.1.18 – Mobile Device Connection
2.1.19	**סודיות מידע ביטחוני במנוחה במכשירים ניידים** הארגון יוודא כי כל פריט מידע ביטחוני אשר הועבר לאחסנה (קצרה או ארוכה) במכשיר נייד או פריט הנוצר בו, אם כרשומה או קובץ או תיקייה, אלו יוצפנו (תאימות מול תקן FIPS 140-1 / 2) בכל עת בה אינם נדרשים בשידור או בעיבוד (Data at Rest). ההצפנה תכלול את כלל מצע האחסון של המכשיר או הצפנה סלקטיבית של פריטי המידע הבטחוני כדוגמת קבצים או תיקיות..

	CMMCv2; AC.L2-3.1.19 – Encrypt Data on Mobile
2.1.20	**ניהול חיבורים לרשתות ומערכות מידע חיצוניות** הארגון ינהל וישלוט בחיבורים בין הסביבה המפוקחת לבין רשתות אחרות חיצוניות לה – רשתות שכנות אשר נמצאות מחוץ לסביבה המפוקחת אף אם הינן נמצאות בתוך הארגון, או רשתות אשר נמצאות מחוץ לשליטת הארגון, לדוגמא רשת צד ג', ענן, אינטרנט ציבורי. תיקבע מדיניות אשר תמנע את הפגיעה ברשת המפוקחת, ובהתאם לה יוצבו חומות אש ומנגנונים יעילים לסינון בידוק וניטור כך שיוגבלו החיבורים והשימושים מתוך הרשת אל מערכות חיצוניות, והפוך, מן הסביבה החיצונית אל הרשת המפוקחת. CMMCv2; AC.L1-3.1.20 – External Connections
2.1.21	**הגבלת השימוש בהתקני אחסון ניידים** הארגון יגביל ויצמצם את השימוש ברכיבי אחסון מידע ניידים למינימום. הארגון יגביל את החיבור/שימוש של התקני האחסון הארגוניים מול מערכות החיצוניות לארגון או כל סביבת עבודה אחרת. הארגון יטמיע מנגנונים רוחביים לשליטה בשימוש בהתקני אחסון ניידים אשר כן מותרים בשימוש. מנגנוני ההגנה יבקרו ויגבילו את אופן השימוש של ההתקנים המורשים בחיבור ע"פ העקרונות - א. כברירת מחדל ייחסם השימוש בהתקני אחסון ניידים. ב. זיהוי חד-ערכי של התקן החומרה מול משתמש מאומת, בדיקת הרשאה לחיבור בנקודת החיבור ובמועד המוגדר. ג. ביצוע חיבור לוגי אל המערכת הארגונית המורשית בלבד. ד. הגבלת השימוש בהתקן לצורך הפונקציה העסקית המוגדרת, במסגרת זמן נתונה. לאחר מכן המשתמש יחזיר את ההתקן. ה. ניטור ותיעוד החיבורים. ו. ניהול רשימת התקנים מאושרים, משתמשים והרשאות החיבור. ז. הכתובים במסמך המדיניות הכוללת נהלי נשיאה ושימוש בהתקן מחוץ לארגון, זאת כדי לצמצם את הזמן בו ההתקן נמצא מחוץ לסביבת האחסנה הארגונית המוגדרת לו, לרבות הגדרות מפורשות היכן מותר ההתקן בחיבור/בשימוש. ח. יש לוודא כי ההתקן מסומן בצורה ברורה – זהות בעליו, ייעודו, מידור, פרטי התקשרות. ט. יש להשתמש בהתקן אחסון הכולל הצפנה של מרחב האחסון הכללי (תואמת תקן FIPS 140-1 / 2) לרבות סיסמת גישה לשימוש (PIN). י. יש לוודא נוהל גריטה סדור של התקן אחסון תקול או היוצא משימוש.

	דוגמאות למצעים/רכיבי אחסון ניידים: כונן דיסק קשיח חיצוני, רכיב זיכרון בחיבור USB (DoK), כרטיסי זיכרון פלאש, כונן פלאש, תקליטורים, וכד'. CMMCv2; AC.L2-3.1.21 – Portable Storage Use
2.1.22	**מניעת הפרסום של מידע ביטחוני** הארגון ימנע העברה לא מבוקרת של מידע ביטחוני מפוקח אל מחוץ לגבולות המוגדרים של הרשת המפוקחת כך שתמנע נגישות ציבורית או פרסום לא רצוי, לרבות חשיפתו במצגות או הצגות ציבוריות, באופן בו סודיות המידע תישמר. יש לוודא בקרה על תהליכים, הרשאות משתמשים, נגישות וממשקים למערכות מידע/תוכן חיצוניות ואופן הפעלתם. נגזרת מידע אשר מקורה במידע ביטחוני מפוקח הנדרשת להצגה או להעברה אל מחוץ לגבולות הרשת המפוקחת, תעבור תהליך סדור של עיבוד תוכן והתאמתה לרמת פרסום ציבורי גלוי, תהליך המבוצע על ידי נאמן ביטחון כאשר תוכן המידע הפרטני מאושר על ידי ממונה הביטחון. אם מתגלה מידע ביטחוני מפוקח במערכת הנגישה לציבור, יש לפעול מידית להסרת מידע זה ובמקביל להתריע על האירוע. CMMCv2; AC.L1-3.1.22 – Control Public Information
פרק 2 – מודעות הגנה והדרכה **Awareness and Training (AT)**	
2.2.1	**יצירת מודעות לאבטחת מידע** הארגון יפעל לטיפוח ויצירת מודעות ארגונית לתחום אבטחת המידע וההגנה בסייבר בקרב כלל אוכלוסיית עובדי הארגון, תוך הנגשת תכנים עדכניים, באופן רציף, עם מיקוד המסרים באופן אשר יותאם לבעלי התפקיד השונים וזאת לצורך השגת - א. בעלי התפקיד מכירים בחשיבות אבטחת המידע ומעורים במתרחש בתחום זה גם מחוץ לסביבה הארגונית באופן כללי. ב. בעלי התפקיד מבינים את השפה והמונחים הבסיסיים בשימוש. ג. בעלי התפקיד יודעים לזהות את הסיכונים העיקריים הכרוכים באבטחת מערכות ומידע והדרכים הנפוצות להתרחשותם. ד. בעלי התפקיד מכירים את המדיניות, התקנים והנהלים הקשורים לאבטחת המידע. ה. בעלי התפקיד בקיאים בכלים ו/או בהמלצות ליישום (Best Practices) הרלוונטיות להגנה על המערכות והתהליכים הקשורים באופן ישיר לתפקידם או לפעולתם. ו. בעלי התפקיד בקיאים באופני ההפעלה המיטביים של מכשירים ממוחשבים בסביבתם אשר מצמצמים את הפגיעות ומרחב התקיפה הפוטנציאלי. ז. בעלי התפקיד בעלי נגישות למקורות ידע נרחבים. יש לוודא את היכולת למדידת ההשפעה של תהליכים אלו על בעלי התפקיד .

	CMMCv2; AC.L2-3.2.1 – Role-Based Risk Awareness
2.2.2	**הכשרה ואימון** הארגון יוודא כי בעלי התפקיד עברו הכשרה נאותה בתחום אבטחת המידע וההגנה בסייבר המותאמת לדרישות על פי תפקידם והתהליכים אותם הם מפעילים וכי כשירות זו נשמרת לאורך זמן. א. ההכשרה לתפקיד הארגוני כוללת היבטים באבטחת מידע וסטנדרטים התואמים לדרישות התפקיד ואלו מיושמים במסגרת התהליך אותו הם מבצעים. ב. מוגדרות ומבוצעות שגרות אימונים תקופתיות לשמירת כשירות המשתמש בתפקידו ובתהליכים אותם הוא מבצע. ג. נקבעו יעדים להשגה, רמת מיומנות, ומדדים להצלחה. כל אלו מבוקרים. CMMCv2; AC.L2-3.2.2 – Role-Based Training
2.2.3	**מודעות לאיום הפנימי** הארגון יפעל ליצירת מודעות ארגונית בקרב כלל אוכלוסיית עובדי הארגון, אשר יותאם למתאר האיומים הנשקף לארגון כתוצאה מפעילות זדונית של עובדים אחרים, בסביבת העבודה או מחוץ לה, לגביהן מבוקשת השגת ההכרה, עירנות, ויצירת מוטיבציה לדיווח, וכל זאת לצורך השגת - א. עובדים מודעים המכירים בסיכונים לארגון הכרוכים באיום הפנימי. ב. העובדים יודעים לזהות התנהגויות ומאפיינים של עובדים אחרים בסביבתם העשויים להוות סימנים להתרחשות איום פנימי. ג. מנהלים יעברו הכשרות רלוונטיות לנושא. ד. העובדים יודעים כיצד לדווח באמצעות מנגנוני דיווח וחקירה דיסקרטים. סימנים לאיום פנימי מצד עובדים כוללים לדוגמא – גישה בלתי מוסברת, גישה שאינה נדרשת לתפקיד, העברות נתונים משמעותיות, הפרות נהלים ושיטות עבודה, דיווחים לא נכונים, שעות עבודה חריגות שלא לצורך, עויינות וחוסר שביעות רצון קיצוני כלפי הארגון, פגיעה וחבלה בציוד ארגוני, ניצול תשתיות ארגוניות למטרה אחרת, ביצוע מעשים או פעילויות לא חוקיות, יחסים לא תקינים עם ממונים, פגיעות בעובדים תחת מרות, בעיות רפואיות או כלכליות לא פתורות, השתייכות לכתות וקבוצות אידיאולוגיות קיצוניות, התנהגות לא הולמת מחוץ לעבודה, וכד'. CMMCv2; AC.L2-3.2.3 – Insider Threat Awareness
פרק 3 – רישום לוג ואירועים **Audit and Accountability (AU)**	
2.3.1	**רישום לוגים במערכות**

	בכל מערכת יופעל מנגנון רישום לוגים (תיעוד אירועי המערכת) . המנגנון יופעל באופן רציף וכי נרשם בצורה שלמה ומפורטת ככל הניתן תיעוד אודות פעילות המערכת עצמה, וכן תיעוד אודות פעולות המשתמשים בה, זאת לצורך בקרה וכדי לאפשר במידת הצורך ניטור, ניתוח, וחקירה של פעילות לא חוקית. יש לוודא כי רישום הלוגים מכיל בין השאר את המאפיינים הבאים – א. רשומות המידע מכילות חותמת זמן (Time-stamp). ב. המידע הנכלל ברשומה מפורט דיו לצורך תחקור לאחור (שיוך למשתמש, כתובות יעד ומקור, משאב הגישה ברשת, ועוד). ג. מבוצע רישום של פעולות שצלחו, וגם רישום פעולות שכשלו. ד. הרשומות מועברות מן המערכת החוצה אל מערכת ייעודית או אחסון חיצוני המוגן מאפשרות לביצוע שינויים. CMMCv2; AU.L2-3.3.1 – System Auditing
2.3.2	**ניטור פעילות משתמשים** הארגון יבטיח כי ניתן לסקור את הלוגים ולהגדיר חוקה בכדי לאתר רישומי פעילות ספציפיים אשר בוצעו על ידי משתמשים ספציפיים ובכך לתמוך בניטור פעילות של משתמש או בביקורות המבוצעות מול משתמשים. יש לוודא כי המידע המאותר משוייך למשתמש מאומת וזאת לטובת מניעת ההכחשה. CMMCv2; AU.L2-3.3.2 – User Accountability
2.3.3	**שמירת לוגים אפקטיבית לאורך זמן** הארגון יבטיח כי מערכות רישום הלוגים המתעדות אירועים, אלו מוגדרות מראש בתצורה אשר תומכת ברישום נתונים אפקטיבי אשר יוכל לשרת בעת הצורך העתידי ביצוע תהליכי סקירה וניתוח אירועי אבטחת מידע, זאת כאשר מבנה שדות הנתונים אופטימאלי והרשומות נשמרות לאורך זמן ארוך דיו. יש לוודא כי מבוצעות הערכות חוזרות של הגדרות תצורה בהתאם לדרישות שעולות, תוך כיול המאפיינים, סינון מידע עודף שאינו רלוונטי, רישום מחזורי (Circular Logging), טיוב שדות נתונים, וכד'. CMMCv2; AU.L2-3.3.3 – Event Review
2.3.4	**התראה על כשל ברישום לוגים** הארגון יבטיח כי בכל מקרה של כשל במנגנון רישום הלוגים תופק התראה וזו תגיע לטיפול אל הגורם האחראי על רציפות פעילות המערכת. יש לוודא ניטור כשלים ברמת החומרה או התוכנה בכלל הרבדים – א. כשל ייצור במערכת המייצרת את הלוגים. ב. כשל בהעברת הלוגים. ג. כשל במנגנוני סינון תוכן וחוקה. ד. כשל במנגנון ניתוח המטפל Online ברשומות המידע.

	ה. כשל במאגר האחסון ארוך הטווח של הלוגים. CMMCv2; AU.L2-3.3.4 – Audit Failure Alerting
2.3.5	**ניתוח והצלבת ממצאים** הארגון יבצע תהליכי סקירה וניתוח נתונים רציפים על מאגר רשומות הלוגים תוך ביצוע קורלציות בינהן ויפיק דיווחים על איתור ממצאים העשויים להעיד על פעילות לא חוקית, בלתי מורשית, חשודה או חריגה בזמן אמת, זאת לצורך מתן תגובה לאירועים ביטחוניים והפעלת פעולות מתקנות בהמשך. CMMCv2; AU.L2-3.3.5 – Audit Correlation
2.3.6	**העשרת ממצאים ודיווח** הארגון יבטיח כי ממצאים העולים במערכי הניטור יעברו תהליך להעשרתם במידע ערכי ויועברו בדחיפה אל הגורם המטפל לצורך מתן תגובה לאירוע ופעולות מתקנות. יש לוודא כי התהליך כולל את המאפיינים הבאים – א. העשרת הנתונים – הרחבת הדיווח באמצעות הקשרים/קורלציות בין אינדיקציות שונות, בין מערכות שונות, העמדה על ציר זמן, הצבעה של קשר סיבה ותוצאה, רמות קריטיות והחשדה, חיבור למידע הארגוני, חיבור לנכסי הרשת, וקישור למודיעין סייבר. ב. אנומליות – זיהוי והצבעה על פעילות חריגה מן הנורמה השגורה. ג. תובנות – הפקת תובנות ודרכים מיטביות לטיפול באירוע/ממצאים. ד. דיווח אחוד – איסוף ואיחוד של הנתונים והתובנות לכדי דוח דיגיטאלי אחוד, בהיר, המונגש בשפה המובנת לגורם המטפל. ה. העברת הדיווח עם הפקת התרעה לגורם המטפל. CMMCv2; AU.L2-3.3.6 – Reduction & Reporting
2.3.7	**סנכרון זמן רישום לוגים** הארגון יבטיח כי כל המערכות הארגוניות, לרבות התקנים המתחברים אליהן, יסנכרנו את שעון הזמן שלהם מול שרת זמן מרכזי, זאת בכדי להבטיח כי כל רישום הפעילויות עבור קבצים ולוגים כוללים חתימת זמן אוניברסלית ומוסמכת. CMMCv2; AU.L2-3.3.7 – Authoritative Time Source
2.3.8	**הגנת רישום הלוגים** הארגון יבטיח כי מערכות רישום הלוגים יהיו מאובטחות כהלכה כך שלא ניתן יהיה לשנות או למחוק את המידע אשר נוצר בהן, לרבות לא ניתן יהיה לשנות את פעולתם המוגדרת, בין אם בכוונה או לא בכוונה. יש להגן על רבדי המערכת – א. המערכות היוצרות את הלוגים. ב. הרכיבים המעבירים לוגים.

	ג. מערכות הטיפול בתוכן – סינון, חוקה, העשרה, דיווח. ד. מערכת האחסון ארוך הטווח של הלוגים, לרבות הגיבויים. CMMCv2; AU.L2-3.3.8 – Audit Protection
2.3.9	**ניהול מערכות רישום הלוגים** הארגון יבטיח כי הגישה למערכות רישום הנתונים והגיבוי שלהן תהיה מפוקחת ותינתן למשתמשים מורשים בלבד, בעלי תפקיד הנושאים באחריות הקשורה לניטור ביטחוני או הפעלת ביקורת, ועל פי הצורך הלגיטימי בלבד. משתמשים חזקים או מנהלי מערכת בעלי הרשאות מובנות הכוללות יכולת לשינוי/מחיקה של נתונים במערכת זו, יש להגדיר עבורם הרשאות מופרדות תפקיד למקרה זה. CMMCv2; AU.L2-3.3.9 – Audit Management
פרק 4 – ניהול תצורה **Configuration Management (CM)**	
2.4.1	**מיפוי נכסים ומערכות** הארגון יקים ויתחזק מיפוי רחב של כלל מלאי הנכסים הדיגיטאליים, המערכות וההתקנים הממוחשבים (כולל חומרה, תוכנה, קושחה ותיעוד) בהם הוא עושה שימוש במסגרת פעילותו העסקית או לטובת פיתוח מוצריו/שירותיו, ויוודא כי המיפוי מכיל את המאפיינים – א. תצורת הבסיס של המערכת הנדרשת לפעולתה – גרסאות הרכיבים והתוכנה. ב. תיעוד ארכיטקטורה וחיבורים בין רכיבים / מערכות. ג. מיקום לוגי ומיקום גיאוגרפי של רכיבים. ד. שינויים והחרגות מתצורת הבסיס שנקבעה. הארגון יעדכן את השינויים המבוצעים בתצורות אלו אל מול המיפוי כך שיישמר עדכני. CMMCv2; CM.L2-3.4.1 – System Baseline
2.4.2	**אכיפה של תצורת הגנה מיטביות** הארגון יקים, ישמר, ויאכוף את תצורות ההגנה המיטביות ה ניתנות ליישום עבור מערכות ורכיבים ארגוניים וזאת ע"פ אמות מידה מוכרות (Best Practices) או ע"פ המלצות היצרנים, כך שיובטח כי המערכות מותאמות לבצע את התפקיד המיועד להן בביטחה. יש לוודא כי קיים תיעוד או רשימות תיוג הכוללות את מפרט הבסיס של המערכות והרכיבים ומכאן, את מפרט השינויים המאושרים לביצוע הנדרשים בכדי להתאים את מנגנוני ההגנה לדרישות הארגון.

	תצורת הגנה תכלול בין השאר – אופן הרכבת מערכות ומנגנוני הגנה ייעודיים, נקודות ממשק וחיבור בין מערכות/רשתות, סנני תוכן ופרוטוקולים, הרשאות, התקנת/הסרת שירותי מערכת הפעלה, וכד'. CMMCv2; CM.L2-3.4.2 – Security Configuration Enforcement
2.4.3	**מעקב אחר שינויי תצורה** הארגון יבטיח את המעקב והבקרה אחר כלל שינויי התצורה המבוצעים במערכות הארגון וישמור לוג אירועים עבור כל שינוי שיושם. ניהול שינויי תצורה יכלול טיפול בהיבטים – א. תחזוקת המצב הבסיסי במצב מוקשח. ב. מעקב אחר שינויי תצורה או שידרוגים. ג. בדיקת השינוי באספקט חוסן המערכות ואם מחליש את רמת ההגנה. ד. בחינה לאישור או אי אישור הפצת השינוי. חלופות. ה. יכולת לביטול שינויים והחזרת מצב לאחור. ו. לוג/תיעוד השינויים. CMMCv2; CM.L2-3.4.3 – System Change Management
2.4.4	**ניתוח השפעת השינוי על רמת ההגנה** הארגון יבטיח כי תבוצע בדיקה סדורה לניתוח ולקביעת אופן ההשפעה על רמת ההגנה של המערכות הארגוניות מול כל שדרוג או שינוי מהותי מתוכנן, זאת קודם ליישום השינוי, כך שאבטחת סביבת ההפעלה תיבדק, בעיות יוצפו, ויבוצע תהליך סדור לקביעת אופן היישום המיטבי של השינוי. ככל שמדובר על שינוי מורכב הכולל הכנסת תוכנות/מוצרים חדשים או שדרוג מערכות הפעלה, יש להבטיח ביצוע בדיקה רחבה מקדימה ברשת/סגמנט נפרד בכדי לבחון את אפקט יישום השינוי. יש לוודא את האותנטיות של הרכיבים הנבדקים. CMMCv2; CM.L2-3.4.4 – Security Impact Analysis
2.4.5	**הגבלת גישה לביצוע שינויים** הארגון יבטיח כי הגישה לבצע שינויים פיזיים או לוגיים במערכות ורכיבים ארגוניים תהיה מוגבלת, ותתאפשר לביצוע רק על ידי משתמשים מורשים ומוסמכים. יש לוודא טיפול בהיבטים – א. מניעת הנגישות הפיזית לבלתי מורשים אל מתחמי תקשורת ושרתים. ב. מצב האפס של מערכת שהותקנה יהיה מוקשח בפני שינוי. ג. תמיכה בתהליך עבודה וכללים מוגדרים לביצוע שינוי. ד. הגדרת משתמשים מוסמכים לביצוע שינוי. ה. הגבלת הרשאות במערכות. ו. חסימת היכולת להרצת קבצי ריצה והתקנה בעמדות עבודה.

	ז. חלונות זמן מוגדרים לביצוע שינויי תצורה. CMMCv2; CM.L2-3.4.5 – Access Restrictions for Change
2.4.6	**יישום מינימום פונקציונאליות** הארגון יבטיח כי המערכות יספקו את סט השירותים המינימאלי ביותר אשר עדיין עומד מול הדרישה התפעולית, וכל שאר הפונקציונאליות העודפת תוגבל או תוסר. יש לוודא טיפול בהיבטים – א. ביטול ברירות מחדל לאחר התקנה הפותחות מנעד רחב של שירותים. ב. איתור פונקציות ושירותים שגרתיים בתיעוד המוצרים. ג. השבתה וחסימת שירותים אשר לא נדרשים. ד. זיהוי וחסימת אפיקי תקשורת (פורטים, פרוטוקולים) אשר אינם בשימוש או אינם בטוחים. ה. שרת או Container יספקו שירות מצומצם ומוגדר יחיד. CMMCv2; CM.L2-3.4.6 – Least Functionality
2.4.7	**הגבלת פונקציונאליות לא חיונית** הארגון יזהה את הפונקציונאליות והשירותים אשר אינם חיוניים לתפעול השוטף העסקי של הארגון, ואלו יוגבלו, יושבתו או יוסרו משימוש. יש לסקור פונקציונאליות בתחומים – א. מוצרים / תוכנות שאינם חיוניות. ב. שרתים, עמדות עבודה, מכונות והתקנים שאינם עוד חיוניים. ג. אוטומציה לא חיונית בתהליכים. ד. אפיקי תקשורת וחיבורים שאינם חיוניים. ה. הרחבות, יכולות, Addons שאינם חיוניים. ו. הגדרות תפקיד שאינן חיוניות. CMMCv2; CM.L2-3.4.7 – Nonessential Functionality
2.4.8	**קביעת מדיניות הפעלת יישומים** הארגון יגדיר ויפעיל מדיניות הפעלת יישומים ברשת הארגונית אשר תמנע שימוש בתוכנה שאינה מורשית, תציב מנגנונים לזיהוי החתימה האותנטית של התוכנות, ותפעל על פי אחד משני עקרונות היישום להלן – א. רשימה לבנה (Whitelisting) – כל התוכנות אינן מותרות להרצה, מלבד אלו המופיעות ברשימה הלבנה. ב. רשימה שחורה (Blacklisting) – כל התוכנות מותרות להרצה, מלבד אלו המופיעות ברשימה השחורה. יש לוודא תקינות רשימות ההיתרים וחתימות התוכנות אל מול מאגרי מידע ייעודיים.

	CMMCv2; CM.L2-3.4.8 – Application Execution Policy
2.4.9	**בקרה על תוכנות המותקנות על ידי משתמשים** הארגון יקבע מדיניות ויציב מנגנונים לטיפול בהתקנות של תוכנות המבוצעות על ידי משתמשים על עמדות העבודה, על ציוד ארגוני או על ציוד פרטי המתחבר למערכות הארגון, כך שההתקנות ינוטרו, יזוהו, ובמידת הצורך יוגבלו אם ההתקנה מפרה את המדיניות שנקבעה או נחשדת כעוינת. CMMCv2; CM.L2-3.4.9 – User-Installed Software
פרק 5 – זיהוי ואימות **Identification and Authentication (IA)**	
2.5.1	**זיהוי** הארגון יבטיח כי כל המשתמשים במערכות המידע, כי כל התהליכים או המכשירים הפועלים בשם משתמשים יהיו מזוהים. יש לוודא כי המזהים בשימוש הינם ייחודיים וחד-ערכיים המצביעים על משתמש, תהליך או מכשיר יחיד. CMMCv2; IA.L1-3.5.1 – Identification
2.5.2	**אימות** הארגון יבטיח כי כל המשתמשים במערכות המידע, כי כל החיבורים, כי כל התהליכים, כל או המכשירים הפועלים בשם משתמשים זהותם תהיה מאומתת, זאת טרם תינתן להם גישה למערכות. CMMCv2; IA.L1-3.5.2 – Authentication
2.5.3	**אימות רב-שלבי** הארגון יבטיח כי תהליך האימות של המשתמשים מול מערכות המידע יכלול אימות רב-שלבי (Multifactor Authentication - MFA), בעל שילוב של שני גורמי אימות או יותר, זאת ללא תלות במקור או בצורת גישת המשתמש לחשבון. יש לוודא כי המנגנונים מיושמים על כלל המשתמשים , לרבות חשבונות ניהול המערכות , חשבונות חזקים ללא יוצא מן הכללולרבות משתמשים המתחברים למערכות מרחוק. CMMCv2; IA.L2-3.5.3 – Multifactor Authentication
2.5.4	**אימות עמיד מול הפעלה חוזרת** הארגון יבטיח כי תהליך האימות של המשתמשים מול מערכות המידע יהיה עמיד בפני שיכפול האימות והפעלה נוספת בזמן או במקום אחר בכדי להשיג כניסה לא מורשית.

	יש ליישם מנגנוני אימות / פרוטוקולים העמידים בהתקפות שידור חוזר (Replay Attack) מסוג זה. CMMCv2; IA.L2-3.5.4 – Replay-Resistant Authentication
2.5.5	**אי שימוש חוזר במזהים** הארגון יבטיח כי לא יבוצע שימוש חוזר במזהי מיחשוב – לא יועברו שמות משתמש מאדם לאדם, לא יועברו מזהים ממכשיר למכשיר, לא יועברו מזהים מתהליך לתהליך, כך שלא יעשה שימוש חוזר באותו המזהה אשר קושר בעבר לסט הרשאות, משאבים או רישום הלוגים במערך הניטור. יש להקצות מזהים חדשים ייחודיים עבור כל מכשיר, משתמש, תפקיד, תהליך, חיבור חדשים. CMMCv2; IA.L2-3.5.5 – Identifier Reuse
2.5.6	**השבתת מזהים/חשבונות בחוסר פעילות** הארגון ישבית/יבטל מזהי מחשובי במערכות המידע לאחר תקופה מוגדרת של חוסר פעילות או בשל פעילות חריגה. יש להבטיח כי חשבונות שאינם פעילים, משתמשים שעזבו או עברו לתפקיד אחר, חיבורים, תהליכים ושירותים לא פעילים יושבתו ולא יהיה ניתן לנצלם למטרות תקיפה. לצורך כך יש להטמיע מנגנון אוטומטי הסורק פעילות חשבונות ע"פ חוקה מוגדרת ומצביע על חשבונות הנדרשים להשבתה או מבצע השבתה. CMMCv2; IA.L2-3.5.6 – Identifier Handling
2.5.7	**שימוש בסיסמאות מורכבות** הארגון יאכוף שימוש בסיסמאות מורכבות / חזקות בכל תהליך של הנפקת סיסמא חדשה למשתמש, מכשיר או שירות, וכן בכל תהליך של ביצוע שינוי של סיסמא על ידי משתמש. יש לוודא כי מוגדרת מדיניות לנושא המכילה התייחסות למינימום מספר התווים, שילוב מספרים אותיות וסימנים, מינימום מוגדר של שינויים בשינוי סיסמא, זמן תוקף מוגבל לסיסמא, המלחת סיסמאות, רישום שינוי סיסמא בלוג. CMMCv2; IA.L2-3.5.7 – Password Complexity
2.5.8	**הגבלת היסטוריית סיסמאות** הארגון יגביל שימוש חוזר בסיסמאות, כך שלא ניתן יהיה לחזור ולהשתמש בסיסמא בה נעשה שימוש קודם מול אותו המזהה למשך פרק זמן מוגדר, או במספר מחזורי שינויי הסיסמא הבאים. CMMCv2; IA.L2-3.5.8 – Password Reuse

2.5.9	**הגבלת שימוש בסיסמאות זמניות** הארגון יגביל את השימוש בסיסמאות זמניות, כך שסיסמאות זמניות יונפקו לצורך חד-פעמי ו יידרשו להחלפה בסיסמאות מורכבות קבועות מייד עם הכניסה הראשונה למערכת. ססמאותזמניות אלו יפוגו תוך פרק זמן קצר אם לא נעשה בהן שימוש. CMMCv2; IA.L2-3.5.9 – Temporary Passwords
2.5.10	**הצפנת סיסמאות** הארגון יבטיח כי סיסמאות יוצפנו בעת אחסנתם (At rest) או בעת העברה/שליחה ממקום למקום (In Transit). יש לוודא כי סיסמאות גלויות (Clear Text) מוצפנות באמצעות מנגנוני הצפנה המיישמים טרנספורמציה חד-כיוונית על הסיסמא המקורית והפיכתה לקוד Hash הכולל מורכבות, לרבות המלחה (Salt), כך שמרגע זה לא ייעשה עוד שימוש בתצורה המקורית הגלויה של הסיסמא והיא תאבד. CMMCv2; IA.L2-3.5.10 – Cryptographically-Protected Passwords
2.5.11	**הסתרת סיסמה בעת הזנתה** הארגון יגן מחשיפת סיסמאות ואמצעי הזיהוי האחרים בעת הזנתם ,מפני משתמשים אחרים או מפני אמצעים לריגול המותקנים בסביבה וזאת באמצעות טישטוש/הסתרת הססמה המוזנת על אמצעי הקלט והמסכים (לדוגמא, שימוש בכוכביות), הקטנת ממשקי הסיסמא, סגירת ממשקי סיסמא ללא פעילות, הגברת מודעות משתמשים, וכד'. יש לוודא כי בעת הזדהות שכשלה, המערכת אינה חושפת בצד המשתמש מהו פרט ההזדהות שאינו נמצא מתאים (קוד המשתמש, הסיסמא, האימייל, מס' הטלפון לקבלת קוד, וכד'). CMMCv2; IA.L2-3.5.11 – Obscure Feedback
פרק 6 – תגובה לאירועים **Incident Response (IR)**	
2.6.1	**טיפול בתקריות ואירועים** הארגון יקים יכולת לטיפול באירועים תפעוליים/מבצעיים על מערכות הארגון, אירועים בהיבטי סייבר / אבטחת מידע, כאשר יכולת זו תבטיח – א. איתור אירועים – זיהוי אירוע, הצבעה על אינדיקטורים להתקיימות אירוע. ב. ניתוח אירוע – זיהוי הרכיב העוין, ההקשר למידע המוגן, העשרה, מדידת ההשפעה, בטיחות, מקור, מעורבים. ג. בלימה – מניעה או צמצום הפגיעה. ד. התאוששות – תיקונים והחזרת המצב לקדמותו. ה. חוסן – הפקת לקחים וסגירת הפערים שהתגלו.

	ו. דיווח – דיווחים סדורים למנהלים, מזמין, רגולטור ובמקרה הצורך לשותפים ולקוחות. יש לוודא כי הארגון ממנה מנהל מקצועי מוגדר לריכוז הטיפול בתקריות ואירועי סייבר. יש להקצות מומחי תוכן בתוך או מחוץ לארגון לתגבור ותמיכה מקצועית בעת אירוע. יש להכין תמיכה של המערכות הניהוליות למצב חירום. יש להכין מדיניות ונהלים למצבים אלו. CMMCv2; IR.L2-3.6.1 – Incident Handling
2.6.2	**דיווח על אירועי אבטחת מידע וסייבר** הארגון יקים תשתית לביצוע מעקב, תיעוד והעברת שרשרת הדיווחים אודות אירועים תפעוליים/מבצעיים במערכות הארגון לגורמים הייעודיים בתוך ומחוץ לארגון באופן אפקטיבי ובשיקוף נכון של המצב, יכולת זו תבטיח – א. העברת הדיווח מהגורמים בשטח למרכז הטיפול האבטחתי / SOC. ב. העברת הדיווח למנהלי הארגון / בעלי עניין (משפטי, תקשורת, וכד'). ג. תיעוד דיגיטאלי רציף של שרשרת האירועים המלווה עם חתימת זמן. ד. ריכוז סיכום ברמה יומית הכולל גיבוש התובנות, סיכום ממצאים, פעולות ההמשך לביצוע, הקצאת משאבים, הערכת נזקים. ה. תיעוד הפעילויות המבוצעות ע"י מומחי תוכן וספקי שירותים מקצועיים מחוץ לארגון. ו. תיעוד השינויים המבוצעים בתשתיות המערכות ע"י גורמי ה- IT במסגרת האירוע. ז. דיווח לרשויות ייעודיות – רגולטור מגזרי, הרשות המוגדרת במכרז התוצרים של המזמין. ח. דיווח לרשויות החוק והחירום. ט. דיווח במידת הצורך לשותפים / לקוחות. י. תיעוד דיגיטאלי על אופני הטיפול וממצאים שמתגלים – הפעלת אמצעים, חיבורים וניתוקים, השבתות, הפעלת צוותים / כוח אדם, ניטור. יא. שמירת התיעוד לאורך זמן. יש להכין נהלים ורשימות תיוג למצבים אלו. CMMCv2; IR.L2-3.6.2 – Incident Reporting
2.6.3	**בדיקה ותרגול יכולת התגובה לאירועים**

	הארגון יקים תהליך עיתי לבדיקת יכולת הארגון להתמודדות ומתן תגובה לאירועים תפעוליים/מבצעיים על מערכות הארגון, בו יבדקו אפקטיביות הנהלים והאמצעים שהוקמו, אופן ניהול האירוע, ניהול המשאבים בארגון, שילוב ה- IT וכן אופן הדיווח, תוך כדי זיהוי חולשות וליקויים פוטנציאליים, וזאת באמצעות סימולציות, תרגילי שולחן או תרגילים מקיפים, הכוללים בסיכום תחקיר, המלצות והתייחסות מנהל הארגון. CMMCv2; IR.L2-3.6.3 – Incident Response Testing
פרק 7 – תחזוקת מערכות **Maintenance (MA)**	
2.7.1	**תחזוקה שוטפת** הארגון יבטיח את התחזוקה השוטפת של המערכות הארגוניות ברמת הרכיבים (כולל חומרה, קושחה, תוכנה), לרבות ההתקנים המחוברים אליהן (מדפסות, מכונות צילום, צב"ד, וכו') באופן בו יבוצעו עבורם תיקונים ושיפורים על פי הצורך, מול כשלים ופגיעויות שמתגלות בהקשר אליהם, כך שלא יתפתחו פערים בהיבטי סייבר/אבטחת המידע של המערכות. פעילות התחזוקה תטפל בהיבטים הבאים – א. תחזוקה מתקנת (תיקון תקלות והחזרת המצב המוגדר לקדמותו). ב. תחזוקה מונעת (יישום עדכונים למוצרים/לתוכנה כפי שפורסמו לטובת איתור ותיקון תקלות סמויות לפני שהן הופכות לתקלות בפועל או הופכות להיות פגיעות לתקיפה). ג. תחזוקה אדפטיבית (בדיקה והתאמה לסביבה כאשר זו משתנה). ד. תחזוקה משפרת (ביצוע שינויים מבוקרים בכדי לשפר פונקציונאליות). CMMCv2; MA.L2-3.7.1 – Perform Maintenance
2.7.2	**תחזוקה מבוקרת** הארגון יבטיח כי הכלים והאמצעים המשמשים את הארגון לבצע את התחזוקה השוטפת של המערכות הארגוניות, לרבות השיטות והכוח אדם המשמש לתחזוקת המערכת, הינם נמצאים תחת בקרה בכדי לוודא שאינם מהווים פתח לפגיעה מכוונת או שאינה מכוונת ברשת ובמערכות. יש לוודא כי אופן השימוש באמצעים/כלים בערוצי התחזוקה מתבצעת על ידי מורשים, באופן מורשה, ההפעלה מתבצעת במגבלות הרשאות המערכת, מסגרת התחזוקה מוגדרת, הכלים נבדקו והם אמינים לביצוע הפעולה, הכלים עצמם הינם מאובטחים ואינם מהווים אמצעי להחדרת קוד עוין וכי הכלים עצמם יהיו עדכניים ומעודכנים. CMMCv2; MA.L2-3.7.2 – System Maintenance Control
2.7.3	**מחיקת מידע ביטחוני ברכיבים בתחזוקה** הארגון יבטיח כי בכל העברה של מכשיר או כלי ממוחשב לצרכי תחזוקה וטיפול

	מחוץ לגבולות המאובטחים של הארגון, או מחוץ לסביבה הממודרת, הרכיב יעבור תהליך בדיקה להימצאות מידע ביטחוני האגור עליו (או שהיה אגור בעבר), ואם אכן היה, הרכיב יעבור תהליך סדור של מחיקת מידע או הסרתו השלמה, ובמידת האפשר גם גריטתו, עד כי לא ניתן יהיה לאחזר או לשחזר עוד את המידע, זאת טרם יועבר לגורם התחזוקה. CMMCv2; MA.L2-3.7.3 – Equipment Sanitization
2.7.4	**בדיקת מדיה/תוכן חיצוני בכניסה למערכות (הלבנה)** הארגון יבטיח כי בכל מקרה בו נדרש להעביר תוכן דיגיטאלי מסביבה חיצונית פנימה אל רשתות הארגון (משותפים, לקוחות, אינטרנט וכו'), החומר הדיגיטאלי ו/או המדיה איתה הועבר יוגדרו כבלתי אמינים (Untrusted), ומכאן יעברו תהליך לאבחון ובדיקה של קוד עוין (הלבנה) טרם יעשה בחומר שימוש במערכות הארגון. תהליך הבדיקה לאבחון ואיתור קוד עוין יכיל את עקרונות הטיפול להלן – א. לא יכנס חומר דיגיטאלי בפורמט/אובייקט בו המערכת אינה יודעת לטפל. ב. ייבדק מקור החומר ומסלול הגעתו. ג. יבוצע אימות לתוכן הקובץ למול סוגו (Truetype) ד. תבוצע סריקה לאיתור חתימות קוד עוין ידועות. המאגר יהיה עדכני. ה. תבוצע סימולציה לבחינת התנהגות הקובץ בסביבתו המיועדת. ו. יבוצעו המרות תוכן, מפורמט לפורמט או פירוק ובניה מחדש (CDR) כך שייווצר שיבוש ברצף קוד עוין ללא תלות אם קיים. ז. המערכת עצמה תהיה חסינה ומוקשחת כנגד השתלטות/התפשטות קוד עוין. ח. לא יהיו נקודות אחרות ברשת להכנסת חומר אשר יעקפו מנגנון/תהליך זה. CMMCv2; MA.L2-3.7.4 – Media Inspection
2.7.5	**אימות זיהוי חזק בערוץ התחזוקה מרחוק** הארגון יבטיח כי בכל הפעלה של חיבור תחזוקה מרחוק של מורשה אל מערכות הארגון, מרשת חיצונית, רשת חיוג או מן האינטרנט, יבוצע על ידי המערכת תהליך לאימות והזדהות רב-שלבי (Multifactor Authentication) מול הגורם המבקש את ההתחברות טרם חיבורו. CMMCv2; MA.L2-3.7.5 – Nonlocal Maintenance
2.7.6	**בקרה לאנשי תחזוקה חיצוניים** הארגון יבטיח כי בכל הפעלה של גורמי תחזוקה חיצוניים (ללא הרשאה בגישה) על מערכות הארגון יתבצע פיקוח צמוד על ידי גורמים מתאימים מהארגון במהלך פעילות התחזוקה. יש לוודא כי הגישה הניתנת לתחזוקה זמנית בלבד ונחסמת בסיום הפעילות. יש ליישם הגבלות כדוגמת: חשבונות זמניים עם מועד תפוגה, מינימום הרשאות, גישה מוגבלת, בקרה על הכנסת חומר, בקרה על חיבור מחשבים וצב"ד שאינו ארגוני, ליווי

	ופיקוח פיזי במקום הפעילות. CMMCv2; MA.L2-3.7.6 – Maintenance Personnel
פרק 8 – הגנה על מדיות **Media Protection (MP)**	
המונח "מדיה" מתייחס למגוון רחב של אמצעים המאחסנים מידע, כולל מסמכי נייר, דיסקים קשיחים, קלטות, מצלמות, כונני USB, תקליטורים/DVD, מצעי זיכרון פלאש, וטלפונים.	
2.8.1	**הגנה פיזית על מדיות** הארגון יבטיח כי רכיבים המכילים מידע ביטחוני, בין אם מופיעים בתצורתם כרכיבים דיגיטאליים כמדיות (דיסק קשיח, דיסק פלאש, תקליטורים, קלטת/סרט מגנטי, וכד') או בין אם המידע מופיע בצורה פיזית (תדפיסי נייר, חוברות, וכד') –יהיו מוגנים פיזית בסביבה התפעולית, כך שלא תתאפשר אליהם גישה פיזית של גורמים לא מורשים. עקרונות ההגנה יכללו טיפול בתחומים – א. ניהול מלאי ומיקום של הרכיבים. ב. סביבה היקפית מאובטחת שאינה נגישה ללא בקרה. ג. מערכות התרעה ואזעקה על כניסה לא מורשית לאזור המבוקר. ד. אחסון ארוך טווח, ארכיב. ה. סריקות ייזומות בסביבות העבודה לאיתור מדיות לא רשומות או שאינן עומדות במדיניות שנקבעה. CMMCv2; MP.L2-3.8.1 – Media Protection
2.8.2	**הגבל נגישות פיזית למדיות למורשים בלבד** הארגון יבטיח כי רכיבים המכילים מידע ביטחוני, בין אם מופיעים בתצורתם כרכיבים דיגיטאליים כמדיות (דיסק קשיח, דיסק פלאש, תקליטורים, קלטת/סרט מגנטי, וכד') או בין אם המידע מופיע בצורה פיזית (תדפיסי נייר, חוברות, וכד') – הגישה הפיזית אל רכיבים אלו (כניסה למתחם המבוקר, שחרור נעילה, לקיחת מדיה, וכד') תותר לגורמים מורשים בלבד, תחת בקרה ותיעוד. עקרונות ההגנה יכללו טיפול בתחומים – א. קביעת מדיניות נגישות ע"י הבעלים של המידע. ב. בקרת גישה לסביבת האחסון למורשים בלבד. ג. הוצאה והחזרת מדיה מן המתחם המבוקר על ידי מורשה. ד. ניהול יומן נגישות של מורשים לרכיבים. CMMCv2; MP.L2-3.8.2 – Media Access
2.8.3	**סילוק מדיות**

	הארגון יבטיח כי טרם השלכה אל מחוץ לארגון, מחזור, או שחרור לשימוש חוזר של מדיות אשר מכילות מידע ביטחוני (או אשר הכילו מידע ביטחוני בעבר), הרכיב יעבור תהליך סדור של מחיקת מידע, מחיקה קריפטוגרפית, הסרת רכיב המידע, או כאשר לא ניתן להבטיח מחיקה אזי גריטה/גריסה/השמדה, עד כי לא ניתן יהיה לאחזר או לשחזר עוד את המידע. יש לוודא כי מדיה/דיסקים המכילים מידע ביטחוני מסומנים מראש. המונח "מדיה" מתייחס למגוון רחב של אמצעים המאחסנים מידע, כולל מסמכי נייר, דיסקים קשיחים, קלטות, מצלמות, כונני USB, תקליטורים/DVD, מצעי זיכרון פלאש נשלפים או מובנים (On-Board) וטלפונים. CMMCv2; MP.L1-3.8.3 – Media Disposal?!?
2.8.4	**סימון מדיות** הארגון יבטיח כי רכיבים המכילים מידע ביטחוני, בין אם מופיעים בתצורתם כרכיבים דיגיטאליים כמדיות (דיסק קשיח, דיסק פלאש, תקליטורים, קלטת/סרט מגנטי, וכד') או בין אם המידע מופיע בצורה פיזית (תדפיסי נייר, חוברות, וכד') – יסומנו בסימון נגיש, בתוויות נצמדות או בהדפס, הכולל סימון בהיר המיועד להבחנת גורמי אנוש, כדי להתריע כי היא מכילה מידע ביטחוני, לרבות סימון המציג את השיוך למידור או לפרויקט. CMMCv2; MP.L2-3.8.4 – Media Markings
2.8.5	**שינוע מדיות** הארגון יבטיח כי רכיבים המכילים מידע ביטחוני, בין אם מופיעים בתצורתם כרכיבים דיגיטאליים כמדיות (דיסק קשיח, דיסק פלאש, תקליטורים, קלטת/סרט מגנטי, וכד') או בין אם המידע מופיע בצורה פיזית (תדפיסי נייר, חוברות, וכד') – יהיו מוגנים במהלך השינוע/הובלה שלהם מחוץ לאזורים המבוקרים. עקרונות ההגנה יכללו טיפול בתחומים – א. מינוי גורם אחראי, בעל תפקיד או צוות המורשה לשינוע. ב. שילוב מנגנוני נעילה. ג. שילוב מנגנוני הצפנה. ד. שילוב מנגנוני Anti-Tamper לעיכוב או זיהוי פריצה. ה. בקרה על מסלול ההובלה ומניעת חניית ביניים. ו. מעקב אחר השינוע עד הגעת הרכיב ליעדו. יש להעדיף שינוע חומר בתצורה דיגיטאלית מוצפנת על פני שינוע חומרי נייר. CMMCv2; MP.L2-3.8.5 – Media Mobility ?!
2.8.6	**הצפנת מדיות ניידות** הארגון יבטיח כי מדיות והתקני אחסון דיגיטאליים בעלי פוטנציאל להכיל מידע ביטחוני ויכולת לחיבוריות ו/או ניידות (דיסק קשיח, דיסק פלאש, תקליטורים, DoK, קלטת/סרט מגנטי, וכד') – המידע האגור בהם (Data-at-Rest) ישמר באופן מוצפן

	במצב המנוחה/נשיאה, כך שגם במקרה והמדיה תאבד, הנתונים לא יהיו נגישים. וודא כי המדיה לא תכיל את מפתחות ההצפנה. וודא כי מימוש ההצפנה (מוצר החומרה/תוכנה) מאושר לשימוש להגנה על מידע ביטחוני או בעל תאימות מול תקן FIPS 140-1 / 2. CMMCv2; MP.L2-3.8.6 – Portable Storage Encryption
2.8.7	**הגבלת השימוש בהתקני מדיה נתיקים** הארגון יבטיח את הגבלת השימוש במדיות ובהתקני איחסון נתיקים מול מערכות הארגון (מחשב נייד, DoK, דיסק USB, מצעי פלאש, תקליטורים, וכד') למינימום האפשרי ויגן על האמצעים הנתיקים הנדרשים להיות מחוברים אל המערכות במקום הפעלתם (דיסקים/RAID, קלטות) מפני ניתוקם על ידי לא מורשה. עקרונות ההגנה יכללו טיפול בתחומים – א. איסור שימוש בהתקנים אישיים/פרטיים. ב. חסימת חיבור התקנים בעמדות עבודה של משתמשים. ג. חיבור התקנים מורשים בלבד. ד. נעילת התקנים נתיקים פיזית מאחורי כלובים. ה. סריקה עיתית לאיתור וירוסים/קוד עוין. ו. הנחיות לרכש. ז. מדיניות וכללים. CMMCv2; MP.L2-3.8.7 – Removeable Media
2.8.8	**בעלים יחיד למדיות נתיקות משותפות** הארגון לא יאשר שימוש במדיות והתקני אחסון דיגיטאליים נתיקים בעלי פוטנציאל להכיל מידע ביטחוני אשר הינם בשימוש על ידי מספר גורמים (משותפות), ולא מוגדר עבורם גורם יחיד האחראי לאבטחתו.. CMMCv2; MP.L2-3.8.8 – Shared Media
2.8.9	**הגנה על גיבויים** הארגון יבטיח את ההגנה על סודיות גיבויי המידע הביטחוני במקומות אחסונם. עקרונות ההגנה יכללו טיפול בתחומים – א. הצפנת קבצים / מדיה. ב. ניהול מורשים בגישה. ג. הגנה פיזית / נעילה של מקומות האחסון של מדיות הגיבוי. ד. הפעלת שירותי ההגנה הייעודית של ספקי גיבוי בענן. וודא כי המימוש ההצפנה (מוצר החומרה/תוכנה) מאושר לשימוש להגנה על מידע ביטחוני או בעל תאימות מול תקן FIPS 140-1 / 2.

RM-2

	CMMCv2; MP.L2-3.8.9 – Protect Backups
פרק 9 – אבטחת כוח אדם **Personnel Security (PS)**	
2.9.1	**בדיקת רקע ואמינות** הארגון יבטיח כי לא תינתן לאדם (בכל מעמד, אם עובד, מנהל, שותף, וכד') גישה או הרשאה למערכות ארגוניות לגביהן קיים פוטנציאל לחשיפה למידע ביטחוני, לרבות לא תינתן גישה או הרשאה לטיפול במידע ביטחוני, זאת טרם נבדקו על ידי הרשות הביטחונית הממונה, ישירות או בתיווך הגורם המזמין, בכפוף לדרישה הרשומה במכרז, והושג לגביהם אישור אישי מפורש (הכשר ביטחוני) הניתן בכתב בחתימת ממונה ביטחון, אישור רשמי המותאם לסיווג המידע הביטחוני. ככל שמדובר על מידע ביטחוני בסיווג בלמ"ס, או כאשר הארגון אינו בעל זיקה ביטחונית, מומלץ ליישם כחלופה תהליך הכולל שילוב של בדיקות כדוגמת בדיקות אישיות באמצעות חברות מומחה (הכוללות תאימות של תכונות יושרה ואמינות, שיקול דעת, נאמנות, ויציבות), בדיקות רקע על ידי ממליצים במקומות העבודה הקודמים, סקירה באינטרנט לאיתור השתייכות לארגונים בעלי אינטרס הסותר לאינטרסי הארגון, בקשה להיעדר רישום פלילי (תעודת יושר), חתימה על הסכמי סודיות, מילוי הצהרות אישיות, עריכת בדיקות פוליגרף, אם נדרש, באימות של ממצאים מול המועמדים. CMMCv2; PS.L2-3.9.1 – Screen Individuals
2.9.2	**ניוד כוח אדם** הארגון יבטיח כי החשיפה למידע ביטחוני במערכות הארגוניות תטופל בהתאמה לתהליכי ניוד כוח האדם וסטאטוס התפקיד העדכני בארגון, כך שעבור עובדים/משתמשים שסיימו תפקיד או הועברו לתפקיד אחר שאינו דורש נגישות למידע ביטחוני, תבוצע התאמה מהירה של הנגישות וההרשאות למצב החדש, לרבות תהליך מסודר להחזרת אמצעים בסיום העסקה. עקרונות ההגנה יכללו טיפול בתחומים – א. חסימת גישה והרשאות למערכת בסיום תפקיד / סיום העסקה. ב. החזרת כל ציוד ה- IT של הארגון (כגון, מחשבים ניידים, טלפונים סלולאריים, התקני אחסון, מדיות) ג. החזרת כרטיסים ואמצעי הזדהות. ד. החזרת מפתחות, ביטול גישה הפיזית למתחמים עם מידע ביטחוני. ה. החזרת חומר כתוב ומדיות. ו. סגירת היכולת לחיבור מרחוק. ז. תדריך יציאה לריענון הסכמי סודיות ולאיתור פערים אבטחתיים בעזיבה. ח. חסימת חשבונות כללית מהירה למשתמשים במצבים של השעיית עובד עקב פעילות סוררת. ט. רישום תהליכים סדור ודיווח לממונה ההגנה.

	CMMCv2; PS.L2-3.9.2 – Personnel Actions
פרק 10 – הגנה פיזית **Physical Protection (PE)**	
2.10.1	**מניעת גישה פיזית לנכסים ומערכות ממוחשבות** הארגון יבטיח כי לא תתאפשר גישה פיזית לגורמים לא מורשים לסביבה בה נמצאות ופועלות מערכות ממוחשבות, שרתים, ציוד תקשורת, רכזות, והתקנים שונים התומכים בהם, לרבות לא תתאפשר הגישה הפיזית למתחמי עבודה, משרדים, מעבדות, מתחמי ייצור והרכבה, בהם מעובד או מאוחסן מידע ביטחוני, או מתחמים המכילים נכסים טכנים אחרים הנדרשים בהגנה. עקרונות ההגנה יטפלו בתחומים – א. הצבת הציוד בחדרים נעולים או איזורים מאובטחים, שמירה והגנה. ב. תגי הזדהות, כרטיסים עם קוראים, אישורי הרשאה למתחמים שאינם ציבוריים. ג. הצבת מנגנוני אחסון ונעילה פיזיים, כספות, ארונות, כלובים ומנעולים. ד. הצבת דלתות מעכבות פריצה. ה. ניהול ותחזוק רשימות מורשים בגישה. CMMCv2; PE.L1-3.10.1 – Limit Physical Access
2.10.2	**ניטור הסביבות המוגנות** הארגון יבטיח כי המתחמים המוגנים בפני גישה פיזית לא מורשית יהיו מנוטרים באופן רציף על ידי מערכות גילוי וחיישנים מסוגים שונים בכדי לוודא כי לא מבוצעת פריצה או מעקף של מנגנוני מניעת הגישה, ההתקנים והנעילות השונות. בכל מקרה של זיהוי או חשד לאירוע מסוג זה, תועבר ההתרעה לטיפול המוקד הארגוני וגורמי ההגנה. מערכות גילוי וחיישנים אלקטרוניות יכללו למשל – מצלמות וידאו, מערכות DVR, גלאי נפח ותנועה, גלאי קול וניפוץ, מערכות לזיהוי פנים, גלאי גדר, גלאי פתיחת דלתות וחלונות. מערכי גילוי אחרות יכללו למשל – שומרים, מאבטחים, כלבים. CMMCv2; PE.L2-3.10.2 – Monitor Facility
2.10.3	**ליווי מבקרים** הארגון יבטיח כי מבקרים או אורחים אשר נדרשים בכניסה למתחמי העבודה של הארגון יהיו מבוקרים ומטופלים ביטחונית – מאושרי כניסה, מלווים ברציפות ע"י עובדים, יהיו מסומנים כאורחים ופעילותם תהיה מנוטרת. עקרונות ההגנה יכללו טיפול בתחומים – א. הרשאה לכניסת מבקרים/אורחים הינה מבוקרת ומתועדת – בייזום הארגון, איש קשר, צורך מוגדר, רציפות ומשך ביקור מאושרים מראש. ב. ליווי המבקרים ע"י עובדים במשך כל זמן שהייתם במתחמים.

	ג. מבקרים יזוהו כאורחים באמצעות ענידת תג מיוחד. ד. פעילות המבקרים במתחמי הארגון תהיה מנוטרת ומצולמת. ה. העלאת מודעות עובדים לערנות והגבלת תנועה חופשית של מבקרים. CMMCv2; PE.L1-3.10.3 – Escort Visitors
2.10.4	**תיעוד גישות פיזיות** הארגון יבטיח כי פעילויות עובדים ומבקרים הכרוכות בגישה פיזית למתחמים או נכסים ארגוניים מוגנים יאספו ממערכות בקרת הכניסה באתרים השונים ויהיו מתועדות ביומן רשומות או באמצעות מערכת לוג ממוחשבת, עם יכולת אחזור רשומות, ושמירת הנתונים לאורך זמן. גישות פיזיות הנדרשות בתיעוד יכללו למשל – הנפקת כרטיס גישה, כניסה/יציאה לארגון, מעבר/כניסה למתחם מבוקר/קרוסלה, פתיחת דלת מבוקרת, פתיחת נעילה של ארון/כספת מבוקרים, הפעלת קורא כרטיסים לזיהוי, מעבר בנקודת זיהוי פנים נטרול או הפעלה של מערכת אזעקה וגילוי פריצה. CMMCv2; PE.L1-3.10.4 – Physical Access Logs
2.10.5	**ניהול מערכות בקרת הגישה הפיזית** הארגון יבטיח כי המערכות, ההתקנים ואמצעי הנעילה אשר משמשים לביצוע בקרת הגישה הפיזית למתחמים ונכסים מוגנים ברחבי הארגון יהיו מנוהלים – מתועדים, שמישים, חסינים, ומופעלים כשורה. עקרונות ההגנה יכללו טיפול בתחומים – א. תרשימי פריסת אמצעים והתקנים בשטח. ב. רישום הקצאת תגים ומפתחות לאנשים. ג. רישום הקצאת התקני כספות, מיקום, בעלים, הקצאת מפתחות וקודים. ד. בקרה על השימוש בהפעלת מערכות אזעקה, מנעולים, ונעילה היכן שנדרש. ה. בקרה על אופן התקנת ההתקנים והאמצעים ע"פ הוראות היצרן ובחינת חוסנם. ו. בקרה רציפה על שמישות התקני בקרת הכניסה, מצלמות וחיישנים, מנגנוני ההתרעה. ז. שגרת החלפת נעילות, קודים, סיסמאות כניסה. ח. החזרת תגים ומפתחות בסיום תפקיד. ט. גישה מוגבלת למערכות הניהול ובקרת הגישה הפיזית למורשים בלבד. CMMCv2; PE.L1-3.10.5 – Manage Physical Access
2.10.6	**אבטחת המידע הביטחוני מחוץ לארגון** הארגון יבטיח כי רציפות אבטחת המידע הביטחוני תישמר גם במתחמי עבודה חלופיים הנמצאים מחוץ לארגון, כך שיובטח כי – א. באתרי העבודה החלופיים מותקנים ומופעלים אמצעי הגנה באופן הזהה

	לארגון. ב. באתרי העבודה החלופיים נאכפים הנהלים על העובדים והמבקרים באופן הזהה לארגון. ג. תהליכי הבקרה והניהול של מערכות ההגנה מבוצעים באופן הזהה לארגון. ככל שמדובר על מתחמי עבודה של עובדים "מן הבית", תובטח זהות רמת הגנה והגישה המאובטחת למערכות הארגון. יותאמו הדרישות ויוקצו האמצעים לביצוע הגנה הפיזית על הציוד הארגוני ואמצעי הגישה מרחוק. לא תאושר אחסנה של מידע ביטחוני בתצורה פיזית (נייר, התקני מדיה לא מוצפנים) מחוץ לארגון, לרבות בתים של עובדים. CMMCv2; PE.L1-3.10.6 – Alternative Work Sites
פרק 11 – ניהול סיכונים **Risk Assessment (RA)**	
2.11.1	**הערכת סיכונים עיתית** הארגון יבצע תהליך בחינה ברמת הארגון, ברמת המשימה, ברמת התהליכים העסקיים, וברמת מחזור החיים של פיתוח התוצרים, ויעריך את הסיכונים היכולים לנבוע מכל גורם היכול להפחית את הבטחת המשימה, לפגום בהצלחתה, לפגוע בתדמית או במוניטין, לפגוע ביחידים, לפגוע בארגונים שותפים או לקוחות, לפגוע בסביבה ,במדינה, או להביא לפגיעה או חשיפה של מידע ביטחוני. מכאן, תשוקלל רמת הפגיעה הפוטנציאלית, ותוקם תכנית לטיפול/התמודדות מול פגיעויות אלו. הערכת הסיכונים נדרשת להיות מתועדת על כל שלביה. יש לבצע את הערכת הסיכונים במרווחי זמן קבועים ומוגדרים. יש לוודא כי מומחה תוכן לאבטחת מידע / CISO יוביל את חלק הבדיקה הרלוונטי לסיכונים, תרחישים, כשלים הנוגעים למערכות ממוחשבות, תשתיות טכנולוגיות וכל הקשור למידע ביטחוני. הערכת הסיכונים תכלול טיפול שלם בנושאים – א. בחירה ופעולה לפי פרקטיקה / מתודולוגיה / מודל לניהול סיכונים מוגדרת המתאימה לארגון. ב. איתור והגדרת מקורות הסיכון, פנימיים וחיצוניים (ספקי שירותים, עובדים, כשל של מערכות לפעול כמתוכנן, כשלים בטכנולוגיות, תהליכים עסקיים שאינם מתוכננים כהלכה, תהליכים המבוצעים בצורה גרועה, פעילות בשוגג אל אנשים, אסונות טבע, כשל בתשתיות ציבוריות, כשל בשרשרת האספקה, הפרות/תביעות משפטיות, הפרות רגולציה, ועוד). ג. התרחישים הרלוונטיים למימוש האיום בסביבות ותשתיות הארגון, והערכת סבירות להתרחשותם. ד. תאימות לגבי עוצמת הפגיעה והנזק לארגון. ה. הערכת תעדוף לטיפול בסיכונים/פגיעויות, השקעה נדרשת, עלות-תועלת.

	ו. המלצות לאופן ההתמודדות/התיקון מול הסיכונים/פגיעויות. ז. תאימות מחדש של הסיכונים לאחר מימוש ההתמודדות/תיקון. CMMCv2; RA.L2-3.11.1 – Risk Assessments
2.11.2	**סקירת פגיעויות** הארגון יבצע סקירה יזומה מול המערכות, ההתקנים, התשתיות, התהליכים והיישומים הארגוניים בתדירות מוגדרת בכדי לגלות בהם באופן אקטיבי כשלים / פגיעויות (סמויות, מוכרזות או חדשות) אשר יכולות להשפיע ולסכן את המערכות, ההתקנים והיישומים בעלי פוטנציאל נגישות למידע ביטחוני, זאת באמצעות תהליכים ייעודיים המשלבים בין השאר גם כלים אוטומטיים. שגרת סריקת הפגיעויות תכלול התייחסות וטיפול בעקרונות/התחומים/הנושאים – א. הגדרת תדירות ביצוע הסקירות ע"פ סוגן – אקראיות, מדגמיות, רציפות, מתוזמנות. ב. אפיון הסריקה – תעדוף מוקדי הסקירה ע"פ ממצאי תכנית ניהול הסיכונים, הגדרת ההישג הנדרש, נקודת המבט (תוקף חיצוני או פנימי), היקף הסקירה, מערכות והתקנים בתכולת הסקירה, שכבות הפעולה, שיטה (למשל Black Box או White Box). ג. הקמת צוות הבדיקה (לאחר האפיון הנ"ל) – איתור גורם מקצועי מומחה, התאמת הכלים למשימה, אישור סקריפטים להפעלה, סיכונים ומניעת גרימת נזק. ד. ייזום סקירות – ביצוע סקירות ייזומות תוך פרק זמן קצר בעקבות פרסום פגיעות רלוונטית חדשה. ה. סיכום סקירות הפגיעויות תכלול בסיומה הפקת דוח מקצועי הכולל את פירוט הממצאים והמלצות לתיקון. להלן הסוגים השונים של הסריקות הנדרשות להיכלל במסגרת הדרישה: 1) ביצוע סריקות לאיתור גרסאות לא מעודכנות או אי התקנה של טלאי הגנה במערכות תוכנה. 2) ביצוע סריקות לאיתור פגיעויות מוכרזות (CVE) מול התקנים ומערכות מחשב תוך פרק זמן קצר עם פרסומן, לרבות שקלול רמת הפגיעות של הפגיעויות המוכרזות (CVSS). 3) ביצוע סריקות מן האינטרנט לבחינת חשיפת כתובות IP, פורטים, ממשקי תחזוקה, והתקנים. 4) ביצוע סריקות לאיתור פרסומים גלויים של חומרים/מסמכים רגישים מתוך הארגון החושפים שיטות, בעלי תפקיד, מפרטים טכנולוגיים, מזהי תקשורת, פרטי הזדהות, שמות וקודים של נכסים תקשוביים, ועוד. 5) ביצוע מבדקי חדירה (PT) / צוות אדום לאימות החוסן בתרחישים מוגדרים. 6) ביצוע סריקות אוטומטיות לבחינת חולשות ונקודות תורפה בקוד תוכנה עליו מבוצעות התאמות או קוד המגיע ממקורות לא אמינים.

	7) ביצוע סריקות לאיתור הפעלת תכונות הגנה נאותות במערכות צד-שלישי ויישומי ענן. CMMCv2; RA.L2-3.11.2 – Vulnerability Scan
2.11.3	**תיקון פגיעויות** הארגון יבצע תיקון לנקודות התורפה והפגיעויות אשר התגלו בתהליך הערכת הסיכונים או תהליכי סריקת הפגיעויות, זאת תוך התחשבות בגורמים – תעדוף הפגיעויות הקריטיות, הסיכון לניצול הפגיעות, רמת המאמץ הנדרשת בתיקון, משך זמן התיקון והמשאבים הנדרשים, עלות מול תועלת, לרבות הרלוונטיות להגנה על מידע ביטחוני. הארגון יתעד וירשום כל פגיעות שהתגלתה, רציונאל ההחלטה לתיקון או שלילתו, קישור אל תכנית/משימת התיקון, ויעקוב אחר כל פעילויות תיקון הפגיעות כדי להבטיח את השלמתן. הארגון יתעדף ביצוע פעילויות מתקנות הניתנות ליישום מהיר אשר מפחיתות את משטח הפגיעות או את הדרכים לניצול הפגיעות, זאת באמצעות למשל – הפעלת דרכים למעקף הבעיה (Workarounds) ע"פ פרסומי יצרנים, שינוי קונפיגורציה, רידוד תכונות, ניתוק חיבוריות וקישורים, שינוי תהליכים, החלפת תוכנות/רכיבים/כלים באחרים, התקנת כלי נוסף בטור, וכד'. CMMCv2; RA.L2-3.11.3 – Vulnerability Remediation
פרק 12 – הערכת רמת ההגנה **Security Assessment (CA)**	
2.12.1	**בקרת המערכות ואמצעי ההגנה** הארגון יבצע באופן תדיר בדיקות על המערכות ואמצעי ההגנה המופעלים בארגון בכדי לוודא כי אלו פועלות באופן תקין ואפקטיבי ע"פ המוגדר להן, ויחזיק רשימת ליקויים עדכנית הנדרשת בטיפול. עקרונות ההגנה יכללו טיפול בתחומים – א. יצירת רשימת נכסי המערכות ואמצעי ההגנה הארגוניים. ב. קביעת תדירות ביצוע הערכת בקרות ההגנה לפי מערכת. ג. ביצוע הערכת ההתאמה לדרישה, רציפות ההפעלה, ומדידת היעילות של בקרות ההגנה. ד. סריקת פגיעויות, עדכון גרסאות, טלאי הגנה. ה. תוצאות וממצאים אודות הליקויים מתועדים ברשימה/דוחות. ו. הגדרה לתעדוף הביצוע של פעילויות מתקנות הניתנות ליישום מהיר והמשקמות לפחות חלק מיכולות ההגנה. CMMCv2; CA.L2-3.12.1 – Security Control Assessment

2.12.2	**פיתוח ויישום תוכניות פעולה לתיקון ליקויים** הארגון יקים, יתחזק ויישם תוכניות פעולה אשר נועדו לתקן ליקויים ופגיעויות, להפחית נקודות תורפה או לשקם יכולות שנפגמו במערכות ובאמצעי ההגנה הארגוניים. העקרונות לפיתוח התוכנית יכללו טיפול בתחומים – א. רשימת ליקויים ופגיעויות הנדרשות בטיפול/תיקון. ב. תכנית פעולה מעשית לתיקון הליקוי, הפגם, נקודת התורפה, או כחלופה – שיקום חלקי ומהיר של יכולות אמצעי ההגנה כמצב זמני. ג. התכנית כוללת תיעוד של – בעלים של המשימה, הגדרת אבני דרך ברורות, הגדרת אחראים לביצוע, משאבים, תאריכי סיום. ד. מבוצעת בדיקה למדידת הכיסוי, היעילות והתפוקה האבטחתית של התכונה שתוקנה. ה. תכניות העבודה מיושמות ומבוקרות עד להשלמתן על ידי מנהל ההגנה. CMMCv2; CA.L2-3.12.2 – Plan of Action
2.12.3	**ניטור ומדידת בקרות ההגנה** הארגון יבצע ניטור רציף ומעקב אחר בקרות ההגנה המיושמות במערכות הארגון בכדי למדוד ולהבטיח את האפקטיביות שלהן. עקרונות הניטור והמדידה יכללו טיפול בתחומים – א. יכולת ניטור ספציפית מול בקרת הגנה או קבוצת בקרות בעלות משימה ייעודית. ב. יכולת רב שכבתית – ניטור תכונות ברכיבי חומרה, בתוכנה, במערכות הפעלה, בתקשורת ברשת, ביישומים, קונפיגורציה, במסדי נתונים, במערכות אחסון. ג. יכולת ניטור רציפה. ד. יכולת ניטור אוטומטית, מבוצעת באמצעים טכנולוגיים. ה. יכולת מדידת האפקטיביות, הצבת פרמטרים מאפיינים לתקינות, עדכניות, והגעה להחלטה האם האמצעי פועל תקין. ו. תוצר הניטור מצביע על ליקויים ותקלות בזמן אמת תוך העברת התרעות למרכז הניטור האבטחתי (SOC). ז. מוקצים בעלי תפקיד האחראים לתפעול וניהול מערכות הניטור. ח. מופקים דוחות להצבעה על תפוקות הניטור לבעלי עניין. CMMCv2; CA.L2-3.12.3 – Security Control Monitoring
2.12.4	**תוכנית לאבטחת מערכות הארגון** הארגון יקים, יפתח, יתחזק ויעדכן תוכניות מקיפות לאבטחת כלל הנכסים והמערכות הארגוניות.

	התכניות יובלו ויבוקרו על ידי מנהל אבטחת המידע / CISO. הארגון יסמן ויציג בתכניות אלו את ההיבטים/הנושאים הקשורים לתיחום הנכסים והמערכות הכוללות טיפול במידע ביטחוני. התכניות יכללו את התחומים והנושאים הבאים ברמת פירוט של מערכת – א. תוכניות ההגנה יכללו את הגדרת היקף הנכסים הכלולים בתיחום המוגדר עבור מידע ביטחוני. ב. תוכניות ההגנה יכללו את רשימת הנכסים הכלולים תחת התאימות המבוצעת באמצעות תקן זה. ג. תוכניות ההגנה יכללו את התיאור הטכני הכללי, סביבת הפעולה ואופן הפעולה של כל מערכת מידע המעבדת, מאחסנת ומעבירה מידע, לרבות תיאור ממשקיה. ד. תוכניות ההגנה יכללו תיאור בעלי תפקיד והאחריות המוטלת עליהם בהקשר הקמה ואחזקה תפעולית שוטפת (IT), בהקשר הפעלת תכונות המערכת (כמשתמשים), ובהקשר אבטחת המערכת. ה. תוכניות ההגנה יכילו את הצגת החיבוריות/קישוריות, קשרי הגומלין והתלויות של מערכות זו לזו. ו. תוכניות ההגנה יכילו את דרישות ההגנה – סט הדרישות המוטלות על אופן הטיפול במידע בארגון הנגזרות מחוקים, פקודות הנהלה, מדיניות, נהלים, תקינה/רגולציה, תקנות ארגוניות, אשר נועדו להבטיח את הסודיות, המהימנות, והזמינות של המידע המעובד, מאוחסן או מועבר במערכות הארגון. ז. תוכניות ההגנה יפנו למדיניות ממנה נבעו דרישות ההגנה. ח. תוכניות ההגנה יתרגמו את דרישות ההגנה למערך של בקרות ואמצעי הגנה מעשיים ליישום. ט. תוכניות ההגנה יכללו תיאור-על כיצד הבקרות ואמצעי ההגנה ליישום עומדים באפקטיביות הנדרשת מול הדרישה. י. תוכניות ההגנה יפנו לנהלים ומסמכי Best Practices אשר תומכים ביישום בקרות ההגנה. יא. תוכניות ההגנה יפנו למפרטים ומסמכי תיעוד אחרים אשר ירחיבו את המידע. יב. תוכניות ההגנה יכילו הגדרת תדירות העדכון שלהן, בדרך כלל לפחות מדי שנה. CMMCv2; CA.L2-3.12.4 – System Security Plan (SSP)
פרק 13 – הגנה על תקשורת בין מערכות **System and Communications Protection (SC)**	
2.13.1	**הגנת גבולות הרשת**

	הארגון יגן על מבואות הרשת, על הקישורים שלה, הממשקים, החיבוריות, השערים הלוגיים המחברים אותה לסגמנטים נפרדים או לרשתות זרות. זאת באמצעות בקרה על הקמת הקשר ולאחר מכן ניטור ושליטה על תעבורת התקשורת העוברת דרך רכיבי הגבול - נתבים, חומות אש, ממשקים מאובטחים, מגשרים, שרתי פרוקסי, מצפינים, וכו'. עקרונות יישום ההגנה יכללו טיפול בתחומים – א. גבולות הרשת/הסגמנטים מוגדרים, נקודות החיבור החוצה מוגדרות. ב. כל נקודות החיבור יקושרו ע"י רכיב גבול המותאם לביצוע משימת ההגנה. ג. כברירת מחדל חיבורים ייחסמו ורק חיבורים מורשים יאופשרו. ד. רכיב הגבול ינטר את תעבורת הנתונים, יעביר את הנתונים ליעד המתאים, ויגביל מעבר תעבורה לא רצוייה. ה. תנועה חשודה תפיק התרעות – רכיב הגבול יפיק לוג פעילות, לרבות תיעוד הפעילות אשר זוהתה כלא רצוייה, וזו תועבר למערכות איסוף וניתוח אבטחתיות SIEM/SOC. ו. רכיבי הגבול מוקשחים ע"פ הוראות יצרנים ו- Best Practices. CMMCv2; SC.L1-3.13.1 – Boundary Protection
2.13.2	**תכנון אפקטיבי של אמצעי ההגנה** הארגון יטמיע את האמצעים ומערכות ההגנה הארגוניות רק לאחר שפעל בעזרת מומחי תוכן ייעודיים, לתכנן, לנתח, לפתח, ולהציב את רכיבי ההגנה, בארכיטקטורות ובתצורות המיטביות ביותר המתועדות בעקרונות מקצועיים להנדסת הגנה, זאת כדי להשיג התאמה, אמינות ויעילות מקסימלית. עקרונות התכנון יכללו טיפול בתחומים – א. תכנון הנדסי מקדים בפרויקטים להקמת מערכות חדשות או שדרוג בהיקף גדול. ב. דרישות ההגנה יוטמעו בכל שלבי מחזור החיים של פיתוח מערכות. ג. שילוב העקרונות המופיעים בפרסומי היצרנים וב- Best Practices בתכנון וביישום. ד. הוקם נוהל ואומצו שיטות לפיתוח תוכנה מאובטח בהם הוכשרו המפתחים. CMMCv2; SC.L2-3.13.2 – Security Engineering
2.13.3	**ערוץ נפרד לניהול מערכות** הארגון יפריד בין הפונקציואליות המיועדת עבור משתמשים לבין הפונקציונאליות הנדרשת עבור מנהלי מערכות ארגוניות, עבורם יוגדר ערוץ ניהול מערכות נפרד אשר לא יהיה נגיש/זמין למשתמשים הרגילים. עקרונות ההפרדה יכללו טיפול בתחומים – א. משתמשים כלליים לא יורשו לבצע פונקציות ניהול מערכת. מנהלי המערכת יורשו לבצע פונקציות ניהול מערכת באמצעות חשבונות מועדפים/חזקים.

	ב. הפרדה חזקה של ערוץ הניהול באמצעים פיזיים או לוגיים – כדוגמת מחשבים נפרדים, כתובות IP שונות, ערוץ Out of Band, סביבות ווירטואליות שונות, הפרדה רשתית VLANs. ג. יישום הקשחה נוספת (מעל משתמש רגיל) בבקרת הגישה או בשיטת הזיהוי והאימות. CMMCv2; SC.L2-3.13.3 – Role Separation
2.13.4	**הפרדת משאבים משותפים** הארגון ימנע מצב בו ניתן יהיה להעביר מידע בצורה לא מורשית או לא מכוונת באמצעות שימוש במשאבי מערכת משותפים. משאבי מערכות משותפים יכללו לדוגמא – מאגר נתונים/קבצים שטוח ללא מידור והרשאות, הקצאת תיקיות אחסון משותפות, הרשאות שלא טויבו במעבר משתמשים בין תפקידים, שימוש חוזר בדיסקים או אמצעי זיכרון שלא נמחקו, מידע שיורי העובר בין משאבי מערכת וזיכרון המשותפים בין יישומים. CMMCv2; SC.L2-3.13.4 – Shared Resource Control
2.13.5	**הפרדת מערכות בעלות גישה ציבורית** הארגון יפריד בין המערכות הנגישות לציבור או מכילות גישה ישירה מן האינטרנט לבין הרשתות הפנימיות הנדרשות בהגנה, באמצעות סגמנטציה רשתית, פיזית או לוגית, המיושמת באמצעות מערכת הגנה ייעודית לזה (לדוגמא, חומת אש). עקרונות יישום ההגנה יכללו – א. אין למקם מערכות פנימיות באותה הרשת עם המערכות הנגישות לציבור. ב. מערכות ארגוניות הנדרשות לכלול נגישות ציבורית ישירה (לדוגמא אתר האינטרנט של הארגון) יורכבו על גבי רשתות מבודלות, DMZ, או יאורחו אצל ספקי שירותי ענן. ג. יש לחסום גישה תקשורתית כברירת מחדל בין סגמנט הרשת המופרד לבין המערכות הפנימיות. ד. חומרים הנדרשים בהעברה פנימה או החוצה בין הרשת הפנימית לבין המערכות הנגישות לציבור, יועברו סלקטיבית בתהליכים מבוקרים באמצעות מנגנוני הגנה אסינכרוניים או ממשקים אוטומטיים מאובטחים. CMMCv2; SC.L1-3.13.5 – Public-Access System Separation
2.13.6	**דחיית תעבורת רשת כמצב ברירת המחדל להתקנים** הארגון יישם עיקרון תעבורת רשת בכל הגבולות וממשקי הרשת על פיו – ברירת המחדל להעברת תקשורת נכנסת ויוצאת מן הרשת תהיה חסימה מלאה, כאשר תקשורת רצוייה תתאפשר להעברה באופן סלקטיבי, על בסיס מדיניות התקשורת, תוך הגדרת חוקת הממשק לאפשר את מעבר הנתונים בצורה המצומצמת ביותר האפשרית. עקרונות יישום ההגנה יכללו –

	א.ברירת המחדל היא שלילת הכל, מכאן, ההיתרים שינתנו הם התוספת/החריג. ב. צמצום תעבורת הנתונים המורשית למינימום האפשרי. ג. סקירת חוקת הממשקים באופן תדיר כדי לוודא שלא בוצעו בה שינויים. CMMCv2; SC.L2-3.13.6 – Network Communication By Exception
2.13.7	**מנע מינהור מפוצל** הארגון ימנע חיבור של התקן לרשת הארגונית במצב בו מינהור (Tunneling) מפוצל הופעל – מצב בו התקנים המתחברים לרשת הארגונית מרחוק (למשל מחשבים ניידים או טלפונים סלולארים) מכילים בו זמנית חיבור לרשת הפנימית, ובמקביל מכילים גם חיבור לאינטרנט, חיבור המנותב שלא דרך תשתיות הארגון. CMMCv2; SC.L2-3.13.7 – Split Tunneling
2.13.8	**הצפנת נתונים בתעבורה** הארגון יטמיע מנגנונים להצפנת תעבורת רשת לטובת ההגנה על הסודיות של מידע ביטחוני בזמן העברתו בין המקור אל היעד, במיוחד על גבי תשתיות האינטרנט. וודא כי מודל המימוש להצפנה (מוצר החומרה/תוכנה) הינו מאושר לשימוש להגנה על מידע ביטחוני או בעל תאימות מול תקן FIPS 140-1 / 2. CMMCv2; SC.L2-3.13.8 – Data In Transit
2.13.9	**ניתוק חיבורים לאחר פרק זמן** הארגון יבטיח כי החיבורים/התקשרויות (Sessions) המורשים אשר בוצעו בין התקנים ברשת, לא ישארו פתוחים ופעילים לזמן בלתי מוגבל, אלא יופסקו וינותקו, יבוטלו הקצאות יישויות הרשת שניתנו לחיבור, וזאת לאחר פרק זמן מוגדר של חוסר בפעילות, סיום המשימה לטובתה בוצע החיבור, או הגעה לגבול זמן חיבור המאקסימאלי. CMMCv2; SC.L2-3.13.9 – Connection Termination
2.13.10	**אבטחת מפתחות הצפנה** הארגון יבטיח את ההגנה על מפתחות ההצפנה, למן הרגע בו הם נוצרו, בזמן העברתם למערכת היעד, ובזמן השימוש בהם, כך שימנע מן המפתחות להיות משוכפלים על ידי גורמים לא מורשים, להיגנב או לאבוד. עקרונות יישום ההגנה יכללו – א. אבטחת סביבת יצירת המפתחות. ב. שימוש במנגנוני ייצור מפתחות נפרדים, רנדומאליים, עם הרכבת מקדם Salting אקראי. ג. כל מפתח ישא תאריך סופי לשימוש, כאשר לאחר מכן יבוטל. ד. הגנה על המפתחות כאשר הם מופצים.

	ה. הגנה על המפתחות בזמן אחסנתם. ו. השמדה/מחיקה חזקה של מפתחות פגי תוקף או שבוטלו. ז. הגבלת הגישה לניהול המפתחות למורשים בלבד. ח. קיימת בארגון מדיניות ונוהל לניהול מפתחות הצפנה. CMMCv2; SC.L2-3.13.10 – Key Management
2.13.11	**סטנדרט ההצפנה להגנה על מידע ביטחוני** הארגון יבטיח כי כל שימוש במוצרים, התקנים, אמצעים, או מנגנונים המשלבים תכונות הצפנה, יצירת גיבוב (Hash) או מספרים אקראיים, בכל המקרים בהם אלו נדרשים ליישום לטובת ההגנה על מידע ביטחוני, אזי יבוצע שימוש בקריפטוגרפיה בעלת תאימות מול תקן FIPS 140-1 / 2, לרבות המודלים (חומרה/תוכנה) המממשים אותה. CMMCv2; SC.L2-3.13.11 – CUI Encryption
2.13.12	**מניעת הפעלה לא מבוקרת של מיחשוב שיתופי** הארגון יבטיח כי התקנים ומערכות ארגוניות אשר הועמדו לשימוש משותף של משתמשים בסביבות העבודה (למשל – מערכות מולטימדיה, וועידות וידאו (VC), מערכות הקלטה, שירותי לוח White Boards בענן, מצלמות ומיקרופונים, ועוד), אלו יבוקרו באופן שימנע שימוש לרעה בתכונות השיתופיות הקיימות במכשירים אלו. עקרונות יישום ההגנה יכללו – א. התקני המחשוב השיתופיים העומדים לשימוש המשתמשים בארגון יהיו מזוהים. ב. התקני המחשב השיתופיים לא יפעלו ללא מעורבות משתמש או ללא הסכמת משתמש. ג. התקני המחשוב השיתופיים יציגו אינדיקציה ברורה לכך שהינם נמצאים בשימוש, כאשר האינדיקציה תהיה בהירה לנמצאים בסביבת העבודה/הפעולה של ההתקן (למשל, נורית חיווי, הקפצת חלון הודעה, נעילת כניסות, צליל שמע). ד. אין לאפשר השתלטות מרחוק לצורך הפעלת התקני מיחשוב שיתופיים בסביבות העבודה של משתמשים, לרבות פתיחת מצלמות ומיקרופונים. CMMCv2; SC.L2-3.13.12 – Collaborative Device Control
2.13.13	**מניעת הרצת קוד מחשב נייד** הארגון יבטיח את הבקרה והשליטה על ריצת קוד מחשב נייד (למשל סריפטים, קוד מאקרו, ActiveX, Applets) על גבי התקנים ממוחשבים או על גבי סביבות יישומים הארגוניים (למשל דפדפן, תוכנות אופיס), קוד נייד אשר מקורו מחוץ לארגון, זאת בכדי לוודא כי השימוש בו מתיישב עם המדיניות התקפה – חסימה של קוד לא מורשה, הגבלת הרצה על התקנים/יישומים, יישום סינון תוכן על פי סוג ומקור.

	עקרונות יישום ההגנה יכללו – א. הרצת קוד נייד מורשה הכולל חתימה דיגיטאלית בלבד. ב. זיהוי וסינון לרכיבי קוד נייד מורשים במערכות התקני הגבול – למשל חומות אש ו- White List. ג. אכיפת תצורה למניעת הרצת קוד נייד ביישומים (למשל, מניעת הרצת JavaScript בדפדפן, מניעת הרצת VBScript במוצרי אופיס). ד. אכיפת תצורה למניעת התקנה של קוד נייד בהתקנים – מחשבים, ניידים, טלפונים חכמים. CMMCv2; SC.L2-3.13.13 – Mobile Code
2.13.14	**אבטחת תקשורת טלפוניה VoIP** הארגון יבטיח את הבקרה והשליטה על השימוש במוצרים והתקנים המממשים טכנולוגיות טלפוניה רשתית – Voice over Internet Protocol (VoIP), כדי לצמצם את התרחישים העויינים האופייניים לשימוש בתשתית זו. עקרונות יישום ההגנה יכללו – א. ניטור ותיעוד פעילות חיבור התקנים (טלפונים), ופעילות משתמשים (רישום שיחות, שלוחות, יעדים, מועדים). ב. הפעלת תכונות הצפנת תעבורת השיחות. ג. הפרדת סגמנט רשת הטלפוניה מרשת הנתונים. ד. זיהוי חיבורי התקנים (טלפונים) מתוך רשימה White-List. ה. הפעלת תכונות שיחה מזוהה, אבחנה בין שיחה פנימית לחיצונית. ו. הפעלת דרישה לסיסמאות בתיבות קוליות. ז. ניהול מרכזיית הטלפון ע"י מורשים בלבד, באימות רב-גורמי. ח. שימוש בציוד קצה אשר הוקשח למניעת האפשרות לפתיחת ערוץ המיקרופון לציטוט שקט (בהפעלת פקודות בערוץ האיתות) ללא הקמת שיחה וללא ידיעת המשתמש. ט. הקשחת ציוד קצה מפני ניהול עדכוני תוכנה/קושחה באופן עצמאי. CMMCv2; SC.L2-3.13.14 – Voice Over Internet Protocol
2.13.15	**הגנה על אוטנטיות ההתקשרויות** הארגון יבטיח את האוטנטיות של הפעלות ההתקשרות (Sessions) כך שיוקמו יחסי אמון בין שתי הקצוות של ערוצי ההתקשרות המבוססים על מנגנוני זיהוי ואימות הכוללים פרוטוקולים אמינים, חסינים, עדכניים, לרבות מוגדרים ומופעלים כהלכה, זאת למניעת התרחשות התקפות מסוג הזרקת מידע כוזב, Man-in-the-Middle או Session Hijacking. CMMCv2; SC.L2-3.13.15 – Communications Authenticity

2.13.16	**אבטחת סודיות המידע הביטחוני במצב מנוחה** הארגון יבטיח את ההגנה על הסודיות של מידע ביטחוני בזמן מנוחה (Data-on-Rest) – קרי, כאשר המידע אינו נמצא בעיבוד, אינו עובר ממקום למקום, אלא ממוקם סטטית על התקן מחשובי בעל יכולת אחסון (כוננים קשיחים, מדיה, זיכרון פלאש, מכשירים ניידים, קלטות גיבוי, וכד'). עקרונות יישום ההגנה יכללו – א. הצפנת המידע. ב. יישום מנגנונים יעילים להגנה על מידע ביטחוני במנוחה בעמדות עבודה של משתמשים. ג. אחסנת המידע על התקן האחסון כאשר הוא במצב לא מקוון, מנותק מן הרשת, או נעול פיזית במקום מאובטח. ד. החמרת הדרישות מול מכשירים ללא יכולת מובנית להצפנת המידע – הוצאה והכנסת המכשיר לארון נעול בסוף יום עבודה, אי האישור להוצאת מכשירים אלו מחצרות הארגון. וודא כי מודל המימוש להצפנה (מוצר החומרה/תוכנה) הינו מאושר לשימוש להגנה על מידע ביטחוני או בעל תאימות מול תקן FIPS 140-1 / 2. CMMCv2; SC.L2-3.13.16 – Data At Rest
פרק 14 – שלמות המידע והמערכות **System and Information Integrity (SI)**	
2.14.1	**תיקון פגמים** הארגון יבטיח כי יזהה, ידווח, ויתקן בזמן פגמים (חשיפת פגיעויות סמויות, הגדרות שגויות, שיבוש רשומות מידע, וכד') אשר אותרו במערכות הארגוניות או במידע. עקרונות יישום ההגנה יכללו – א. גילוי פגמים במהלך תהליכי הערכת הגנה, ניטור רציף, תגובה לאירועים, טיפול בשגיאות מערכת, תיקון תקלות. ב. רכישת תמיכה טכנית רציפה. תהליך לבדיקת הודעות ועדכונים של ספקי המוצרים / יצרנים. ג. תהליך לאיתור ייזום של פגמים כפי שמפורסמים במאגרים פומביים (לדוגמא CVE). ד. תיקון הפגמים תוך פרק זמן מוגדר – על בסיס קריטיות וחומרת הפגיעות הפוטנציאלית. ה. תיקון הפגמים ללא השפעה לרעה – לאחר בחינתם בשדה בדיקות, או בהפצה מוגבלת. ו. תעדוף ביצוע תיקונים בעמדות משתמשי הקצה. CMMCv2; SI.L1-3.14.1 – Flaw Remediation

2.14.2	**יישום כלי הגנה בפני קוד זדוני** הארגון יבטיח את השימוש בתהליכים ובכלים ייעודיים נגד תוכנות זדוניות, המורכבים במיקומים מתאימים במערכות הארגון, כדי לעצור או להפחית את יכולתם לפעול כנגד המידע ומערכות הארגון. רכיבי קוד זדוני מופיעים בתצורות רבות ונקראים בשמות שונים, לרבות וירוסים, תולעים, סוס טרויאני, תוכנות ריגול ומעקב, כופרות, פצצות לוגיות, דלת אחורית, כאשר אלו מועברים באמצעות מגוון אמצעים למשל, דואר אלקטרוני, מדיה נשלפת, אתרי אינטרנט, תוכנה ממקור עוין, ועוד. עקרונות יישום ההגנה יכללו – א. הגדרת מיקומים מתאימים ברשת להצבת אמצעים לטיפול בקוד זדוני. ב. תהליכי רכש מהימנים, הורדת קוד תוכנה ממקור אמין, בדיקות מוניטין. ג. הפעלת הכלים במסגרת סריקות תדירות לאיתור חתימות קוד זדוני בשרתי קבצים, שרתיי יישומים ועמדות עבודה. ד. יכולת לסריקה מתקדמת לאיתור קוד עוין החבוי בקבצים דחוסים, מקודד ומוסתר בקבצים תמימים (סטגנוגרפיה), מקודד כקוד סקריפט. ה. סינון קבצים וקישורים בדואר אלקטרוני נכנס. ו. הגבלת גלישה לאתרים ברמת אמינות נמוכה. ז. הגבלת הורדת קבצים מן האינטרנט. ח. הדרכות ויצירת מודעות אצל המשתמשים. CMMCv2; SI.L1-3.14.2 – Malicious Code Protection
2.14.3	**ערוצי התרעות הגנה וייעוץ** הארגון יחבור ויעקוב אחר ערוצים המפרסמים התרעות ועצות לאבטחת מידע, ינתח את המידע המתקבל, וינקוט פעולות וצעדי תגובה מול הנושאים הרלוונטיים. עקרונות יישום ההגנה יכללו – א. הבטח כי הינך מחזיק במידע העדכני ביותר. ב. חבירה לערוצי התרעות מדינתיים / מגזרים (CERT). ג. חבירה לערוצי התרעות מסחריים והמלצות ליישום כשירות מנויים. ד. זהה והירשם למקורות מידע רלוונטיים לטכנולוגיה ואבטחת מידע. ה. הגדר תהליך לבחינת ההתרעות המתקבלות, שתף, הפץ, ובצע התייעצות לגבי אלו צעדים עליך לנקוט כדי לטפל בהן, זאת עם קבלתם. ו. וודא כי התהליכים מביאים לכדי תיקון פגמים במערכות. CMMCv2; SI.L2-3.14.3 – Security Alerts & Advisors
2.14.4	**עדכניות ההגנה בפני קוד זדוני** הארגון יבטיח את העדכון של מנגנוני ההגנה בפני קוד זדוני כאשר מהדורות חדשות של הכלים, החתימות, ועדכוני תוכנה/קושחה להם זמינים, זאת בכדי לשמור על

	יעילות ההגנה. יש לוודא יישום מנגנונים המבצעים עדכונים אוטומטיים. CMMCv2; SI.L1-3.14.4 – Update Malicious Code Protection
2.14.5	**סריקת מערכות וקבצים** הארגון יבצע סריקות ייזומות תקופתיות, וסריקות בזמן אמת של קבצים המתקבלים ממקורות חיצוניים, כאשר אלו יורדים מן האינטרנט או הדואר אלקטרוני, וכאשר הם נפתחים או מופעלים על ידי המשתמשים, זאת באמצעות הכלים הייעודיים לאיתור חתימות קוד זדוני. עקרונות יישום ההגנה יכללו – א. קביעת התדירות לביצוע סריקות הייזומות, יעדים, התאמת כלים. ב. סריקה תדירה על גבי שרתי קבצים, שרתיי יישומים ועמדות עבודה. ג. סריקות תקופתיות יכללו גם קבצים שנשמרו בעבר מול החתימות העדכניות. ד. סריקות בזמן אמת יופעלו עבור כל קובץ חדש שיורד, נפתח או נשמר. ה. יישום הסריקות יבוצע עבור קבצים המגיעים מכל מקור – מן האינטרנט, דואר אלקטרוני, קבצים ממדיה (USB או CD-ROM/DVD). CMMCv2; SI.L1-3.14.5 – System & File Scanning
2.14.6	**ניטור אינדיקטורים למתקפה** הארגון יבצע מעקב אחר המערכות הארגוניות, לרבות אחר תעבורת התקשורת הנכנסת ויוצאת, זאת בכדי לזהות התקפות פעילות או אינדיקטורים להתקפות פוטנציאליות. עקרונות יישום ההגנה יכללו – א. איתור הנקודות האפקטיביות ביותר ברשת לביצוע הניטור. ב. ניטור מתמשך ורציף. הקלטת פעילויות בזמן אמת. ג. שמירת רשומות הניטור לזמן ארוך לטובת ניתוח וחקירות. ד. המודלים יפעלו ברמת האירועים, דפוסי הפעילות, קשרים בינהם, התייחסות לציר הזמן, ניתוח סיבה ותוצאה, פעילות חריגה. ה. איתור אינדיקטורים של תקיפה (IOCs & TTPs). CMMCv2; SI.L2-3.14.6 – Monitor Communications for Attacks
2.14.7	**זיהוי שימושים לא מורשים** הארגון יזהה שימוש שאינו מורשה במערכות הארגוניות, זאת כחלק מפעילות הניטור השוטפת. שימוש לא מורשה יזוהה ככזה אם הוגדר כך במערכות השונות, או בשיטה הפוכה, שימוש לא מורשה יזוהה ככל חריגה מהגדרת השימוש המורשה.

	CMMCv2; SI.L2-3.14.7 – Identify Unauthorized Use

***

7 ניקוד וציון ההתאמה הכללי

פרק זה מתאר את אופן החישוב של מערכת הניקוד של התקן. חישוב הניקוד ברמת דרישת התקן יתבצע אחרי שכל הראיות בהיקף המבדק נאספו, נבדקו, אומתו, דורגו ונדונו מול צוות התאימות של הארגון. הבודק המוסמך ירשום המלצתו הסופית וייחשב בשלב זה את ניקוד הסעיף, ולאחר מכן את ניקוד ההתאמה כולה.

7.1 אופן חישוב הניקוד מול סעיף דרישה

הבודק יחשב את מידת ההתאמה (על בסיס מבדק התאימות של המענים מול הדרישה) עבור כל סעיף דרישה באופן פרטני. מידת ההתאמה תהיה בערך של אחוזים מתוך שלם אחד, כך שערך 0% יציג אי התאמה, וערך 100% יציג התאמה מלאה. עקרונות החישוב של אופן ההתאמה של המענים מול הדרישה מופיעים בפרק ביצוע התאימות.

רמת ההתאמה עבור כל דרישה פרטנית תוגדר כאחת מן ההגדרות הבאות: התאמה מלאה, התאמה חלקית (כולל את מידת חלקיות ההתאמה המחושבת בערך של אחוז מן השלם), ללא התאמה, או התאמה לא רלוונטית.

אופן החישוב על פי רמת ההתאמה מוגדר בטבלה להלן –

רמת ההתאמה	**אופן החישוב**	**דוגמא לחישוב**
התאמה מלאה **MET**	ערך הניקוד של הסעיף יהיה הערך המלא המופיע בעמודה "ניקוד", כתוספת.	לדוגמא, עבור סעיף בעל ערך הניקוד לדרישה שהוא 3, הניקוד לסעיף יהיה **<u>3+</u>**.
ללא התאמה **NOT MET**	ערך הניקוד של הסעיף יחושב על פי הערך המופיע בעמודה "ניקוד" בערך <u>מינוס</u>, כלומר יחושב כהפחתה.	לדוגמא, עבור "ללא התאמה" כאשר ערך הניקוד לדרישה הוא 1, הניקוד לסעיף יהיה **<u>1-</u>** (הפחתת ניקוד).
התאמה חלקית **PARTIAL MET**	להלן נוסחת החישוב: - פרמטר S יהיה ערך הניקוד הסעיף בטבלה. - פרמטר ה- % יהיה רמת ההתאמה באחוזים. **ניקוד** = $S-((S \times 2)-(S \times 2) \times 0.\%)$	<u>דוגמא 1</u>: עבור התאמה חלקית של 80%, כאשר ערך הניקוד לדרישה הוא 5, הניקוד לסעיף יהיה **<u>3</u>**. להלן הצגת החישוב: $5-((5x2)-(5x2)x0.80)=\mathbf{3}$ <u>דוגמא 2</u>: עבור התאמה חלקית של 50%, כאשר ערך הניקוד לדרישה הוא 3, הניקוד לסעיף יהיה **<u>0</u>**. אופן החישוב יהיה: טווח הניקוד הוא 10 נקודות. להלן הצגת החישוב:

		3-((3x2)-(3x2)x0.50)=0
התאמה לא רלוונטית **NOT APPLICABLE**	יש להוריד את ערך ההפחתה לסעיף לא רלוונטי מסך ציון ההתאמה הכללי. ראה טבלה בפרק הניקוד.	למשל, אם ערך ההפחתה לציון לא רלוונטי הינו 1, וסך ציון ההתאמה הכללי הוא 110, אזי יש להוריד את הערך מסך ההתאמה הכללי, ונקבל – ציון התאמה כללי חדש של **109**.

שים לב כי ערכי הניקוד להוספה וערכי הניקוד להפחתה בסעיפים בהם הם מופיעים, נועדו לשקלל מעלה את חשיבות הדרישה, וכך כאשר ישנה עמידה מלאה בדרישה הציון יעלה מעבר לרגיל, ובהתאם כאשר אין עמידה מלאה, הציון יופחת מעבר לרגיל.

7.2 חישוב ציון ההתאמה הכללי

הבודק יחשב את ציון ההתאמה הכללי של תכולת בדיקת התאימות, זאת על ידי סיכום סך כל הנקודות המצטברות, לאחר חישוב התוספות, חישוב ההפחתות, חישוב חלקיות הניקוד, והפחתת הערכים לסעיפים לא רלוונטיים, ובהמשך, יחשב את הציון ההתאמה הכללי.

ציון ההתאמה הכללי יהיה בערך של אחוזים.

להלן אופן חישוב ציון ההתאמה הכללי –

א. סכם את סך כל הניקוד שנצבר עבור כל דרישה.

ב. חשב מחדש את "ערך ציון הבסיס" – עבור כל דרישה לגביה הוגדר מצב "לא רלוונטי" יש להפחית את ערך הפחתה לסעיף "לא רלוונטי" כפי שמופיע בטבלת ציוני הבסיס.

לדוגמא, אם "ערך ציון הבסיס" הינו 110, ויש לך 5 דרישות המוגדרות במצב "לא רלוונטי" אזי יש להפחית 5 נקודות (5 x 1) מ- 110, ולהגיע ל"ערך ציון הבסיס" חדש של 105.

ג. חשב את ציון ההתאמה באחוזים – יחס סך הניקוד שנצבר מתוך "ערך ציון הבסיס" שחושב. יש לבצע עיגול שבר עשרוני למספר שלם (מעל 0.5 עיגול מעלה, ומתחת לזה עיגול מטה).

לדוגמא, אם צברנו 80 נקודות, ו- "ערך ציון הבסיס" הינו 110, אזי יש לחשב:

אחוז ההתאמה הכללי: <u>**73%**</u> = 100 x (80 / 110).

שים לב כי הערך המחושב באחוזים יכול לעלות על 100%.

7.3 טבלת ניקוד

א. להלן טבלת ציוני הבסיס להתאמה הכללית –

ערך ציון הבסיס הכללי להתאמה	**110**

ערך הפחתה לסעיף "לא רלוונטי"	1

ב. להלן טבלת דרישות התקן והניקוד הרלוונטי עבור כל סעיף –

מס'	כותרת סעיף	ניקוד לסעיף
2.1.1	גישה מורשית ומזוהה	5
2.1.2	בקרת פעילויות ותהליכים	5
2.1.3	בקרת זרימת המידע הביטחוני	1
2.1.4	הפרדת סמכויות ותפקידים	1
2.1.5	מינימום זכויות גישה והרשאות	3
2.1.6	הגבלת השימוש בחשבונות חזקים	1
2.1.7	הבטחת השימוש הנאות בפונקציות מערכת מורשות	1
2.1.8	טיפול בניסיונות גישה לא מוצלחים	1
2.1.9	הסכמת משתמשים ליישום אכיפת אבטחת מידע	1
2.1.10	נעילת התקשרויות	1
2.1.11	ניתוק התקשרויות	1
2.1.12	בקרת ערוצי הגישה מרחוק	5
2.1.13	הצפנת ערוצי הגישה מרחוק	5
2.1.14	ניתוב ערוצי הגישה מרחוק	1
2.1.15	הגבלת הפעלת פקודות מהותיות מרחוק	1
2.1.16	גישה אלחוטית להתקנים מאושרים	5
2.1.17	הגנת גישה אלחוטית	5
2.1.18	חיבור מכשירים ניידים	5
2.1.19	סודיות מידע ביטחוני במנוחה במכשירים ניידים	3
2.1.20	ניהול חיבורים לרשתות ומערכות מידע חיצוניות	1
2.1.21	הגבלת השימוש בהתקני אחסון ניידים	1
2.1.22	מניעת הפרסום של מידע ביטחוני	1
2.2.1	יצירת מודעות לאבטחת מידע	5
2.2.2	הכשרה ואימון	5
2.2.3	מודעות לאיומים פנימיים	1
2.3.1	רישום לוגים במערכות	5
2.3.2	ניטור פעילות משתמשים	3
2.3.3	שמירת לוגים אפקטיבית לאורך זמן	1
2.3.4	התראה על כשל ברישום לוגים	1
2.3.5	ניתוח והצלבת ממצאים	5
2.3.6	העשרת ממצאים ודיווח	1
2.3.7	סנכרון זמן רישום לוגים	1
2.3.8	הגנת רישום הלוגים	1

2.3.9	ניהול מערכות רישום הלוגים	**1**
2.4.1	מיפוי נכסים ומערכות	**5**
2.4.2	אכיפה של תצורות הגנה מיטביות	**5**
2.4.3	מעקב אחרי שינויי תצורה	**1**
2.4.4	ניתוח השפעת השינוי על רמת ההגנה	**1**
2.4.5	הגבלת הגישה לביצוע שינויים	**5**
2.4.6	יישום מינימום פונקציונאליות	**5**
2.4.7	הגבלת פונקציונאליות לא חיונית	**5**
2.4.8	קביעת מדיניות הפעלת יישומים	**5**
2.4.9	בקרה על תוכנות המותקנות על ידי משתמשים	**1**
2.5.1	זיהוי	**5**
2.5.2	אימות	**5**
2.5.3	אימות רב-גורמי	**3 to 5**
2.5.4	אימות עמיד מול הפעלה חוזרת	**1**
2.5.5	אי השימוש החוזר במזהים	**1**
2.5.6	השבתת מזהים/חשבונות בחוסר פעילות	**1**
2.5.7	שימוש בסיסמאות מורכבות	**1**
2.5.8	הגבלת שימוש חוזר בסיסמאות	**1**
2.5.9	הגבלת שימוש בסיסמאות זמניות	**1**
2.5.10	הגנה על סיסמאות באמצעות הצפנה	**5**
2.5.11	ערפול משובי הזדהות משתמשים	**1**
2.6.1	טיפול בתקריות ואירועים	**5**
2.6.2	דיווח על תקריות ואירועים	**5**
2.6.3	בדיקה ותרגול יכולת התגובה לאירועים	**1**
2.7.1	תחזוקה שוטפת	**3**
2.7.2	בקרת התחזוקה	**5**
2.7.3	מחיקת מידע ביטחוני ברכיבים בתחזוקה	**1**
2.7.4	בדיקת מדיה/תוכן חיצוני בכניסה למערכות (הלבנה)	**3**
2.7.5	הזדהות חזקה בערוץ התחזוקה מרחוק	**5**
2.7.6	בקרה לאנשי תחזוקה חיצוניים	**1**
2.8.1	הגנה פיזית על מדיות	**3**
2.8.2	הגבל נגישות פיזית למדיות למורשים בלבד	**3**
2.8.3	סילוק מדיות	**5**
2.8.4	סימון מדיות	**1**
2.8.5	שינוע מדיות	**1**
2.8.6	הצפנת מדיות ניידות	**1**
2.8.7	הגבלת השימוש בהתקני מדיה נתיקים	**5**
2.8.8	בעלים יחיד למדיות נתיקות משותפות	**3**
2.8.9	הגן על גיבויים	**1**
2.9.1	בדיקת התאמה ביטחונית	**3**

2.9.2	ניוד כוח אדם	**5**
2.10.1	מניעת גישה פיזית לנכסים ומערכות ממוחשבות	**5**
2.10.2	ניטור הסביבות המוגנות	**5**
2.10.3	ליווי מבקרים	**1**
2.10.4	תיעוד גישות פיזיות	**1**
2.10.5	ניהול מערכות בקרת הגישה הפיזית	**1**
2.10.6	אבטחת המידע הביטחוני מחוץ לארגון	**1**
2.11.1	הערכת סיכונים עיתית	**3**
2.11.2	סריקת פגיעויות	**5**
2.11.3	תיקון פגיעויות	**1**
2.12.1	בקרת המערכות ואמצעי ההגנה	**5**
2.12.2	פיתוח ויישום תוכניות פעולה לתיקון ליקויים	**3**
2.12.3	ניטור ומדידת בקרות ההגנה	**5**
2.12.4	תוכנית לאבטחת מערכות הארגון	**5**
2.13.1	הגנת גבולות הרשת	**5**
2.13.2	תכנון אפקטיבי של אמצעי ההגנה	**5**
2.13.3	ערוץ ניהול מערכות נפרד	**1**
2.13.4	הפרדת משאבים משותפים	**1**
2.13.5	הפרדת מערכות בעלות נגישות ציבורית	**5**
2.13.6	דחיית תעבורת רשת כמצב ברירת מחדל להתקנים	**5**
2.13.7	מנע מינהור מפוצל	**1**
2.13.8	הצפנת נתונים בתעבורה	**3**
2.13.9	ניתוק חיבורים לאחר פרק זמן	**1**
2.13.10	אבטחת מפתחות הצפנה	**1**
2.13.11	סטנדרט הצפנה להגנה על מידע ביטחוני	**3 to 5**
2.13.12	מניעת הפעלה לא מבוקרת של מיחשוב שיתופי	**1**
2.13.13	מניעת הרצת קוד מחשב נייד	**1**
2.13.14	אבטחת תקשורת טלפוניה VoIP	**1**
2.13.15	הגנה על אוטנטיות ההתקשרויות	**5**
2.13.16	אבטחת סודיות המידע הביטחוני במצב מנוחה	**1**
2.14.1	תיקון פגמים	**5**
2.14.2	יישום כלי הגנה בפני קוד זדוני	**5**
2.14.3	ערוצי התרעות הגנה וייעוץ	**5**
2.14.4	עדכניות הגנה בפני קוד זדוני	**5**
2.14.5	סריקת מערכות וקבצים	**3**
2.14.6	ניטור אינדיקטורים למתקפה	**5**
2.14.7	זיהוי שימושים לא מורשים	**3**
סה"כ 110 סעיפים		

- הערה לסעיף 5.3: חשב 5 נקודות אם כולל את כל סוגי המשתמשים לרבות משתמשים מרוחקים ומשתמשים חזקים, אחרת חשב 3 נקודות.
- הערה לסעיף 13.11: חשב 5 נקודות אם קיימת תאימות לתקן FIPS, אחרת חשב 3 נקודות.

8 הגדרות ומונחים

8.1 טבלת ראשי תיבות בשימוש

להלן טבלת ראשי תיבות בשימוש באנגלית ופרושם –

Abbreviations	Meaning
APT	Advanced Persistent Threat
BOM	Bill of Materials
BYOD	Bring Your Own Device
CISO	Chief Information Security Officer
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CD	Compact Disk
CERT	Computer Emergency Response Team
CNC	Computer Numerical Control
CDR	Content Disarm & Reconstruction
CUI	Controlled Unclassified Information
CDI	Covered Defense Information
CMMC	Cybersecurity Maturity Model Certification
DFARS	Defense Federal Acquisition Regulation Supplement
DoD	Department of Defense (of the United States)
DVD	Digital Video Disk
DVR	Digital Video Recorder
DoK	Disk on Key
FCI	Federal Contract Information
FIPS	Federal Information Processing Standards
FOUO	For Official Use Only
IR	Incident Response
IOC	Indicator of Compromise
ICS	Industrial Control System
IT	Information Technology
IP	Internet Protocol
MSSP	Managed Security Service Provider
MOD	Ministry of Defense (of Israel)
MFA	Multi-Factor Authentication
N/A	Not Applicable
NIST	National Institute of Standards and Technology
NDA	Non-Disclosure Agreement

PT	Penetration Testing
PIN	Personal Identification Number
POA&M	Plan of Actions and Milestones
PLC	Programmable Logic Controller
ROM	Read-Only Memory
RAID	Redundant Array of Independent Disks
RADIUS	Remote Authentication Dial-In User Service
SIEM	Security Information and Event Management
SOC	Security Operational Center
SCADA	Supervisory Control and Data Acquisition
SSP	System Security Plan
TTP	Tactics, Techniques, and Procedures
UTCI	Unclassified Controlled Technical Information
U.S.	United States
USB	Universal Serial Bus
VC	Video Conferencing
VPN	Virtual Private Network
VB	Visual Basic
VoIP	Voice Over Internet Protocol

להלן טבלת ראשי תיבות בשימוש בעברית ופרושם –

מונח	פירוש
דו"ח	דין וחשבון
נאט"ו	NATO - North Atlantic Treaty Organization
צב"ד	ציוד בדיקה
תוה"ג	תורת ההגנה (בסייבר)
תו"ל	תורת לחימה
תקשו"ב	תקשורת, שליטה ובקרה

טבלת תאימות מונחים –

מונח בעברית	מונח באנגלית
בודק מוביל	Lead Assessor
בודק מוסמך	Certified Assessor
הסמכה	Certification
חבר צוות בודקי תאימות	Assessment Team Member
מבדק תאימות	Assessment

ספק/ים	Contractor(s)
תיחום	Scope

***