המשרד להגנת הסביבה

الوزارة لحماية البيئة
Israel Ministry of Environmental Protection

סייבר בתעשייה
המשרד להגנת הסביבה

# מדריך סייבר
## עמידה בתנאים של היתר רעלים בתחום הסייבר בתעשייה

**2022**
גירסא 2.0


המשרד להגנת הסביבה
אגף חירום וסייבר, יחידת הסייבר בתעשייה

# תוכן העניינים

# 1. הקדמה

1.1 ביום 15.02.2015 התקבלה החלטת ממשלה מספר 2443 (להלן: החלטת הממשלה), שכותרתה "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר". החלטה זו התקבלה בהמשך להחלטת ממשלה מספר 3611 מיום 7.08.2011 בנושא "קידום היכולת הלאומית במרחב הקיברנטי".

1.2 באותו מועד (15.02.2015), התקבלה החלטת ממשלה נוספת שמספרה 2444, בעניין "קידום ההיערכות הלאומית להגנת הסייבר", במסגרתה החליטה הממשלה על גיבוש מדיניות כוללת בתחום הגנת הסייבר ועל הקמת רשות לאומית להגנת הסייבר במסגרת מערך הסייבר הלאומי במשרד ראש הממשלה.

1.3 החלטות אלו נועדו לקדם אסדרה לאומית בנושא הגנת הסייבר להעלאת החוסן הלאומי במרחב הסייבר במדינת ישראל.

1.4 בעקבות החלטת הממשלה, הכוונה והנחיה מקצועית בתחום הגנת הסייבר במשק הישראלי, ישתלבו במערך הרגולציה הממשלתי. משמעותה של קביעה זו היא כי הגנה מפני מתקפות סייבר, העלולות לפגוע בסביבה או בבריאות הציבור ובחיי אדם, תתבצע באמצעות כלי הרגולציה (לדוגמה, היתר רעלים שניתן מכוח חוק החומרים המסוכנים).

1.5 כדי לקבוע הוראות בתחום ההגנה מפני מתקפות סייבר העלולות לגרום לפגיעה בסביבה, בבריאות הציבור או בחיי אדם, הוקמה במשרד להגנת הסביבה, באגף חירום וסייבר, יחידת סייבר בתעשייה. היחידה פועלת בהנחיה מקצועית של מערך הסייבר הלאומי.

1.6 יחידת הסייבר בתעשייה עוסקת בהנחיה, בפיקוח ובאכיפה של הגנת הסייבר בעסקים המחזיקים חומרים מסוכנים. תפקיד היחידה להגדיר את המדיניות המגזרית ואת דרישות האסדרה, ולהעניק ליווי מקצועי שוטף ומענה לפניות מקצועיות בהתאם למאפייני העסקים המפוקחים על ידה.

1.7 היחידה פיתחה מתודולוגיה ייחודית המוצגת במדריך זה, לצורך עריכת סקר סיכונים במפעלים המחזיקים בחומרים מסוכנים המקבלים היתר רעלים מהמשרד להגנת הסביבה. המתודולוגיה שפותחה מבוססת על תורת ההגנה של מערך הסייבר הלאומי, תוך התאמתה לתעשיית החומרים המסוכנים. בתהליך פיתוח המתודולוגיה התקיימו התייעצויות עם גורמים מובילים במשק בתחום הסייבר, מערכות הבקרה וחומרים מסוכנים, תוך שיתוף פעולה עם התאחדות התעשיינים לאורך התהליך כולו.

1.8 מסמך זה הוא גרסה 2.0 המהווה גרסה מחייבת. גרסאות קודמות וגרסה זו הובאו להערות הציבור ולאחר בחינה מדוקדקת של הערות אלה, אומצו חלקן בגרסה זו. כמו כן נעשו עדכונים במתודולוגיה בהתאם לתובנות שעלו מסקרי סיכונים שנעשו בעסקים וכן בהתאם להתייעצויות עם החברות השונות במשק אשר פועלות בעסקים המחזיקים חומרים מסוכנים.

1.9 מדריך זה, כולל בתוכו את השינויים הנדרשים לצורך הרחבת הרגולציה בסייבר למפעלים שהוגדרו ברמות A ו-B ע"י המשרד להגנת הסביבה ושאינם מוגדרים כמפעלי SEVESO.

1.10 ההוראות במסמך זה נועדו לסייע ביישום התנאים המותקנים בהיתר הרעלים והן כוללות הוראות לביצוע מיפוי סיכונים, הערכות הסיכונים ויישום ההגנות הנדרשות.

1.11 חרף האמור בהוראות מדריך זה, לממונה על חומרים מסוכנים יש סמכות להורות, באמצעות היתר הרעלים, על הוראות שונות מההוראות הקבועות במסמך זה. התאמות פרטניות או שינויים ייעשו בתיאום עם הממונה על חומרים מסוכנים במחוז, ובתיאום עם אגף חירום וסייבר במשרד להגנת הסביבה.

1.12 במידה ועל עסק יחולו הוראות של ניהול סיכונים משולב (ניהול סיכונים בחומרים מסוכנים, ברעידות אדמה ובסייבר), יחולו הוראות מדריך זה בשינויים המחוייבים מתנאי ניהול הסיכונים המשולב. במידה ועל העסק יחולו הוראות של ניהול סיכוני סייבר בלבד, הפעילות תתבצע על פי מדריך זה בלבד.

**לשאלות בנושא מדריך זה אפשר לפנות בדואר אלקטרוני לכתובת:**
**cyber_industry@sviva.gov.il**


מחבר המסמך
**יוסי שביט**
ראש יחידת הסייבר בתעשייה
המשרד להגנת הסביבה

מאשרת המסמך
**לילך פדלון**
ראש אגף חירום וסייבר
המשרד להגנת הסביבה

# 2. הגדרות

| מונח | הסבר |
|---|---|
| אבטחה פיזית | האמצעים הפיזיים הנדרשים להגנה על ציוד המחשוב, לגישה למידע של העסק ולשרידות המערכות הממוחשבות המכילות את מאגרי המידע והרכיבים הממוחשבים התעשייתיים. |
| איום | מפגע פוטנציאלי אשר עלול לפגוע בתהליך מסוכן/במערכות ממוחשבות של עסק במכוון או באקראי. |
| אירוע חומרים מסוכנים | התרחשות בלתי מבוקרת או תאונה, שמעורב בה חומר מסוכן, הגורמת או העלולה לגרום סיכון לאדם ולסביבה, לרבות שפך, דליפה, פיזור, פיצוץ, התאיידות, דליקה. |
| אירוע חומרים מסוכנים משמעותי | אירוע שגרם או עלול היה לגרום לפגיעה משמעותית באדם או בסביבה. פגיעה לעניין זה: דליפת חומר רעיל, דליק או נפיץ במרחב הציבורי, פיצוץ או דליקה כתוצאה מנוכחות חומר מסוכן או פגיעה בלתי הפיכה בסביבה. |
| אירוע סייבר / אירוע סייבר בתעשייה | התרחשות אשר מעידה על פגיעה אפשרית במערכת מחשוב, עקב פגיעה מכוונת או פגיעה בשוגג ואשר ביכולתה לגרום לאירוע חומרים מסוכנים משמעותי. |
| בקרות | אמצעים אשר על העסק ליישם על מנת להגן על עצמו מפני אירוע סייבר. |
| בקרה מפצה | בקרה שנועדה לפצות על העדר היכולת לממש את הבקרה המומלצת ונותנת מענה הולם לסוגיית הפער הקיים בהגנת הסייבר. |
| דילול הרשאות | שינוי הרשאות על פי כלל מינימום הרשאות לביצוע הפעילות הנדרשת. |
| הזדהות | תהליך המספק זיהוי מאומת של אדם או מחשב, באמצעות מידע ייחודי חד ערכי לאדם או למחשב, רכיב הזדהות פיזי או תכונה שלו. |
| הזדהות חכמה / הזדהות חזקה | שיטת הזדהות המבוססת על שילוב של לפחות שניים ממאפייני האימות שלהלן:<br>משהו שהמשתמש יודע, כגון: סיסמה.<br>משהו שיש למשתמש, כגון: רכיב פיזי כמו טוקן או מחולל סיסמאות חד-פעמי או כרטיס חכם.<br>מאפיין ביולוגי של המשתמש, כגון: טביעת אצבע, טביעת רשתית עין. |
| המערך | מערך הסייבר הלאומי. |

| מונח | הסבר |
|---|---|
| ה-CERT הלאומי | מרכז לסיוע בהתמודדות עם איומי סייבר, הפועל לשיפור החוסן ההגנתי בסייבר, מסייע בטיפול באיומי סייבר ואירועי סייבר, מרכז ומשתף מידע רלוונטי עם כלל הגורמים במשק ומהווה נקודת ממשק מרכזית בין גופי הביטחון לגורמים במשק. |
| הצורך לדעת (Need to know) | עקרון המנחה להעניק הרשאות מינימליות ומדוייקות ככל האפשר לצורך פעילות עסקית נדרשת. |
| התרחיש החמור ביותר (WCS) | התרחיש שבו מתקיים השחרור של הכמות הגדולה ביותר של חומר מסוכן ממיכל או מתקן, או כשל בתהליך שתוצאותיו המרחק הגדול ביותר לנקודת קצה. |
| זמינות המידע (Availability) | וידוא שלמשתמשים המורשים יש גישה למידע ולתהליכים מסוכנים הקשורים בו, לפי הצורך באופן שוטף וללא הפרעות. |
| חישוב רמת סיכון סייבר | חישוב רמת הסיכון בסייבר מבוסס על שקלול של רמת הנזק (I) הצפויה לנוכח הסיכוי שהנזק יתרחש (רמת חשיפה P) לפי הנוסחה להלן:<br>סיכון I*3+P = (הסיכון שווה לרמת החשיפה ועוד 3 פעמים רמת הנזק). |
| מידע | נתון הנוגע ו/או קשור לפעילותן, תפעולן או תפקודן של מערכות מחשוב בעסקים ונמצא על-גבי אמצעי אחסון ממוחשבים, מגנטיים או אלקטרוניים, מצעי מידע פיזיים וכן מידע המועבר בעל-פה. |
| מזהי תקיפה (IOC) | מזהים מסוגים שונים אשר קשורים לתקיפה. לדוגמא: שם קובץ, נתיב לקובץ, פונקצית גיבוב (HASH), כתובת IP, מחרוזת, כתובת מייל, כתובת אתר, וכדומה. |
| ממונה | כפי שמוגדר בחוק חומרים מסוכנים התשנ"ג, 1993. |
| ממונה הגנת סייבר | גורם בעסק אשר יהיה מופקד על מימוש ויישום התנאים הנוספים במסמך זה למזעור סיכוני סייבר בעסק. |
| מעבדת סייבר לאומית | מעבדה לאומית שתפקידה לבדוק ולאשר מוצרים ושירותים בתחום הגנה בסייבר. |

| מונח | הסבר |
|---|---|
| מערכות מחשוב בקרה תעשייתיות, מערכות ממוחשבות ICS - (Industrial Control System) | מונח כללי הכולל מספר סוגים של מערכות בקרה המשמשות בייצור תעשייתי. המערכות יכולות להיות מורכבות מהרכיבים האלה:<br>יחידות חיישנים ויחידות שליטה מקומית:<br>sensors, actuators and electronic devices - IED<br>יחידות בקרים מתוכנתים:<br>(Remote Terminal Unit) - RTU<br>(Programmable Logic Controllers) - PLC<br>תקשורת בין האתרים למרכז הבקרה:<br>WAN (Wide Area Network Communication)<br>מרכז בקרה של כל התהליך:<br>SCADA (Supervisory Control and Data Acquisition)<br>מערכות בקרה מבוזרות:<br>(Distributed Control Systems) - DCS<br>מחשבים לממשק אדם-מכונה:<br>(Human Machine Interface) - HMI |
| מקום רגיש | כהגדרתו בצו סדר הדין הפלילי עבירות קנס - שמירת הניקיון, (תש"ס - 2000); גן לאומי, שמורת טבע, אתר הנצחה, אתר ארכאולוגי, יער, ים, חוף הים, מקור מים כמשמעותו בסעיף 2 לחוק המים, תשי"ט-1959, או מקום המצוי בקרבת מקור מים. |
| משאבי מחשוב | בסיסי נתונים, קבצים, מערכות, תכניות או אמצעים אחרים אשר כניסה אליהם מאפשרת גישה למידע ולמערכות ממוחשבות שברשות העסק. |
| מתקפת סייבר | פעולה התקפית של חדירה למרחב הקיברנטי של היעד המסכנת תהליך הכולל מערכות, תשתיות ושירותים שנתמכים על ידם. |
| משתמש גנרי | משתמש שאינו חד-חד ערכי שבאמצעות שימוש בשמו ובסיסמתו יכולים מספר משתמשים שונים להכנס למערכת. |
| סודיות המידע (Confidentiality) | מידע שבעליו קבע שאין לחשוף אותו לגורמים שלא מאושרים לכך. |
| סיווג | מדד המגדיר את רמת רגישות המידע והמערכות התומכות. |

| מונח | הסבר |
|---|---|
| סייבר, מרחב סייבר, המרחב הקיברנטי או ה- Cyber Space | מרחב מטפורי של מערכות מחשב ורשתות מחשב שנאגרים בהם נתונים אלקטרוניים ומתבצעת תקשורת מקוונת ואינטראקטיבית ללא תלות במיקום הגיאוגרפי של המשתמשים בו. |
| רשת מתח נמוך | רשת תקשורת מבוססת TCP/IP ייעודית שנועדה להגן ולפקח על ביטחון המתקן.<br>המערכת יכולה להיות מורכבת מהרכיבים האלה:<br>● מצלמות אבטחה IP ומצלמות תרמיות (קבועות/PTZ/LPR)<br>● מערכות VMS ואנליטיקה<br>● מערכות גילוי פריצה<br>● מערכות בקרת כניסה<br>● מערכת גדר חכמה<br>● מערכות רדאר<br>● מערכות שו"ב<br>● IIOT (Industrial IOT) |
| תהליך | פעילות תעשייתית הכוללת חומר מסוכן, לרבות אחסון, ערבוב, ייצור וחיבור למערכות מחשוב. |
| תהליך ממוחשב בתעשייה | פעילות תעשייתית הכוללת חומר מסוכן, לרבות אחסון, ערבוב וייצור אשר מנוהלת/מבוקרת באמצעות תהליכים ממוחשבים. |
| תורת ההגנה | תורת ההגנה בסייבר לעסק של מערך הסייבר הלאומי [1] |
| תצורת "ספגטי" | סלילת כבלי מיחשוב בארון התקשורת בצורה לא מסודרת כאשר לא ניתן להבין מהיכן להיכן מתחברים הכבלים, דבר שעלול לגרום לגישור לא מכוון בין רשתות. |
| תקיפת Zero Day | תקיפה חדשה שאינה ידועה לכלי הגנה בסייבר מבוססי חתימות,<br>לדוגמא: תקיפת כופרה. |
| Sand Box | פתרון לתקיפות Zero Day שאינו מבוסס חתימות. |
| NIST CSF | תקן הנגזר מחבילת תקני NIST לטיפול בהגנת סייבר:<br>National Institute of Standards and Technology - Cyber Security Framework |

1 תורת ההגנה בסייבר לעסק של מערך הסייבר הלאומי

# 3. מטרת המסמך

לסייע ולהדריך עסקים שנקבעו להם תנאים נוספים להגנת הסייבר בהיתר הרעלים, בדרכי יישום התנאים ולקבוע שלבי עבודה ליישום רגולציית סייבר לבעל/אחראי היתר רעלים בעסק.

הוראות המסמך נועדו לתת כלים להפחתת היכולת לפגיעה בבריאות הציבור ובסביבה, ולמזער ככל הניתן את רמת הסיכון להתרחשות אירוע סייבר או פגיעה מסוג אחר בתהליכים טכנולוגיים או במערכות ממוחשבות המנהלות/מבקרות חומרים מסוכנים, אשר עלול לגרום לאירוע חומרים מסוכנים.

מסמך זה קובע דרישות והנחיות הנוגעות לביצוע סקר סיכוני סייבר על מערכות ממוחשבות המנהלות/מבקרות חומרים מסוכנים. התהליך מבוסס על עקרונות תורת ההגנה של מערך הסייבר הלאומי (גרסה 2.0), המסתמך במידה רבה על התקן האמריקני NIST CSF[2], בעניין אבטחה של מערכות בקרה ממוחשבות בתעשייה, תוך התאמתו לעולם התעשייתי בכלל ועולם תעשיית החומרים המסוכנים בפרט.

יודגש כי במקרה של סתירה או אי-התאמה בין הוראות אלה למסמכים אחרים, לרבות תורת ההגנה של מערך הסייבר הלאומי והתקן האמריקני NIST CSF, הוראות מסמך זה גוברות.

# 4. רקע - הגנת סייבר בתחום חומרים מסוכנים

4.1 כשל במערכות ממוחשבות המבקרות/מנהלות ייצור, שינוע, אחסון של חומרים מסוכנים בעקבות אירוע סייבר, עלול לגרום לאירוע חומרים מסוכנים, ובעקבותיו לפגיעה בבריאות הציבור ובסביבה.

4.2 להלן מספר דוגמאות לאירועי חומרים מסוכנים שעלולים להתרחש עקב אירוע סייבר:

- פליטת גזים המסכנים את הציבור.
- פיצוץ חומרים מסוכנים.
- דלקת חומרים מסוכנים בשלושה מצבי הצבירה.
- שפך של חומר מסוכן נוזל ללא שריפה.
- פיזור של חומרים מסוכנים, מוצקים ללא שריפה.
- שפך תעשייה למקור מים זורם / למערכת ניקוז.
- שפך תעשייה לשטח פתוח.
- שפך תעשייה למערכת הביוב (מאגרי מים/קולחין).

4.3 שיתוף מידע בין ארגונים ודיווח על אירועים ליחידת הסייבר בתעשייה במשרד להגנת הסביבה, ובכלל זה ל- CERT הלאומי, יסייעו לגילוי מוקדם של התרחשות פוטנציאלית של אירוע סייבר. בכל אחד מהשלבים המוקדמים יוכל בעל היתר הרעלים לזהות את פוטנציאל התקיפה ולמזער את הסיכון לגרימת נזק פוטנציאלי.

4.4 לאחר סיום אירוע סייבר יכין העסק דו"ח אירוע סייבר לפי נספח ט' במדריך זה. נגרם אירוע חומרים מסוכנים בעקבות אירוע סייבר, ייכלל הדיווח והתחקור במסגרת תחקיר האירוע כמשמעותו בתנאים הכלליים בהיתר הרעלים.

2 https://www.nist.gov/cyberframework

# 5. הסבר התהליך

## 5.1 שלבים מקדימים

### 5.1.1 כתב מינוי ממונה הגנת סייבר

5.1.1.1 בעל היתר רעלים ימנה תוך 60 יום מיום קבלת תנאי סייבר בהיתר הרעלים, גורם מטעמו שיהיה מופקד על מימוש ויישום תנאים נוספים אלה למזעור סיכוני סייבר, ויעביר את נספח ה' ("כתב מינוי ממונה הגנת סייבר בעסק") לממונה במחוז. גורם זה יקרא "ממונה הגנת סייבר" (להלן: "ממונה ההגנה"). בהתאם להחלטה של בעל היתר הרעלים, ממונה ההגנה יעשה את תפקידו במקביל לתפקידו העיקרי, או ימונה בעל תפקיד ייעודי.

5.1.1.2 תפקיד ממונה ההגנה יהא לשמש כאיש הקשר מול יחידת הסייבר בתעשייה במשרד להגנת הסביבה, בכל הקשור לפעילות הנחיית סייבר בעסק.

5.1.1.3 בעל היתר הרעלים ימנה ממלא מקום לממונה ההגנה בזמן היעדרו.

### 5.1.2 מסמך מדיניות

5.1.2.1 העסק יגבש מסמך מדיניות אבטחת מידע והגנת סייבר אשר יגדיר את יעדי האבטחה, תהליכים ניהוליים, אמצעים למימוש, עקרונות ליישום האבטחה, מחויבות הנהלת העסק לתהליך העלאת חוסן העסק בסייבר, כולל הקצאת ותקצוב משאבים וקביעת נהלי עבודה, לרבות נוהל לניהול אירועי סייבר. העסק יציג את מסמך המדיניות לממונה לפי דרישתו.

## 5.2 שלבי התהליך

### 5.2.1 מיפוי

5.2.1.1 **מיפוי החומרים המסוכנים המנוהלים / מבוקרים ע"י מערכות ממוחשבות** - העסק ימפה את החומרים המסוכנים המופיעים בהיתר הרעלים המנוהלים / מבוקרים ע"י מערכות ממוחשבות על גבי נספח ו' למדריך זה ("טופס מיפוי ראשוני של חומר מסוכן המנוהל/מבוקר ע"י מערכת ממוחשבת").

### 5.2.2 עריכת סקר סיכונים והטמעת בקרות

5.2.2.1 **עריכת סקר סיכוני סייבר** - חישוב רמת הסיכון בסייבר המתקבלת משכלול רמת החשיפה ורמת הנזק בהתאם להנחיות מדריך זה. בהתאם לתוצאת סקר הסיכונים, תקבע חבילת הבקרות הנדרשת ליישום.

5.2.2.2 **ביצוע אנליזת פערים (Gap Analysis)** - העסק יערוך השוואה בין הבקרות הקיימות בעסק, לבקרות שעליו ליישם כפי שהתקבלו משלב סקר הסיכונים.

5.2.2.3 **בניית תכנית עבודה** - העסק יבנה תכנית עבודה לסגירת הפערים.

5.2.2.4 **יישום הבקרות לפי תכנית העבודה** - העסק יישם את הבקרות הנדרשות ממסקנות הסקר ובהתאם לתכנית העבודה. אם מסיבה כלשהי לא ניתן ליישם את הבקרות כפי שהן כתובות ברשימת הבקרות, ניתן לבחור בקרות מפצות אשר יתנו מענה לפער, בהתייעצות עם יחידת הסייבר בתעשייה של המשרד להגנת הסביבה.

5.2.2.5 **פיקוח ומעקב שוטפים** - העסק יעקוב ויפקח באופן שוטף על כל שלבי התהליך כפי שתוארו בסעיף זה.

## 5.3 סכמת התהליך


## 5.4 לו"ז ליישום ההנחיות

5.4.1 מיד עם החלת תנאי סייבר בהיתר הרעלים: שלבים 1 עד 3 (כולל שלב 3) - 12 חודשים. לאחר תום פרק זמן זה יבוצע פיקוח מדגמי ע"י הממונה.

5.4.2 מיד בסיום 3 השלבים הראשונים, תחילת ביצוע שלבים 4 עד 6 (כולל שלב 6) - 24 חודשים סה"כ כל התהליך הכולל מיפוי, סקר סיכונים ויישום הבקרות הנדרשות - 36 חודשים.

5.4.3 לאחר יישום הבקרות, תנתן הפוגה של 6 חודשים לצורך השלמות נדרשות ככל שתדרשנה.

5.4.4 תהליך העבודה הינו תהליך מחזורי המתחדש מדי 42 חודשים מיום תחילת התהליך.

## 5.5 חידוש תהליך העבודה

חידוש תהליך העבודה יבוצע באחד מהמקרים שלהלן:

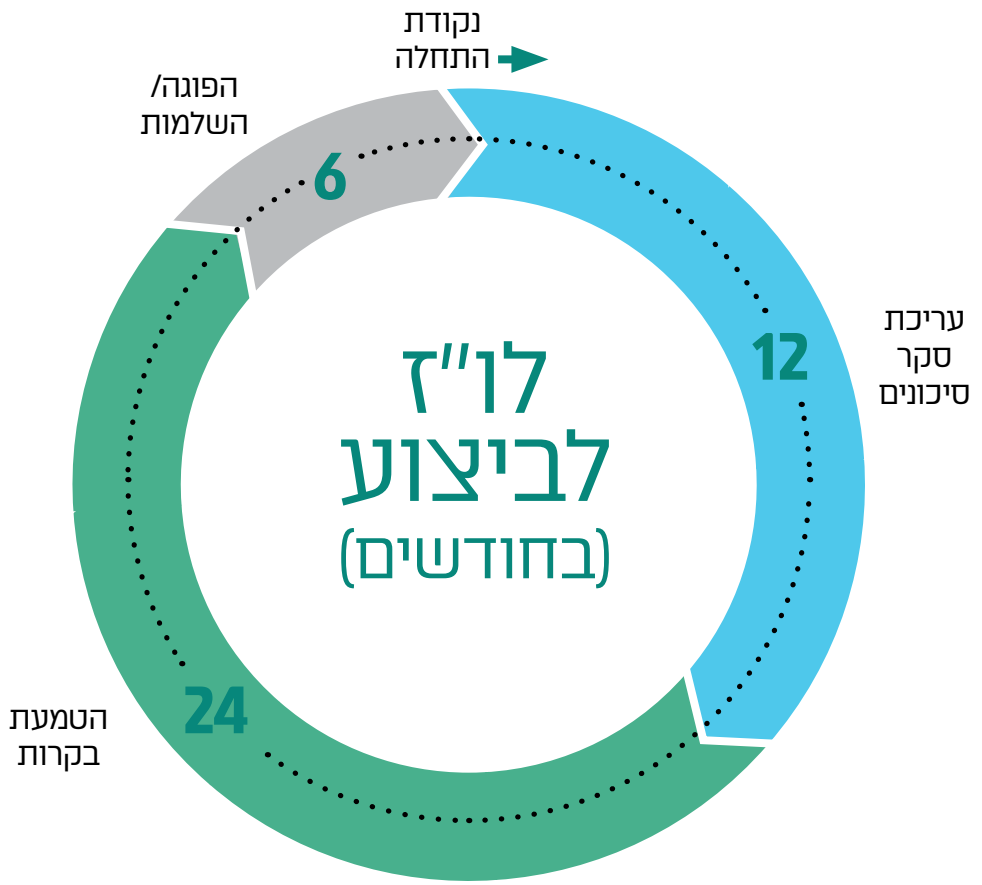
5.5.1 אחת ל- 42 חודשים (3.5 שנים): לאחר השלמת התהליך ותקופת ההשלמות שאורכם 42 חודשים, מתחיל מחזור נוסף.

5.5.2 לאחר הוספת מערכת ממוחשבת חדשה המנהלת/מבקרת חומרים מסוכנים.

5.5.3 לאחר הוספת חומר מסוכן חדש.

5.5.4 לאחר ביצוע שינוי במערכת ממוחשבת קיימת המנהלת/מבקרת חומרים מסוכנים: הוספה, הסרה או שינוי של רכיבי מחשוב למערכת מחשוב קיימת המטפלת בחומרים מסוכנים.

## 5.6 תרשים לו"ז לביצוע:



## 6. תכנון עבודה

6.1 פעילות ההגנה בסייבר אמורה להיות חלק בלתי נפרד מהתרבות הארגונית של העסק, ומבוססת על המחויבות של בעל היתר הרעלים ושל הנהלת העסק ליישם דרישות מסמך זה.

6.2 השלב החשוב בביצוע הוראות מסמך זה הוא תכנון מוקפד של תוכנית העבודה על כל שלביה, בצד הקצאת המשאבים הנדרשים ליישומה ובהתאם ללוחות הזמנים שנקבעו.

## 7. תוצרים נדרשים

7.1 בסיום הסקר יש למלא ולהעביר לממונה את נספח ז' שבמדריך זה, הכולל תצהיר בעל היתר הרעלים אודות ביצוע הערכת סיכוני סייבר בעסק, וטבלה המכילה את שם המערכת, נתוני רמת החשיפה ורמת הנזק כפי שהתקבלו, חישוב רמת הסיכון וחבילת הבקרות שהתקבלה לצורך יישומה על פי מפת חום.

7.2 לאחר ביצוע הסקר תבוצע אנליזת פערים בכתב. מסמך זה ישמר במפעל ואין צורך להגישו לממונה אלא על פי דרישה.

7.3 לאחר ביצוע אנליזת פערים תכתב תכנית עבודה להטמעת הבקרות - תכנית זו תשמר במפעל ואין צורך להגישה לממונה אלא על פי דרישה.

7.4 עם סיום יישום התוכנית והטמעת הבקרות, יש למלא ולהעביר לממונה את התצהיר שבנספח ח' שבמדריך זה, הכולל טבלה המכילה את שם כל אחת מהמערכות שמופו, חבילת הבקרות שהוקצתה לסיכון שהתקבל, רשימת הבקרות שהוטמעו והערות.

# 8. הערכת סיכוני הסייבר

8.1 הערכת סיכוני הסייבר במדריך זה מתייחסת לכל הפעילות ברשת ה- OT (Operation Technology) המכילה את רצפת הייצור שבה פועלות המערכות הממוחשבות המנהלות/מבקרות חומרים מסוכנים.

חשוב לציין כי סיכונים הנובעים מפגיעה במערכות המידע הממוחשבות של המפעל שאינן ברצפת הייצור, ובכללן מערכות ה- IT (Information Technology), כגון מערכות דואר אלקטרוני, גישה לאינטרנט, מידע רגיש עסקית, מידע בסיווג גבוה וכדומה - אינם מטופלים במסגרת הרגולציה בסייבר של המשרד להגנת הסביבה כפי שמפורטת במדריך זה, אולם יש להתייחס אליהם כווקטור תקיפה לרשת ה-OT המכילה בתוכה את מערכות המחשוב המנהלות / מבקרות חומרים מסוכנים.

8.2 במסגרת הערכת סיכוני סייבר יש להתייחס גם לפגיעה במערכות בטיחות, במערכות ההגנה ובמערכות התומכות הנמצאות ברצפת הייצור, לדוגמה: תקיפת סייבר על מערכות בטיחות של בקרים, תקיפת סייבר על גלאים, על מערכות צילום וכדומה.

8.3 יש להתייחס לחשיפת מידע על התהליך הממוחשב המטפל בחומרים מסוכנים ובכלל זה ארכיטקטורת המערכת ומערכי ההגנה שלה: מידע על סוג הבקרים, הדגם, גרסת קושחה, גרסת תוכנה וכדומה.

8.4 יש להתייחס לפגיעה באמינות המערכת - פגיעה בתפקוד תקין של מכשיר או מערכת בהתאם למפרט שלהם ובהתאם לתהליך התכנון שלהם. לדוגמה: תקיפת סייבר המשנה את זרימת המידע של התהליך ועל ידי כך משבשת את התהליך.

8.5 יש להתייחס לפגיעה בזמינות של רכיבי המערכת - פגיעה בזמינות של מערכת אדם-מכונה (HMI), בקר או רכיבי שטח (ברזים, וסתים וכדומה); לדוגמה: תקיפת סייבר במערכות בקרה ממוחשבות הגורמת לכך שלא ניתן לשלוט על בקר, חיישן או כל רכיב שטח. במקרה כזה התהליך עלול להיות בלתי נשלט ולגרום לאירוע חומרים מסוכנים.

8.6 במידה והעסק נדרש להעביר מידע דיגיטאלי אל מחוץ לעסק כגון ניטור ארובות, או ניטור גלאי חומרים מסוכנים, באחריות העסק לבצע את העברת הנתונים בצורה מאובטחת שתמנע שיבוש שלמות הנתונים, שיבוש זמינות הנתונים, או חדירת סייבר דרך תווך משלוח הנתונים הדיגיטאליים אל העסק.

8.7 במידה והעסק יבחר להיעזר בשירותי ייעוץ חיצוני בביצוע סקר סיכוני סייבר או בכל נושא אחר הקשור לסייבר, על היועץ/ת לעמוד בדרישות המופיעות בנספח ד' במדריך זה.

# 9. חישוב רמת סיכוני הסייבר

9.1 ניהול הסיכונים מושתת על הערכת סיכונים המשקפת את מידת פגיעותן של מערכות ממוחשבות, הערכת האיומים, השלכותיהם ומידת ההיתכנות שלהם.

9.2 **הערכת הסיכונים תתבצע על פי עקרונות מדריך זה בגרסתו העדכנית ליום הביצוע**. המדריך מבוסס על תורת ההגנה בסייבר של מערך הסייבר, עם התאמות ייחודיות בתחום החומרים המסוכנים ומערכות בקרה תעשייתיות. התרחישים האפשריים ייבחנו על פי העיקרון "מבט בעיני התוקף", היות שמאחורי המתקפה עומד תוקף אנושי. הדרך לפתרון מיטבי לאבטחת סייבר מחייבת הבנה עמוקה של דרכי פעולתו של התוקף, זיהוין ומניעתן.

9.3 ההנחה היא שבתקיפת סייבר זדונית ישוחרר מרב החומר המסוכן ברכיב המכיל את הכמות הגדולה ביותר בתהליך המסוכן המחובר למערכת המחשוב [3] (בניגוד לשחרור עקב תקלה או תאונה), ועל כן חישובים של פיזור החומרים המסוכנים יהיו בהתאם.

9.4 הסיכונים מבוססים על האיומים הרלוונטיים לרכיבי כל מערכת בהתאם לניתוח הסיכונים שנעשה בעסק.

9.5 **הערכת הסיכונים - חישוב רמת נזק (I)**. הערכת סיכונים מתחילה בהערכה של רמת הנזק (Impact) שעלול להיגרם לסביבה או לבריאות הציבור אם יתרחש אירוע חומרים מסוכנים בעקבות מתקפת סייבר. מידת הנזק תוערך בטווחים שבין 1 ל- 4 לפי השיטה המוצגת בטבלה שבנספח א' במסמך זה. יש לשים לב כי הציון שנקבע בשלב זה הוא לפי הערכת הנזק המרבית.

9.6 **הערכת סיכונים - חישוב רמת החשיפה (P)**. לאחר חישוב רמת הנזק הצפויה במקרה של אירוע חומרים מסוכנים שנגרם בעקבות מתקפת סייבר בעסק, יש לחשב את רמת החשיפה, ההסתברות לאירוע סייבר (Probability) במערכות המנהלות/מבקרות חומרים מסוכנים. חישוב זה מתבצע בטבלה שבנספח ב' במדריך זה.

3 ילקח מצב ה- WSC - Worst Case Scenario

## 9.7 חישוב של הערכת הסיכון וסיווג המערכות בעסק

הערכת רמת הסיכון תהיה מבוססת על שקלול של רמת הנזק הצפויה לנוכח הסיכוי שהנזק יתרחש, לפי הנוסחה להלן:

**סיכון = P+3*I**

**(הסיכון שווה לרמת החשיפה ועוד 3 פעמים רמת הנזק)**

**(I)** = רמת הנזק הצפויה בהתייחס למקרה ה-WCS - Worst Case Scenario (הערך שיתקבל בהתאם לנספח א' במדריך זה).

**(P)** = ההסתברות שהנזק יתרחש (הממוצע המתקבל מהחישוב בהתאם לנספח ב' במדריך זה).

יישום הנוסחה המפורטת לעיל של חישוב רמת הסיכון, ייצר ניקוד בין 4 ל-16.

כל אחת מהמערכות הממוחשבות בעסק המנהלות/מבקרות חומרים מסוכנים כפי שהוגדר במדריך זה, תסווג לאחת מארבע קבוצות לפי הערכת הסיכון שלה, כמפורט להלן:

- רמה 1: פוטנציאל סיכון נמוך (ניקוד בין 4 ל-7).
- רמה 2: פוטנציאל סיכון בינוני (ניקוד בין 8 ל-11).
- רמה 3: פוטנציאל סיכון גבוה (ניקוד בין 12-14).
- רמה 4: פוטנציאל סיכון גבוה מאוד (ניקוד בין 15 ל-16).

**חשוב לציין:**
באתר האינטרנט[4] של המשרד להגנת הסביבה, קיים קובץ אקסל לביצוע חישוב אוטומטי של רמת הנזק ורמת החשיפה.

4 https://www.gov.il/he/departments/publications/reports/cyber_industry_toxins_permit

9.8 מפת החום מתארת את רמות הסיכון כפונקציה של רמת נזק ורמת חשיפה:

| רמת נזק (I) / רמת חשיפה (P) | 4 | 3 | 2 | 1 |
|---|---|---|---|---|
| 4 | 16 | 13 | 10 | 7 |
| 3 | 15 | 12 | 9 | 6 |
| 2 | 14 | 11 | 8 | 5 |
| 1 | 13 | 10 | 7 | 4 |

9.9 כמות הבקרות להטמעה בכל רמת סיכון (כפי שמופיעות בנספח ג' במדריך זה):
יש לשים לב שכל רמת בקרות כוללת את הבקרות מרמה שמתחתיה. למשל רמת בקרות 4 כוללת את כל הבקרות האפשריות מרמות 1,2,3,4.

| פוטנציאל הסיכון | חבילת הבקרות בהתאם לפוטנציאל הסיכון | כמות הבקרות לרמה זו |
|---|---|---|
| 7- 4 | 1 | 44 |
| 11- 8 | 2 | 18 |
| 14- 12 | 3 | 24 |
| 16- 15 | 4 | 13 |
| סך כל הבקרות לכל הרמות | | 99 |

# 10. קביעת הבקרות הנדרשות ליישום

10.1 לאחר חישוב רמת הסיכון של התהליך, ידע העסק איזו חבילת בקרות[5] ליישם על פי המפתח שלהלן:

- רמת סיכון בערכים שבין 4-7 (כולל): חבילת בקרות 1.
- רמת סיכון בערכים שבין 9-11 (כולל): חבילת בקרות מרמה 2 (הכוללת בקרות מרמה 1 ובקרות מרמה 2).
- רמת סיכון בערכים שבין 12-14 (כולל): חבילת בקרות מרמה 3 (הכוללת בקרות מרמה 1, בקרות מרמה 2 ובקרות מרמה 3).
- רמת סיכון בערכים שבין 15-16 (כולל): חבילת בקרות מרמה 4 (הכוללת בקרות מרמה 1, בקרות מרמה 2, בקרות מרמה 3 ובקרות מרמה 4).

5 על פי רשימת הבקרות בנספח ג' במסמך זה

11.1 מסגרת הבקרות מבוססת על מסגרת NIST CSF (Cyber Security Framework) המורכבת מחמשת הפונקציות הבאות:

- Identify – זיהוי הסיכונים הכולל מיפוי החומרים המסוכנים המחוברים למערכות ממוחשבות המנהלות / מבקרות חומרים מסוכנים וביצוע סקר סיכונים על אותן מערכות.
- Protect – הטמעת בקרות על פי רמת הסיכון שהתקבלה בסקר הסיכונים על מנת למזער ככל האפשר את הסיכוי לארוע סייבר שיגרום לאירוע חומרים מסוכנים.
- Detect – הטמעת יכולות זיהוי תקיפה קיימת או תקיפה בשלבי התרחשותה.
- Respond – תגובה לארוע, לאחר התממשות הארוע.
- Recover – התאוששות מארוע וחזרה לשגרה.

## 11. אנליזת פערים - השוואה בין מצב נוכחי לבקרות נדרשות ומיפוי פערים

11.1 אל מול רשימת בקרות ההגנה המפורטות בנספח ג' שבמסמך זה, על העסק לבדוק מה מיושם בזמן סיום סקר הסיכונים בנוגע לכל אחת מהמערכות הנבדקות, ומה נדרש ליישם על פי תוצאות סקר הסיכונים.

11.2 תוצר התהליך המתואר בסעיף קודם יהיה רשימת פערים (Gap Analysis) - "רצוי מול מצוי" שיכין העסק.

11.3 יש להקפיד על בדיקה פרטנית בעסק לגבי כל מערכת ממוחשבת המנהלת/מבקרת חומרים מסוכנים.

11.4 רשימת הפערים המתקבלת מהווה את הבסיס לבניית תוכנית העבודה של העסק.

## 12. בנייה של תוכנית עבודה על בסיס מיפוי הפערים

12.1 באחריות בעל היתר הרעלים / ממונה הגנת הסייבר בעסק לגבש תוכנית עבודה ליישום הבקרות הנדרשות, בציון הגורמים האחראים, לוחות הזמנים ודרכי הטיפול. בעל העסק יקצה את המשאבים הנדרשים ובכללם תקציב, כוח אדם וזמן הנדרשים ליישום הבקרות הנדרשות.

12.2 סדר העדיפויות של יישום הבקרות החסרות לעסק במסגרת תוכנית העבודה, ייקבע באמצעות שקלול רמת הסיכון של התהליך המסוכן, עלות הפתרון של יישום הבקרות, מורכבות המימוש ומהירות יישום הבקרות.

12.3 העסק יחליט בעצמו על סדר העדיפויות של יישום הבקרות כל עוד הוא עומד בלוח הזמנים שנקבע במדריך זה.

# 13. נספחים

## נספח א' - טבלת חישוב רמת הנזק (I) של עסק המחזיק חומרים מסוכנים

בטבלה זו יש לענות על כל 4 השאלות שבעמודת "שאלה" על ידי מתן ציון מ-1 עד 4. לאחר מתן ציונים לכל השאלות, מידת הנזק תהא הערך הגבוה ביותר שהוזן בעמודת "ציון".

| שאלה | 1 | 2 | 3 | 4 | ציון (4-1) |
|---|---|---|---|---|---|
| | הנזק מוערך כאחד או יותר מהקריטריונים להלן[6]: | | | | |
| S (Safety) | 1. **בריאות הציבור:** ללא פגיעה ברצפטור ציבורי<br>2. **סביבה:** ללא פגיעה בסביבה | 1. **בריאות הציבור:** ללא פגיעה ברצפטור ציבורי<br>2. **סביבה:** פוטנציאל לאירוע חומרים מסוכנים שעלול לגרום לפגיעה בסביבה | **בריאות הציבור:**<br>1. פוטנציאל פגיעה ברצפטור ציבורי ברמת PAC 2<br>2. פוטנציאל לפיצוץ (UVCE): לחץ מרבי לרצפטור ציבורי של 0.1 באר<br>3. פוטנציאל לאירוע דלקה (BLEVE) - 1.6 קילו ואט למטר רבוע למשך 60 שניות רצופות (או קרינה בעוצמה מקבילה לזמן קצר יותר) | **בריאות הציבור:**<br>1. פוטנציאל פגיעה ברצפטור ציבורי ברמת PAC 3<br>2. פוטנציאל לפיצוץ (UVCE): לחץ מרבי לרצפטור ציבורי של 0.28 באר<br>3. פוטנציאל לאירוע דלקה (BLEVE) - 5 קילו ואט למטר רבוע למשך 60 שניות רצופות (או קרינה בעוצמה מקבילה לזמן קצר יותר) | S (Safety) |
| מהי מידת הנזק לבריאות הציבור או לסביבה שעלולה להיגרם עקב פגיעה בבטיחות המערכת שבבעלות העסק? | | | | | |
| C (Confidentiality) | | | | | C (Confidentiality) |
| מהי מידת הנזק לבריאות הציבור או לסביבה שעלולה להיגרם עקב חשיפת מידע על מערכת ממוחשבת המנהלת/מבקרת חומרים מסוכנים שבבעלות העסק? | | | | | |
| I (Integrity) | | | | | I (Integrity) |
| מהי מידת הנזק שייגרם לבריאות הציבור או לסביבה עקב שיבוש המידע ברכיב התעשייתי או עקב שיבוש התהליך שהרכיב התעשייתי הוא חלק בלתי נפרד ממנו? | | | | | |
| A (Availability) | | | | | A (Availability) |
| מהי מידת הנזק שיגרם לבריאות הציבור או לסביבה עקב השבתת הרכיב התעשייתי או תהליך ממוחשב? | | | | | |

6 הנתונים לקוחים מתוך חוזר מנכ"ל - מדיניות מרחקי הפרדה במקורות סיכון נייחים

## נספח ב' - טבלה לקביעת רמת החשיפה (P) של עסק המחזיק חומרים מסוכנים

בטבלה זו יש לענות על כל 36 השאלות שבעמודת "פרמטר נבדק" על ידי מתן ציון מ-1 עד 4. לאחר מתן ציונים לכל השאלות, יש לחשב את רמת החשיפה על ידי סיכום כל הציונים **וחישוב ממוצע** לכל הטבלה. התוצאה המתקבלת היא רמת החשיפה - P.

יש לבצע את הניתוח לפי טבלה זו בנוגע לכל התהליך המצוין במיפוי התהליכים המסוכנים ובנוגע לכל מערכת ממוחשבת בכל אחד מתהליכים אלה.

| רמת חשיפה ◄ / פרמטר נבדק ▼ | 1 | 2 | 3 | 4 | ציון (1-4) |
|---|---|---|---|---|---|
| 1. מספר עובדים החשופים למערכות אדם - מכונה (HMI) המנהלות/מבקרות חומרים מסוכנים | עד 5 | 6 - 10 | 11- 50 | יותר מ-50 | |
| 2. מספר עובדים בעלי גישה לבקרים המנהלים/מבקרים מערכת חומרים מסוכנים | עד 10 | 11- 25 | 26 - 50 | יותר מ-50 | |
| 3. אחריות הטיפול במערכות אדם - מכונה (HMI) | רק עובדים פנימיים | ספקים חיצוניים קבועים | ספקים חיצוניים מזדמנים | נגישות לגורמים נוספים | |
| 4. אחריות הטיפול בבקרים המשפיעים על מערכת חומרים מסוכנים | רק עובדים פנימיים | ספקים חיצוניים קבועים | ספקים חיצוניים מזדמנים | נגישות לגורמים נוספים | |
| 5. מספר עמדות אדם - מכונה (HMI) שיש בעסק | 1 | 2 - 5 | 6 - 10 | יותר מ-10 | |
| 6. מספר בקרים המנהלים/ מבקרים חומרים מסוכנים בעסק | עד 5 | 6 - 10 | 11 - 50 | יותר מ-50 | |
| 7. תקשורת בין רשת מנהלית לרשת תפעולית | אין - קיים ניתוק פיזי ברמת כבילה בין הרשתות | יש באמצעות חומת אש ודיודה חד-כיוונית | יש באמצעות חומת אש בלבד | יש ללא אמצעי בקרה | |
| 8. האם מתאפשרת גישה לאינטרנט מסביבת הבקרים התעשייתיים? | לא | יש חיבור, אבל בדרך כלל מנותק. מופעל לצורך תמיכה מרחוק | כן, אך עם בקרת חומת אש וסינון תוכן או רכיבי אבטחה נוספים | כן | |

| רמת חשיפה / פרמטר נבדק | 1 | 2 | 3 | 4 | ציון (1-4) |
|---|---|---|---|---|---|
| 9. עדכון קושחה בבקרים | מתבצע באופן מלא וקבוע | מתבצע באופן רחב | מתבצע באופן מועט | לא מתבצע | |
| 10. עדכון תוכנה בבקרים ובמערכות ICS נלוות. | מתבצע באופן מלא וקבוע | מתבצע באופן רחב | מתבצע באופן מועט | לא מתבצע | |
| 11. אבטחה פיזית למערכות אדם - מכונה (HMI) | נגישות לגורמים מורשים בלבד | נגישות לספקים חיצוניים קבועים | נגישות לספקים חיצוניים מזדמנים | נגישות גם לגורמים נוספים | |
| 12. אבטחה פיזית לבקרים הקשורים לחומרים מסוכנים | נגישות לגורמים מורשים בלבד | נגישות לספקים חיצוניים קבועים | נגישות לספקים חיצוניים מזדמנים | נגישות גם לגורמים נוספים | |
| 13. אבטחה פיזית לרכיבים בשטח שמשפיעים על חומרים מסוכנים (ברזים, וסתים, שסתומים וכדומה) | נגישות לגורמים מורשים בלבד | נגישות לספקים חיצוניים קבועים | נגישות לספקים חיצוניים מזדמנים | נגישות גם לגורמים נוספים | |
| 14. מספר אמצעי מיגון ואבטחה פיזית במערכת הנבדקת מבין 4 האמצעים הבאים: מצלמות, מערכת אזעקה, גישה ביומטרית, מאבטחים | 4 | 3 | 2 | 1 | |
| 15. מספר הגנות לוגיות קיימות למערכות אדם - מכונה (HMI), לדוגמא: הגנת תקשורת, הגנה אפליקטיבית, אנטי-וירוס | 3 ומעלה | 2 | 1 | אין | |
| 16. מספר הגנות לוגיות (הגנת תקשורת, הגנה אפליקטיבית, אנטי-וירוס) לבקרים הקשורים לחומרים מסוכנים | 3 ומעלה | 2 | 1 | אין | |
| 17. קמפיין מודעות עובדים לאבטחת מידע לעובדים ברצפת הייצור | מתבצע באופן סדיר וקבוע | מתבצע לעיתים קרובות | מתבצע לעיתים רחוקות | לא מתבצע כלל | |

| פרמטר נבדק / רמת חשיפה | 1 | 2 | 3 | 4 | ציון (1-4) |
|---|---|---|---|---|---|
| 18. האם מתנהל תהליך מסודר בקליטת עובד בעל גישה למערכות מחשוב תעשייתיות? | כן | תהליך חלקי | הוראות בעל-פה בלבד | לא | |
| 19. האם מתנהל תהליך מסודר בעזיבת עובד הכולל גריעת הרשאות / מחיקת משתמש? | כן | תהליך חלקי | הוראות בעל-פה בלבד | לא | |
| 20. האם יש תהליך לניוד עובד מתפקיד אחד לתפקיד אחר בתוך העסק בנוגע לגישה למערכות מחשוב תעשייתיות? | כן | תהליך חלקי | הוראות בעל-פה בלבד | לא | |
| 21. שימוש ברכיבי IIOT/ IOT בעסק | אין שימוש ברכיבים כאלה כלל | יש שימוש בעד 3 רכיבים | יש שימוש מ-4 ועד 10 רכיבים | יש שימוש ביותר מ-10 רכיבים | |
| 22. האם יש מדיניות ארגונית כתובה לצורך ניהול, בקרה והגנה על סביבת בקרים תעשייתיים? | כן | באופן חלקי | באופן מצומצם מאוד | אין | |
| 23. האם נעשה מיפוי תהליכים מסוכנים? | כן | באופן חלקי | באופן מצומצם מאוד | לא | |
| 24. האם נעשה שימוש בטכנולוגיית סלולר לצורך התחברות לעמדות HMI או לרכיבים אחרים במערך ה-ICS? | לא | כן, בתקשורת מוצפנת ובהזדהות חכמה | כן, בתקשורת לא מוצפנת או בהזדהות לא חכמה | כן, בלי תקשורת מוצפנת ובלי הזדהות חכמה | |
| 25. טיפול בהרשאות גישה של ברירת מחדל (משתמש וסיסמה של ברירת מחדל) | משנים שם משתמש וסיסמה של ברירת המחדל | משנים רק את סיסמת ברירת המחדל | משנים רק שם משתמש | משאירים ערכים של ברירת מחדל | |
| 26. האם יש רשת Wireless ברצפת הייצור? | לא | כן, אך מוגנת בהצפנה חזקה | כן, והיא מוגנת בהצפנה חלשה | כן, ולא מוגנת כלל | |
| 27. האם נעשים רישום ובקרה על מצאי הרכיבים במפעל העלולים להשפיע על אירוע חומרים מסוכנים? | נעשים באופן שוטף | נעשים לעיתים קרובות | נעשים לעיתים רחוקות | לא נעשים כלל | |

| רמת חשיפה ◀ / פרמטר נבדק ▼ | 1 | 2 | 3 | 4 | ציון (1-4) |
|---|---|---|---|---|---|
| 28. אפשרות גישה מרחוק למערכות אדם - מכונה (HMI) | אין | יש בתקשורת מוצפנת ובהזדהות חכמה | יש בתקשורת לא מוצפנת או בהזדהות לא חכמה | יש בלי תקשורת מוצפנת ובלי הזדהות חכמה | |
| 29. אפשרות גישה מרחוק למערכות הבקרה התעשייתיות (ICS) | אין | יש בתקשורת מוצפנת ובהזדהות חכמה | יש בתקשורת לא מוצפנת או בהזדהות לא חכמה | יש ללא תקשורת מוצפנת וללא הזדהות חכמה | |
| 30. שימוש במחשוב ענן | אין | יש במידה מועטה | יש במידה רבה | יש באופן מלא | |
| 31. ביצוע מבדקי חדירות | מבוצע באופן שוטף | מבוצע לעיתים קרובות | מבוצע לעיתים רחוקות | לא מבוצע כלל | |
| 32. קיום יתירות לרכיבי מחשוב קריטיים אשר מטפלים בחומרים מסוכנים | יש באופן מלא | יש ברוב הרכיבים הקריטיים | יש בחלק קטן מהרכיבים הקריטיים | אין יתירות | |
| 33. שימוש במדיה נתיקה במערכות אדם - מכונה (HMI) | התקן USB מושבת | התקן USB מופעל עם יכולת הלבנה | התקן USB מופעל עם הרשאות למורשים בלבד | התקן USB מאופשר חופשי | |
| 34. האם מוטמעת מערכת לאיסוף וניטור לוגים? | כן | מוטמעת ברובה | מוטמעת חלקית | לא מוטמעת | |
| 35. האם הגישה לממשקי אדם - מכונה (HMI) מאופשרת אך ורק באמצעות משתמשים אישיים לכל מפעיל? | משתמשים אישיים בלבד | משתמשים אישיים ברובם | משתמשים גנריים ברובם | משתמשים גנריים בלבד | |
| 36. הזדהות לממשקי אדם - מכונה (HMI) | הזדהות חכמה לרבות ביומטרי | הזדהות חכמה ללא ביומטרי | סיסמה כפופה למדיניות | סיסמה ללא מדיניות | |
| | | | | | Average (1-36) |

## נספח ג' - רשימת בקרות נדרשות

1. מבוא

בכדי להפחית את הסיכון להתממשות אירוע סייבר, בעל היתר הרעלים נדרש ליישם בקרות בתחומים שונים הקשורים לסייבר. בקרות אלו כוללות תהליכים, נהלים, מערכות הגנה, טכנולוגיות ועוד.

בקרות אלו מאוגדות על פי הנושאים השונים: בקרות להגנה על שרתים ותחנות קצה, בקרות על ניהול משתמשים, בקרות ניטור, נהלים ועוד.

2. פירוט רשימת הבקרות

קיימות ארבע רמות של בקרות, מרמה 1 עד רמה 4. בעל העסק יבצע סקר סיכונים ויישם את רמת הבקרות הנדרשת בהתאם לרמת הסיכון שהתקבלה. במידה ומתגלה סתירה או אי-התאמה בין בקרות שונות, הבקרה ברמה הגבוהה יותר היא הקובעת.

3. רשימת הבקרות בטבלה להלן:

**רשימת הבקרות**

| סעיף | בקרה נדרשת | פירוט | המלצות / הערות | רמה | בדיקה | מס' הבקרות בפרק זה |
|---|---|---|---|---|---|---|
| 1 | **מיפוי מערכות מחשוב ובקרת חומרים מסוכנים**<br><br>1.1 בעל העסק יבצע מיפוי כל החומרים המסוכנים אשר מטופלים במערכות ממוחשבות.<br><br>1.2 בעל העסק יבצע מיפוי כל מערכות המחשוב, הרשת, הבקרה, החישה והאוטומציה בעסק ואלה הן:<br>א. הנוגעות לאחסון, שימוש, זרימה, ייצור, שינוע, השמדה וגילוי חריגות ודליפות של חומרים מסוכנים.<br><br>ב. העלולות לגרום או לתרום לפריצת חומרים מסוכנים בפעולה זדונית או לא תקינה בהם.<br><br>ג. הנוגעות לרישום מלאי ולוגיסטיקה של חומרים מסוכנים. | 1.2 המיפוי יכלול:<br>רשימת המחשבים - בציון תפקידם והמערכות המותקנות עליהם לצורך תפקידם;<br>עמדות HMI/ אוטומציה ייעודיות/ משולבות מכונה - בציון דגם וגרסת תוכנה;<br>בקרים ומרכזות גלאים - בציון דגם, גרסת קושחה/תוכנה וסוג התקשורת Ethernet), Wi-Fi טלפון, אחר);<br>רכיבי IoT/IIoT וגלאים בציון דגם, מקום וסוג התקשורת אליהם;<br>רכיבי הרשת (מתגים, נתבים, נקודות גישה אלחוטיות, חומת אש) בציון דגם וחיבורם לרשתות אחרות/אינטרנט. | 1.2 ב. מומלץ להיוועץ באנשי מקצוע בתחום החומרים מסוכנים על מנת לברר אם מערכת ממוחשבת שאינה מטפלת בחומרים מסוכנים אבל עשויה להתלקח או להתפוצץ עקב התקפת סייבר (למשל דוד קיטור בעל בקר מתוכנת) - מסכנת חומרים מסוכנים בסביבתה. | 1 | 1.1 האם בוצע מיפוי חומרים מסוכנים.<br><br>1.2<br><br>האם בוצע מיפוי מערכות המחשוב והבקרה. | 2 |
| 1 | **בדיקת חדירות (Penetration Test)**<br><br>1.6 יש לבצע אחת לשנתיים בדיקת חדירות בעזרת מומחה אבטחת מידע, אשר תכלול לפחות:<br>א. בדיקת עמידות מערכות המחשוב ובקרת החומרים המסוכנים להתקפה מחוץ לעסק.<br><br>ב. בדיקת עמידות מערכות המחשוב ובקרת החומרים המסוכנים להתקפה מרשת ה-IT בעסק. | | 6.1 א. על מנת לא לפגוע במערכות הייצור, בדיקת החדירות יכולה להתבצע באחת מן הדרכים הבאות:<br><br>1. בזמן השבתה<br><br>2. ע"י הקמת סביבת מעבדה<br><br>3. הקמת סימולציה קרובה ככל האפשר למערכת הייצור באמצעות טכנולוגיות ייעודיות כגון Digital Shadow או Digital Twin | 4 | 1.6 דוח הבדיקה | 1 |

| סעיף | בקרה נדרשת | פירוט | המלצות / הערות | רמה | בדיקה | מס' הבקרות בפרק זה |
|---|---|---|---|---|---|---|
| 4 | **בקרת גישה בסיסית**<br><br>4.1 עמדות המחשוב יהיו מוגנות בשם וסיסמה אישיים, ויינעלו אוטומטית אחרי 10 דקות של חוסר שימוש או על פי החלטת העסק, ולא יותר מ- 30 דקות.<br><br>4.2 משתמשי מערכות המחשוב יופרדו לפחות לשתי רמות הרשאות ברמת מערכת ההפעלה - "משתמש" (ולהם ייאכפו הרשאות מינימליות להפעלת מערכות על פי תפקידם, גישה מינימלית לקבצים ומשאבים ברשת, אי יכולת להתקין תוכנה) ו"מנהל" בעל הרשאות רחבות יותר לשיקול העסק.<br><br>4.3 לעמדות הפעלה (HMI/ אוטומציה ייעודיות/משולבות מכונה) יוגדרו הרשאות גישה אפליקטיביות למשתמשים מורשים. ההרשאות יהיו ברמת צפייה, רמת הפעלת תהליכים מוגדרים, וברמת ביצוע שינויים במערכת ובתהליכים.<br><br>4.4 יוגדרו בעלי תפקיד המורשים לבצע שינויי הגדרות ופעולות תחזוקה לבקרים, חיישנים ורכיבי SCADA. יזוהו שמית (ולא גנרית) המורשים לעשות זאת מרחוק (באמצעות אפליקציה, חיבור רשת, טלפוניה וכו').<br><br>4.5 יוגדרו בעלי תפקיד הרשאים לבצע שינויים והגדרות ברשתות העסק.<br><br>4.6 לכל עמדת HMI, תחנת עבודה ומחשב המשמש לתכנות בקרים תוגדר תצורת התוכנות הדרושות ותיאסר התקנת תוכנות אחרות. | מדיניות בקרת הגישה נועדה לוודא כי רק גורמים מורשים יכולים לגשת למחשוב ובקרת חומרים מסוכנים, לצפות ולבצע שינויים, וכל זאת בהתאם להגדרות תפקידיהם וכפוף לפיקוח. | | 1 | 4.1-3 הדגמה מוצלחת של הזדהות, הרשאות שונות על עמדות אקראיות.<br><br>4.4-5 הצגת רשימת בעלי התפקידים.<br><br>4.6 בדיקת תוכנות המותקנות על עמדות אקראיות. | 6 |

| סעיף | בקרה נדרשת | פירוט | המלצות / הערות | רמה | בדיקה | מס' הבקרות בפרק זה |
|---|---|---|---|---|---|---|
| 4 | **בקרת גישה מתקדמת**<br><br>4.7 יש לסקור את רשימת המשתמשים מורשי הגישה למערכות מחשוב ובקרת חומרים מסוכנים, לפחות בתדירות רבעונית ולעדכן אותה אם חל שינוי בכוח האדם ובעלי התפקידים המורשים בעסק. יש לדלל הרשאות על פי כלל "הצורך לדעת" (Need to Know).<br><br>4.8 יש להגביל התחברות משתמש למערכת לאחר 5 ניסיונות התחברות כושלים באמצעות נעילת האפשרות לביצוע התחברות במשך פרק זמן מוגדר.<br><br>4.9 תוגדר ותיאכף מדיניות העוסקת בהתחברות מרחוק לרשת התפעולית. כל חיבור מרחוק יהיה מוצפן מקצה לקצה ומזוהה אישית בהזדהות חזקה (2FA).<br><br>4.10 תיאסר ותיחסם גישה למערכות מחשוב ובקרת חומרים מסוכנים מרשתות אלחוטיות של העסק, ותותר רק ממחשבי העסק המחוברים בחיבור חוטי לרשת.<br><br>4.11 תוגדר ותיאכף מדיניות סיסמאות נאותה הכוללת אורך, מורכבות וזמן תפוגה.<br><br>4.12 תוגדר מדיניות אישור מחשבים ניידים המשמשים לקונפיגורציה מקומית של בקרים ומערכות אוטומציה.<br><br>4.13 לביצוע שינויים קריטיים בעמדות HMI דוגמת שינויי לחצים, טמפרטורות וזרימה תידרש הקפצת חלון הדורש הזדהות נוספת. לא ייעשו שינויים קריטיים על פי הוראה שניתנה בדואר אלקטרוני / הודעת טקסט / שיחת טלפון / שיחת וידאו. | 4.11 מומלץ 8 תווים לפחות, מורכבות של 3 מתוך 4 (אותיות גדולות, קטנות, מספרים ותווים מיוחדים).<br><br>4.12 מחשב נייד ייעודי ללא חיבור לאינטרנט שלא יוצא מתחומי העסק ומיועד לתכנות הבקר בלבד, או מחשב של טכנאי חיצוני מוכר שנבדק לעדכוני אבטחה במערכת הפעלה ועדכוני אנטי וירוס ונבדק כי אין בו נוזקות.<br><br>4.13 יש לתוקפים יכולת זיוף דואר אלקטרוני, הודעות טקסט, התחזות בטלפון ואף בשיחת וידאו. כמו כן קיימות ברשת האינטרנט תוכנות רבות לזיוף קולי. | 4.10 ניתן ליישום באמצעות מערכת לחיבור חד-כיווני לסיגנלים החשמליים ישירות מהסנסורים והמפעילים (level 0) בתצורה מנותקת לחלוטין מהרשת המפעלית ולא מושפעת ממנה.<br><br>4.13 ניתן לממש בקרה מפצה לפי שיקול העסק להקפצת חלון הדורש הזדהות נוספת. על הבקרה המפצה לוודא שלא יעשה שינוי משמעותי אשר עלול לגרום לאירוע חומרים מסוכנים ע"י גורם בלתי מורשה. | 2 | 4.7 הצגת רשימה מעודכנת.<br><br>4.8 בדיקה על עמדה אקראית.<br><br>4.9 הדגמת אופן חיבור מרחוק.<br><br>4.10 בדיקה באמצעות מחשב ברשת האלחוטית.<br><br>4.11 הדגמת שינוי סיסמה.<br><br>4.12 הצגת המדיניות.<br><br>4.13 הדגמת התהליך של הקפצת חלון. | 7 |

| סעיף | בקרה נדרשת | פירוט | המלצות / הערות | רמה | בדיקה | מס' הבקרות בפרק זה |
|---|---|---|---|---|---|---|
| 4 | **בקרת גישה מחמירה**<br><br>4.14 מדיניות החיבור מרחוק תוגבל רק למשתמשים שהזדהו בהזדהות חזקה (2FA) ומחשבם נבדק וזוהה כבטוח (סרוק ונקי מקוד זדוני ובעל עדכוני אבטחת מידע במערכת ההפעלה כמו גם אנטי וירוס מעודכן).<br><br>4.15 במידה ומשתמש המנסה לבצע פעולה אסורה (כגון: הכנסת DOK, התקנת תוכנה) יש לוודא כי תצא התראה למנהל המערכת, העובד ינעל ידנית וינקטו נגדו צעדים משמעתיים.<br><br>4.16 משתמש בעל הרשאות גבוהות (מנהל מחשוב, יכולת שינויי תצורה במערכות הייצור) יידרש להזדהות חזקה ויוגבל ברמת המשתמש (במידה והמערכת מאפשרת זאת) לעבודה בעמדה אחת בלבד בו-זמנית.<br><br>4.17 תיאסר ותיחסם כליל אפשרות השתלטות ישירה על מערכות מחשוב של חומרים מסוכנים העובדות במוד אינטרנטי (Remote Desktop, TeamViewer, Remote Assist, AnyDesk וכו').<br><br>4.18 תיאסר ותיחסם גישה ישירה לרכיבי חומרה (בקרים, חיישנים וכו') מחוץ לעסק.<br><br>4.19 יש לנטר ולבצע רישום של כל פעילות המבוצעת מרחוק.<br><br>4.20 יש לתעד ביומן רישום אוטומטי (רישום Log) של כל יצירה, שינוי, אפשור, נעילה והסרה של חשבון. | | 4.16 אפשרי באמצעות כרטיס עובד או בקרה מפצה אחרת שתאושר ביחידת הסייבר של המשרד להגנת הסביבה ואשר עונה על הצורך האבטחתי.<br><br>4.17 תתאפשר בקרה מפצה הולמת אשר מונעת את אפשרות הגישה של גורם בלתי מורשה למערכות המחשוב / המנהלות מבקרות חומרים מסוכנים.<br><br>4.19 מומלץ לבצע הקלטה במידת האפשר.<br><br>4.20 מומלץ לבצע הקלטה במידת האפשר. | 3 | 4.14 הדגמת התהליך.<br><br>4.15 הדגמת התהליך.<br><br>4.16 הדגמת התהליך.<br><br>4.17 בדיקת הגדרות במחשבים וברשת (FW/SWITCH)<br><br>4.18 הדגמת התהליך.<br><br>4.19 הצגת התיעוד.<br><br>4.20 הצגת התיעוד. | 7 |
| 4 | **בקרת גישה מרבית**<br><br>4.21 לא תינתן גישה למערכות מחשוב ואוטומציה המטפלות בחומרים מסוכנים, ע"י מחשבים אשר הגיעו מחוץ לעסק או עזבו את תחומו.<br><br>4.22 לא יתאפשר חיבור מרחוק כלשהו אל הרשת התפעולית, למעט צפייה בלבד (קבלת סטטוס) בחיבור חד-כיווני מאובטח.<br><br>4.23 יש להגדיר ולאכוף תנאים לחסימת שימוש בחשבונות, בהתאם לשעות פעילות העסק, ובהתאם לשעות העבודה של סוגי העובדים השונים. | 4.21 כגון מחשבים ניידים של טכנאים, אפליקציות SCADA לטלפונים חכמים על מכשירי העובדים.<br><br>4.23 דוגמאות לתנאי חסימת כניסה: סופי שבוע, שעות הלילה. הנחיה זו תקפה רק לאתרים בתוך העסק אשר אינם מאויישים 24/7 | 4.22 ניתן ליישום באמצעות מערכת לחיבור חד-כיווני לסיגנלים החשמליים ישירות מהסנסורים והמפעילים (level 0) בתצורה מנותקת לחלוטין מהרשת המפעלית ולא מושפעת ממנה. | 4 | 4.20 הצגת התיעוד.<br><br>4.21 הצגת הפתרון החד-כיווני.<br><br>4.22 הצגת אופן המימוש. | 3 |

| סעיף | בקרה נדרשת | פירוט | המלצות / הערות | רמה | בדיקה | מס' הבקרות בפרק זה |
|---|---|---|---|---|---|---|
| 6 | **הקשחת תחנות עבודה, HMI ושרתים**<br>6.1 יש להגדיר את תצורת המערכת כך שתספק את הפונקציונליות המינימלית הנדרשת (תוך הסרת אפליקציות, חסימת פונקציות, פורטים ופרוטוקולים שאינם נדרשים), על בסיס פרקטיקות מקובלות, לרבות שיכללו לכל הפחות:<br>א. חסימת פורטים שאינם נחוצים.<br>ב. הסרת אפליקציות, ושירותים לא נחוצים.<br>ג. הסרת חשבונות אורח/ברירת מחדל ומנהל מקומי.<br>ד. מנגנון קבלת עדכוני מערכת הפעלה.<br>ה. חסימת הכנסת התקני אחסון ומדיה.<br>ו. חסימת התקנת תוכנה וחומרה על-ידי משתמשים לא מורשים.<br>ז. מדיניות תוכנות מורשות בעמדת ה-(HMI Application list ) | 6.1 ד. כגון WSUS, SCCM או הבאה ידנית של עדכונים ע"ג מדיה אשר עברה אימות של מנפיק העדכונים (checksum) ואשר עברה הלבנה.<br><br>6.1 ה. כגון DOK, CD/DVD, מכשיר סלולרי, מצלמה וכדומה. | 6.1 ניתן להתבסס על פרקטיקות מקובלות, כגון NIST, פרסומי ה-CERT הלאומי וכדומה, או על שירותי מומחה, אשר יכין נוהלי הקשחה לפי הטכנולוגיה הרלוונטית. | 1 | 6.1 הצגת אופן ההקשחה שבוצעה לכל סוג של מערכת מחשוב. | 1 |
| 7 | **מניעת קוד זדוני בסיסית**<br><br>7.1 יש להטמיע כלים לזיהוי ולמניעה של קוד זדוני על תחנות עבודה ושרתים בעסק. כלים אלו יופעלו במתכונת התראה / הגנה אקטיבית (לשיקול העסק) וכן יבוצעו סריקות תקופתיות.<br><br>7.2 העסק יגדיר נהלים לטיפול בתחנות, בשרתים או בשרתות הנגועים בקוד זדוני.<br><br>7.3 יש לקבוע מנגנון קבלת/העברת עדכונים לכלים (מסעיף 7.1) בתדירות דו שבועית לפחות. | 7.1 מאחר וחלק מהפוגענים עשויים לחדור את מנגנוני האבטחה, יש לוודא כי בקרות לטיפול בקוד זדוני ייושמו בכל השרתים ובתחנות העבודה.<br><br>7.3 בדומה לעדכוני מערכת הפעלה יש להציג פתרון עדכונים לכלי. | 7.1 ניתן להשתמש בכל כלי לזיהוי ומניעה של קוד עוין (כגון אנטי-וירוס) מיצרן מוכר. | 1 | 7.1 הצגת הכלי המותקן.<br><br>7.2 הצגת הנוהל.<br><br>7.3 הצגת מנגנון העדכון. | 3 |

| סעיף | בקרה נדרשת | פירוט | המלצות / הערות | רמה | בדיקה | מס' הבקרות בפרק זה |
|---|---|---|---|---|---|---|
| 7 | **מניעת קוד זדוני מתקדמת**<br><br>7.4 יש להטמיע כלי לזיהוי וחסימת נוזקות ברמת הרשת. הפתרון יכלול טיפול בתקיפות Zero Day כגון: כופרות.<br><br>7.5 העסק יפעיל אמצעים לזיהוי ומניעה IDS/IPS, המתבססים על זיהוי התנהגות החורגת מהתנהגות מקובלת וסבירה (זיהוי אנומליה ברשת והתנהגות עמדה/משתמש).<br><br>7.6 העסק ינהל באמצעות מערכת בקרה מרכזית (SIEM) את כלל כלי מניעת הקוד הזדוני ואבטחת המידע בעסק.<br><br>7.7 העסק יפתח יכולת לחסום מזהי תקיפה (IOC) בצורה מהירה, הכוללת כתובות IP, חתימות HASH , מפתחות REGISTRY , שמות קבצים, מחרוזות וכל מזהה אחר שיוכל למנוע תקיפה.<br><br>**מניעת קוד זדוני מירבית**<br><br>7.8 מניעת התקפה בשלב המוקדם ביותר, לפני שלב ההרצה (ההדבקה/תקיפה) בשלב ראש הגשר ע"י התמקדות ב-Malware ולא בתוקף, ע"י שימוש בטכניקות של הטעיה, הרתעה, הסתרה, בידוד ברמת הקוד ובכך לייצר סביבה בה הנוזקה לא יכולה להתקיים ו/או לפרוס את ראש הגשר. | 7.4 ניתן למימוש באמצעות אנטי וירוס הכולל בתוכו רכיב Sand Box.<br><br>7.7 ניתן ליישם ע"י כלים כמו חומת אש, אנטי וירוס, SNORT , חוקי YARA וכלים נוספים.<br><br>7.8.מדובר בפתרון לסגירת שכבה נוספת בנוסף למוצר Sand Box. | 7.5 ניתן להשתמש בבקרה מפצה אחרת אשר תיתן מענה לצורך.<br><br>ניתן ליישום באמצעות הטמעה של מערכת לזיהוי אנומליות תהליכיות בסביבת הסיגנלים החשמליים.<br><br>ניתן להפעיל ב-IPS את רכיב ה-IDS בלבד, כל עוד קיים מענה אנושי שיחליף את המענה האוטומטי של חסימה, אשר יפעיל שיקול דעת ויחליט מה לחסום. | 3 | 7.4 הצגת הכלים ואופן הטמעתם.<br><br>7.7 בדיקת הכלים<br><br>7.8 בדיקת הטמעת הכלים | 4 |

| סעיף | בקרה נדרשת | פירוט | המלצות / הערות | רמה | בדיקה | מס' הבקרות בפרק זה |
|---|---|---|---|---|---|---|
| 9 | **אבטחת רשת בסיסית**<br><br>9.1 יש לתעד במסמכים את תיאור הרשתות המשמשות את מערכות המחשוב והאוטומציה של חומרים מסוכנים, ההפרדות, המגבלות וההגנות שיושמו בהן.<br><br>9.2 תוגבל הגישה מרשתות אחרות בעסק (IT, Wi-Fi) לרשתות המשמשות את מערכות המחשוב והאוטומציה של חומרים מסוכנים באמצעות ניהול הרשאות.<br><br>9.3 יש ליישם מנגנונים למניעת חיבור לא מורשה לרשתות המשמשות את מערכות המחשוב והאוטומציה של חומרים מסוכנים.<br><br>9.4 הרשתות המשמשות את מערכות המחשוב והאוטומציה של חומרים מסוכנים ינותקו מרשת האינטרנט למעט אפשרות חיבור ייעודי מוצפן (VPN) ובהזדהות חזקה.<br><br>9.5 יש למנוע גישורים בין רשתות שונות באמצעות כבלים וחיבורים שונים כגון חיבורים סריאליים (RS-485 RS-232 וכדומה) המשמשים לשליטה ובקרה על ציוד. RS 485 , RS-232 וכדומה) המשמשים לשליטה ובקרה על ציוד. יש להמנע מתצורת "ספגטי" בארון התקשורת ויש לדאוג לסידור וסימון רכיבי התקשורת וכן זיהוי חד ערכי של הציוד המחובר. מחשבים המשמשים להגדרת ציוד מקרוב ינותקו מהאינטרנט.<br><br>9.6 יש לוודא כי לכל מרכיבי הרשת (מתגים, נתבים, חומת אש, נקודות גישה) סיסמאות ניהול מורכבות וייחודיות השונות מסיסמת ברירת מחדל של היצרן, והשמורות אך ורק אצל בעלי התפקידים המוסמכים לעשות שינויים בהגדרות הרשת.<br><br>9.7 במידה ונעשה חיבור באמצעות מכשיר סלולרי, יש לבצע זאת באמצעות מכשיר ייעודי לצורךמרחוק ההתחברות בלבד והמנעות משימוש אישי או גלישה לאתרים אחרים. במכשיר יותקן גם אנטי וירוס עדכני , ויבוצעו בדיקת עדכוני מערכת הפעלה שוטפים. תינתן עדיפות למערכת הפעלה IOS. | 9.3 יש לוודא כיבוי כל הפורטים שאינם בשימוש במתגים, והפעלתם בהגדרה ידנית או מנגנוני NAC.<br><br>9.5 מצב "ספגטי" בארון התקשורת גורם לכך שיתכנו גישורים לא רצויים בין רשתות. סידור תקין של כבלי התקשורת בארון כאשר כל כבל חתוך באורך רצוי, נותן מבט ויזואלי טוב יותר ומונע גישורים לא רצויים.<br><br>9.7 ניתן להשתמש גם במכשיר סלולרי ישן שפורמט להגדרות יצרן ובלבד שישמש אך ורק את הפעילות הנדרשת מול רצפת הייצור ולא ישמש בשום מצב לשימוש פרטי של העובד. | מומלץ לבצע הפרדת רשתות פיזית או באמצעות חומת אש. | 1 | 9.1 הצגת תיעוד הרשתות.<br><br>9.2-6 הצגת ההגבלות שיושמו.<br><br>9.7 בדיקת המצאות הסלולרי הייעודי. | 7 |

| סעיף | בקרה נדרשת | פירוט | המלצות / הערות | רמה | בדיקה | מס' הבקרות בפרק זה |
|---|---|---|---|---|---|---|
| 9 | **אבטחת רשת מתקדמת**<br><br>9.8 יש לכבות או להסיר ברכיבי החומרה התומכים בחיבור אלחוטי את יכולת החיבור האלחוטי כמו גם יציאות פיזיות שלא בשימוש (כגון יציאות USB)<br><br>9.9 תימנע גישה ישירה מחוץ לרשת המקומית לרכיבי חומרה. גישה מחוץ לרשת המקומית תוגבל אך ורק לעמדות ניהול הדורשות הזדהות.<br><br>9.10 יש ליישם סינון תקשורת ברמה פרטנית ברשתות המשמשות את מערכות המחשוב והאוטומציה של חומרים מסוכנים ולהגדיר בדיוק את הפורטים ונתיבי התקשורת המותרים.<br><br>9.11 יש לבצע סריקת רשתות תקופתית, לזהות את כל האלמנטים המשתתפים בתקשורת וסוגי התקשורת שהם יוזמים ומקבלים, להסיר אלמנטים לא מזוהים, לנתח חריגות בתקשורת ולתקן בהתאמה את מנגנוני ההפרדה. תדירות הביצוע לא תקטן מאחת ל-18 חודשים. | 9.7 ניתן להשתמש גם במכשיר סלולרי ישן שפורמט להגדרות יצרן ובלבד שישמש אך ורק את הפעילות הנדרשת מול רצפת הייצור ולא ישמש בשום מצב לשימוש פרטי של העובד. | | 3 | 9.8-9 הצגת הפעולות שנעשו.<br><br>9.10 הצגת יישום הסינון.<br><br>9.11 הצגת תוצאות הסריקה האחרונה. | 4 |
| 9 | **אבטחת רשת מרבית**<br><br>9.12 הרשתות המשמשות את מערכות המחשוב והאוטומציה של חומרים מסוכנים יהיו סגורות, חוטיות ונפרדות לחלוטין (מתגים וכבילה נפרדת) מרשתות אחרות של העסק.<br><br>9.13 החיבור היחיד שיותר החוצה הוא הוצאת נתוני בקרה/סטטוס/לוגים חד-כיווני לרשת אחרת, באמצעות פתרון מאושר להעברת מידע באופן חד-כיווני.<br><br>9.14 יש ליישם מנגנונים בתוך הרשתות המסננים תקשורת שאינה תואמת את מבנה הפרוטוקול/ המידע המצופה. | | | 4 | 9.12 הצגת הרשת הנפרדת.<br><br>9.13 הצגת הפתרון החד כיווני.<br><br>9.14 יש להציג את פתרון הסינון. | 3 |

| סעיף | בקרה נדרשת | פירוט | המלצות / הערות | רמה | בדיקה | מס' הבקרות בפרק זה |
|---|---|---|---|---|---|---|
| 10 | **הפרדת סביבת מערכות המחשוב והאוטומציה ברשת התפעולית המכילה חומרים מסוכנים**<br><br>10.1 יש להגדיר תהליך אישור להעברת נתונים, סקריפטים ותוכנה שהתקבלה מסביבה אחרת בעסק או מחוצה לו אל סביבה זו.<br><br>10.2 יש לבצע עדכוני תוכנה וקושחה ישירות מיצרן הציוד או התוכנה באופן מאומת.<br><br>10.3 יש לאסור הכנסת סקריפטים או קונפיגורציות לאוטומציית ייצור/HMI או קונפיגורציות בקרים שמקורם אינו ידוע או אינו מאומת. | 10.2. אימות התוכנה והקושחה באמצעות checksum או קבלת מדיה ישירות מנציג החברה. | | 1 | 10.1-3 הצגת התהליכים להעברת עדכוני קושחה ותוכנה ובדיקתם. | 3 |
| 11 | **שימוש במשאבי ענן ציבורי בעבור מערכות המחשוב והאוטומציה ברשת התפעולית המכילה חומרים מסוכנים**<br><br>11.1 יש להגדיר מספר מצומצם של בעלי תפקידים בעלי גישה לממשק הניהול של שירות הענן.<br><br>11.2 חיבור לממשק הניהול של שירות הענן יהיה מאובטח בהזדהות חזקה.<br><br>11.3 יש לוודא כי גם השרתים/ המכונות המופעלים בענן עונים לכל הדרישות המתאימות לרמת הבקרה הנדרשת בהתאם לפוטנציאל הסיכון (לרבות הקשחה, הגבלת תקשורת, כלים למניעת קוד זדוני, שימוש בהרשאות מינימליות למשתמשים וכו'). | 11. כל הבקרות במסמך זה תקפות גם לשימוש במחשוב ענן ציבורי.<br><br>על העסק המעלה נתונים לענן לוודא חלוקת אחריות ברורה לאבטחת המידע בין ספק הענן לעסק. | | 1 | 11.1-2 יש להציג את בעלי התפקידים ואופן ההזדהות.<br><br>11.3 הצגת סוגי המכונות בשימוש וההגנות שיושמו. | 3 |
| 11 | **חיבור חד כיווני**<br><br>11.4 מערכות מחשוב ובקרת חומרים מסוכנים יוגבלו רק לייצא נתונים לענן בחיבור חד-כיווני, באמצעות פתרון מאושר להעברת מידע באופן חד-כיווני. | | 11.4 ניתן ליישום באמצעות מערכת לחיבור חד-כיווני לסיגנלים החשמליים ישירות מהסנסורים והמפעילים (level 0) בתצורה מנותקת לחלוטין מהרשת המפעלית ולא מושפעת ממנה. | 4 | 11.4 הצגת הפתרון החד כיווני. | 1 |

| סעיף | בקרה נדרשת | פירוט | המלצות / הערות | רמה | בדיקה | מס' הבקרות בפרק זה |
|---|---|---|---|---|---|---|
| 12 | **הגדרת כללי שימוש ותחזוקה**<br><br>12.1 יוגדרו בעסק בעלי תפקידים המורשים לגשת לבקרים (לתחזוקה מקרוב) ולעמדות ניהול/ HMI וכן כללים לביצוע שינויי קונפיגורציה, זיהוי והתמודדות עם כשלים בבקרים (אישורים נדרשים, פיקוח, סדר עצירת/הפעלת מערכות).<br><br>12.2 עדכוני קושחה, שינויי קונפיגורציה וכדומה ייבדקו מראש בסביבת מעבדה בטרם העברתם לסביבת ייצור. | 12.1 המטרה למנוע אירוע המערב חומרים מסוכנים עקב טעות אנוש, כשל בבקר או שינוי קונפיגורציה שגוי.<br><br>12.2 ניתן לבדוק גם באמצעות מערכת סימולציה שמדמה את הסביבה האמיתית. | | 1 | 12.1 הצגת הנהלים.<br><br>12.2 הצגת תהליך הבדיקה. | 2 |
| 12 | **מעקב תצורה וגיבוי**<br><br>12.3 העסק ינהל רישום של הבקרים הנוגעים לחומרים מסוכנים ויכלול לפחות: יצרן, דגם, גרסת קושחה, גרסת קונפיגורציה, מיקום קובץ קונפיגורציה לגיבוי, מיקום גרסת קושחה לגיבוי.<br><br>12.4 יש לגבות קושחות וקונפיגורציות בקרים, סקריפטים, תצורות/Image תחנות עבודה/ HMI ותהליכי ייצור במערכת מאובטחת/נפרדת, המרוחקת פיזית (50 קילומטרים לפחות) מאזור לקיחת הגיבוי.<br><br>12.5 העסק צריך להיות בעל יכולת לשחזר בקר מגיבוי, או לשחזר תחנת עבודה/HMI בתוך יום עבודה מזיהוי תקלה או פעולה חריגה. לחלופין השבתת התהליך המבוקר עד לסיום השחזור.<br><br>12.6 על העסק להיות בקשר רציף עם יצרני הבקרים והמערכות שברשותו ולקבל עדכונים על סוגיות אבטחת מידע וגרסאות תוכנה וקושחה עדכניות. | 12.5 היכולת להיות יכולה להיות עצמאית או באמצעות מיקור חוץ. | 12.4 רצוי גם בעותקים על מדיה נתיקה (דיסק, DOK) שישמרו באתר. | 2 | 12.3 הצגת הרישום.<br><br>12.4-6 הצגת הגיבויים, יכולת השחזור, עדכונים מהיצרן. | 4 |

| סעיף | בקרה נדרשת | פירוט | המלצות / הערות | רמה | בדיקה | מס' הבקרות בפרק זה |
|---|---|---|---|---|---|---|
| 12 | **אבטחה מתקדמת**<br><br>12.7 יש לבצע הקשחה של הבקרים על פי הוראות היצרן, ולהשתמש בכל יכולות אבטחת המידע של הבקר הנוגעות להזדהות, צמצום והגנת התקשורת אליו ומניעת שינויים לא רצויים. יש לבצע בדיקה של ההקשחה בסביבת מעבדה לפני העברה לסביבת ייצור.<br><br>12.8 יש לוודא כי לכל בקר סיסמת ניהול מורכבת וייחודית ולא סיסמת ברירת מחדל של היצרן. הסיסמה תהיה שמורה אך ורק אצל בעלי התפקידים המוסמכים לבצע שינויים בבקרים.<br><br>12.9 גישה מרחוק לתחנות עבודה/ HMI תדרוש הזדהות חזקה.<br><br>12.10 מערכת ההפעלה של תחנת עבודה/HMI ללא שימוש תינעל לאחר 10 דקות או לשיקול המפעל אך לא יותר מ-30 דקות, למעט תחנות שהוגדרו לצפייה בלבד.<br><br>12.11 נסיון לבצע שינוי משמעותי בתהליך כדוגמת שינוי ספים ללחצים, טמפרטורות, זרימות או ריאקציות ידרוש הזנה נוספת של סיסמה או ביצוע הזדהות חזקה בטרם השלמתו | 12.7 ליצרנים שונים הנחיות הקשחה שונות בהתאם ליכולות הציוד, לרבות סגירת פורטים, הפסקת תמיכה בפרוטוקולים לא מוצפנים, דרישת הזדהות לפני ביצוע שינוי קונפיגורציה, יכולת שחזור אוטומטית של קונפיגורציה קודמת ועוד. | | 3 | 12.7 הצגת ההקשחות.<br><br>12.8-10 סקירת ההגנה המתקדמת.<br><br>12.11 הצגת יישום ההפרדה. | 5 |
| 12 | **אבטחה מרבית**<br><br>12.12 מערכות המחשוב יחויבו לרוץ על מערכת הפעלה עדכנית נתמכת המקבלת עדכוני אבטחה רציפים.<br><br>12.13 שינויי תהליך ידרשו אישור בהזדהות חזקה של מנהל בכיר.<br><br>12.14 הבקרים יופרדו לרשתות שונות בהתאם לתפקידם/ לתהליך שהם משתתפים בו. תחנות העבודה/HMI יחוברו לרשת נפרדת מהבקרים. תקשורת בין הרשתות תנוהל באמצעות חומת אש. | 12.12 גרסאות נתמכות של חלונות, לינוקס וכו'.<br><br>12.14 ניתן לבצע על בקרים חליפיים כבדיקה לפני העלאה לייצור או על בקרי ייצור בתקופות השבתה / הדממה של מערכות הייצור. | 12.13 ניתן להשתמש במגוון אמצעים, כגון ביומטריה, כרטיסים חכמים, OTP ועוד. | 4 | | 3 |

| סעיף | בקרה נדרשת | פירוט | המלצות / הערות | רמה | בדיקה | מס' הבקרות בפרק זה |
|---|---|---|---|---|---|---|
| 12 | **הגנה והפרדה של מערכות בטיחות, גילוי ואבטחה**<br><br>12.15 יש לוודא כי רשת הגלאים בעסק תבודד ברשת נפרדת ללא אפשרות גישה ממנה אל מערכות מחשוב המנהלות/מבקרות חומרים מסוכנים.<br><br>12.16 עמדת בקר הגלאים תהיה נעולה בארון תקשורת על מנת לוודא שלא יבוצעו שינויים בלתי-מבוקרים.<br><br>12.17 אם בבקר הגלאים יש יכולת לנעילת מצב תכנות הבקר, עליו להיות במצב נעול בזמן שגרה.<br><br>12.18 אם בקר הגלאים מחובר בחיבור רשת/טלפוניה למוקד שמירה/תמיכה, יש לוודא כי נמנעת היכולת לבצע שינויי הגדרות/השבתה מרחוק.<br><br>12.19 גדרות חשמליות, מערכות בקרת גישה, מערכות מתח נמוך וכל מערכת תומכת אחרת שמחוברת לרשת מחשבים- יש להפרידן רשתית ללא אפשרות גישה מהן אל מערכות מחשוב המנהלות/מבקרות חומרים מסוכנים.<br><br>12.20 מצלמות אבטחה - יש למנוע גישה פיזית אל מצלמות האבטחה, ולהפריד רשתית ללא אפשרות גישה מהן אל מערכות מחשוב ובקרת חומרים מסוכנים. | 12.15 אם רשת הגלאים היא חלק מרשת הייצור, פריצה לרשת זאת תאפשר גישה לרשת רצפת הייצור.<br><br>12.16 אם עמדת הבקר גלויה, יש חשיפה לשינוי ערכי סף בגלאים.<br><br>12.17 בבקרים ישנם מצבי תכנות ומצבי עבודה. אין להשאיר את הבקר במצב פתוח לתכנות בזמן עבודה שגרתית.<br><br>12.18 במידת הצורך יאופשר שינוי הגדרות רק לזמן קצוב למתן תמיכה מרחוק וייחסם שוב.<br><br>12.19-20 במצלמות ובמערכות מתח נמוך אחרות שהגישה הפיזית אליהן חופשית, יש אפשרות להכניס מדיה נתיקה או להתערב בצורה אחרת, ודרכם להחדיר קוד זדוני. | 12.15 ניתן ליישם באמצעות חומת אש או בידוד פיזי או פריסת גלאים במגע יבש.<br><br>12.17 ניתן ליישם באמצעות נעילה פיזית או לוגית כפי שנתמכת על ידי הבקר.<br><br>12.19-20 ניתן ליישם באמצעות חומת אש או הפרדה פיזית.<br><br>12.20 מומלץ במידת האפשר להציב את המצלמות גבוה, ולהימנע מחיבור אלחוטי. | 1 | | 6 |

| סעיף | בקרה נדרשת | פירוט | המלצות / הערות | רמה | בדיקה | מס' הבקרות בפרק זה |
|---|---|---|---|---|---|---|
| 15 | **מדיות בשימוש בקרים ועמדות תפעול/HMI**<br><br>15.1 על מנת להעביר גרסאות תוכנה וקושחה, קונפיגורציות, סקריפטים וכו' יש להשתמש במדיה ייעודית של העסק השמורה לשימוש זה בלבד במקום בטוח.<br><br>15.2 מדיות המשמשות לגיבוי גרסאות קושחה, קונפיגורציות בקרים וסקריפטים יאוחסנו במקומות בטוחים ונעולים.<br><br>15.3 יש לבצע סריקת נוזקות במדיה שבה מועבר המידע לפני כל העברה. | 15.1 מדיה שיש לה שימושים אחרים חשופה יותר להידבקות בנוזקה.<br><br>15.3 סריקת נוזקות במדיה במחשב / עמדת הלבנה שאינו קשור למחשוב ובקרה של חומרים מסוכנים. | | 1 | | 3 |
| 18 | **מודעות ואכיפה**<br><br>18.1 יש לבצע הדרכת מודעות עובדים עם דגש על רשתות OT ומערכות ICS לפחות אחת לרבעון.<br><br>18.2 יש להפיץ בקרב העובדים והשומרים הנחיות מתאימות - עובדים ואורחים שאינם קשורים למערכות הבקרה והמחשוב המנהלות/מבקרות חומרים מסוכנים לא אמורים להיות בסביבתם. עובד לא מורשה שיימצא למשל בסמיכות לארונות בקרים או גלאים, מחבר אלמנטים לרשת על דעת עצמו, מנסה לגשת לעמדות תפעול/HMI - יטופל משמעתית. העסק יכתוב ויפיץ בקרב העובדים נוהל ברוח הדברים.<br><br>18.3 יש לנעול ארונות תקשורת וארונות בקרים ולוודא את הימצאות המפתח במקום דיסקרטי. | 18.1 עובד ללא מודעות סייבר ואבטחת מידע עלול לגרום נזק גדול לארגון ע"י מימוש האיום הפנימי. | | 1 | 18.1 ציון מועדי ההדרכה. בדיקה אל מול עובדי העסק.<br><br>18.2 הצגת פעילות ההסברה שנעשתה בקרב העובדים והשומרים.<br><br>18.3 בדיקת נעילה. | 3 |

| סעיף | בקרה נדרשת | פירוט | המלצות / הערות | רמה | בדיקה | מס' הבקרות בפרק זה |
|---|---|---|---|---|---|---|
| 18 | **אבטחה מתקדמת**<br><br>18.4 יש להציב מצלמות אבטחה לתיעוד הגישה לארונות תקשורת, ארונות בקרים ותחנות עבודה/ HMI.<br><br>18.5 יש להתקין מערכת אזעקה שתתריע על ניסיון לגשת לארונות תקשורת, ארונות בקרים ותחנות עבודה שלא בשעות העבודה.<br><br>18.6 יש להפיץ בקרב העובדים והשומרים הנחיות מתאימות - טכנאים חיצוניים ומבקרים יידרשו להפקיד כל מדיה (מגנטית, אופטית), טלפון סלולרי ואמצעי מחשוב שברשותם לפני גישה או קרבה פיזית למערכות מחשוב המנהלות / מבקרות חומרים מסוכנים.<br><br>18.7 עובד לא מרוצה / עובד ממורמר. יש לתת תשומת לב מיוחדת לעובד לא מרוצה / ממורמר ולצמצם הרשאות לוגיות על בסיס Need To Know בלבד וגישה פיסית על בסיס הנדרש לצורך הפעילות בלבד. | הערה: במידה והעבודה בעסק הינה סביב השעון 24/7 ועובדי העסק מאיישים את איזורי ארונות התקשורת, הבקרים ותחנות עבודה / HMI, אין חובה ליישם סעיפים 18.4 ו-18.5.<br><br>18.7 עובד לא מרוצה / עובד ממורמר אשר יש לו גישה פיסית ולוגית נרחבת יכול להוות פוטנציאל ל"איום פנימי". | 18.4 א. ניתן ליישם באמצעות הצבת מצלמות מול עמדות HMI או מצלמות בעלות עדשה נעה אשר סורקות גם את אזור עמדות ה-HMI ופנלים לוקליים.<br><br>ב. במידה וישנה התנגדות פנימית בעסק להצבת מצלמות מסיבות של שמירת הפרטיות, התנגדות וועדי עובדים וכדומה, יש ליישם בקרה מפצה אחרת בהתייעצות עם יחידת הסייבר בתעשייה של המשרד להגנת הסביבה אשר מהווה מענה חליפי והולם לבקרה זו.<br><br>18.6 מומלץ להחיל את הנוהל גם על עובדים, למעט מדיות ייעודיות המשמשות לעבודה בלבד.<br><br>18.7 מומלץ בתהליך גיוס עובדים במערכות קריטיות לעסק, לשלב בדיקות מהימנות ולאחד אותן אחת לתקופה על פי קביעת העסק. | 3 | 18.4-5 הצגת אמצעי האבטחה.<br><br>18.6 הצגת פעילות ההסברה שנעשתה בקרב העובדים והשומרים.<br><br>18.7 בדיקת הרשאות לוגיות והרשאות גישה.<br><br>18.7 הצגת תהליך בדיקת מהימנות. | 4 |

| סעיף | בקרה נדרשת | פירוט | המלצות / הערות | רמה | בדיקה | מס' הבקרות בפרק זה |
|---|---|---|---|---|---|---|
| 19 | **עובדים בעלי גישה למערכות מחשוב ואוטומציה המטפלות בחומרים מסוכנים**<br><br>19.1 יש להחתים את העובדים על הצהרת התחייבות להקפיד על דרישות אבטחת המידע של העסק, והצהרת סודיות לגבי מערכות המחשוב והבקרה של חומרים מסוכנים, רצפטים, תהליכי השימוש והלוגיסטיקה של חומרים מסוכנים בעסק.<br><br>19.2 יש להשעות גישה לעובדים אשר יש לגביהם חשש (ממורמרים, לא יציבים, לא מקפידים על הנחיות).<br><br>19.3 יש לבטל הרשאות גישה ולחסום חשבונות משתמש בעת סיום העסקה. כמו כן יש לדלל ולהתאים הרשאות במידת הצורך במקרה של שינוי תפקיד.<br><br>19.4 יש להנחות עובדים שלא לקבל הנחיות לביצוע פעולות במערכות המחשוב והבקרה של חומרים מסוכנים על פי הוראה שניתנה בדואר אלקטרוני / הודעת טקסט / שיחת טלפון / שיחת וידאו. | 19.1 חשיפת מידע אודות מערכות המחשוב והבקרה, רצפטים של הכנת חומרים כימיים המתקיימים בעסק (הן בערבוב הן בריאקציה), נוהלי לוגיסטיקה ורישום של חומרים מסוכנים בעסק - עלולה לאפשר לתוקף לתכנן ולבצע מתקפת סייבר שתגרום לאירוע חומרים מסוכנים.<br><br>19.3 לדוגמא עובד שקודם ממנהל בקרה שיש לו הרשאות גבוהות לניהול שאינו דורש הרשאות על מערכות, יש להסיר את הרשאותיו הקודמות ולתת לו הרשאות חדשות מתאימות.<br><br>19.4 יש לתוקפים יכולת זיוף דואר אלקטרוני, הודעות טקסט, התחזות בטלפון ואף בשיחת וידאו. | | 2 | 19.1-4 הצגת הפעילות שנעשתה בקרב העובדים. | 4 |

| סעיף | בקרה נדרשת | פירוט | המלצות / הערות | רמה | בדיקה | מס' הבקרות בפרק זה |
|---|---|---|---|---|---|---|
| 24 | **זיהוי וניהול אירועי סייבר למערכות מחשוב ואוטומציה המטפלות בחומרים מסוכנים**<br><br>24.1 על העסק להכין תכנית תגובה לאירוע סייבר במערכות ממוחשבות המנהלות/מבקרות חומרים מסוכנים. הנוהל יתורגל אחת לשנה לפחות.<br><br>24.2 במידה ואומת חשד לאירוע סייבר במערכות ממוחשבות המנהלות / מבקרות חומרים מסוכנים, יש לעדכן את יחידת הסייבר בתעשייה במשרד להגנת הסביבה או את מוקד מערך הסייבר הלאומי.<br><br>24.3 במידה ולאירוע הייתה השפעה על חומרים מסוכנים, ראשית יש לבצע את התהליכים/התרגולות הנדרשים, להזעיק רשויות ולעדכן את רכז החומרים מסוכנים של העסק כפי הנדרש בכל אירוע חומרים מסוכנים בעסק על פי כל דין.<br><br>24.4 יש לוודא כי נהלי/תרגולות העסק לאירוע חומרים מסוכנים כוללות התייחסות למצב שבו מערכות המחשוב והבקרה אינן מתפקדות כשורה.<br><br>24.5 במקרה של ארוע סייבר שעלול לגרום לארוע חומרים מסוכנים, על העסק לבנות נוהל של מעבר לעבודה ידנית ללא מערכות מחשוב או לניטרול מערכות המחשוב מניהול / בקרת החומרים המסוכנים, ולתרגל נוהל זה אחת לחצי שנה. | 24.1 הנוהל יתייחס לבירור ההתנהגות החשודה מול אנשי המקצוע בעסק ומחוצה לו, יידוע הנהלה, סמכות קבלת החלטה לניתוק רכיב/השבתת מערכת/ניתוק תקשורת עד לבירור העניין, בדיקות תקינות שיש לבצע ברכיבים אחרים.<br><br>24.2 העדכון יהיה לאחד מהגורמים הבאים לפי הסדר הבא:<br>א. מרכז הגנה ארצי של המשרד להגנת הסביבה socsviva@cyber.gov.il<br>ב. מוקד חירום של המשרד להגנת הסביבה בטל: 073-2733200 או: 6911*.<br>ג. יחידת הסייבר בתעשייה במייל: cyber_industry@sviva.gov.il<br>מוקד הסייבר הלאומי בטל' 119 (24/7) ובמייל: team@cyber.gov.il | 24.1 ניתן להפנות לנהלים קיימים להשבתת מערכת והחלפת רכיב מקולקל. | 1 | 24.1 הצגת הנהלים.<br><br>24.2 הצגת היסטוריית האירועים שהתגלו ודווחו.<br><br>24.3 הצגת אופן הטיפול באירועים שהשפיעו על חומרים מסוכנים. הצגת השינויים/התוספות לטיפול באירוע חומרים מסוכנים שנבע מפגיעת סייבר.<br><br>24.5 בדיקת הנוהל | 5 |
| | 24.6 על העסק להחזיק צוות IR בכוננות למקרה של צורך בהתערבות באירוע סייבר. | 24.6 רצוי לבצע תרגול מלא ככל האפשר. במידה ולא ניתן, יש יש לבצע תרגול מתודי מתוך הבנה שבזמן אמת ניתן להפוך את התרגול המתודי למצב מציאותי. במקרה של ארוע סייבר שעלול לגרום לאירוע חומרים מסוכנים לנסות ולמנוע ארוע חומרים מסוכנים | | 4 | | 1 |

| סעיף | בקרה נדרשת | פירוט | המלצות / הערות | רמה | בדיקה | מס' הבקרות בפרק זה |
|---|---|---|---|---|---|---|
| 25 | **תיקון וחזרה לפעילות לאחר אירוע סייבר**<br><br>25.1 יש לכתוב במסמך מדיניות אבטחת המידע תהליך ההתאוששות מאירועים - התוכנית תתחשב בתרחישי האסון השונים בחומרים מסוכנים (למשל לכמה זמן ניתן בבטחה להשבית בקר מסוים או מערכת HMI).<br><br>25.2 יש לוודא חזרה לשגרה על פי נוהל חזרה לשגרה.<br><br>25.3 במקרה של אירוע סייבר יש לעדכן מיידית את יחידת הסייבר בתעשייה במשרד להגנת הסביבה. כמו כן יש לדווח ולשלוח ליחידת הסייבר בתעשייה בתוך 60 יום מגילוי האירוע דוח אירוע סייבר (נספח ט' במדריך זה) המסכם את מהות האירוע, הכשלים שאפשרו אותו והלקחים שהופקו. | | 25.1 ניתן להפנות לנהלים קיימים להשבתת מערכת והחלפת רכיב מקולקל. | 2 | 25.1 הצגת הנהלים.<br><br>25.2 הצגת החלפים והגיבויים לצורך יכולת ההתאוששות.<br><br>25.3 הצגת מסמכי תחקיר לאירועים שהתרחשו. | 3 |
| | | | | | | 99 |

## נספח ד' - דרישות סף מיועץ חיצוני לעריכת סקר סיכונים בתחום הסייבר

1. דרישות סף בנושא השכלה:

אקדמאי בעל תואר ראשון בתחומים האלה (כתחום מקצוע עיקרי / משני / התמחות / שילוב בין תארים): מדעי המחשב / מערכות מידע / הנדסת תוכנה / הנדסת מחשבים / הנדסת אלקטרוניקה / מדעים מדויקים

או

תואר אקדמי אחר וכן הכשרות / הסמכות מקצועיות בהגנת סייבר בהיקף ניכר (400 שעות במצטבר)

או

בוגר יחידה טכנולוגית בצה"ל (ממר"ם, 8200, תקשוב ויחידות מקבילות) ו/או בראמ"ם ובלבד שעסק בתחום הטכנולוגי, כפוף לאישורים מתאימים.

או

השתתף בקורס סייבר לאנשי תעשייה בשיתוף המשרד להגנת הסביבה והתאחדות התעשיינים ו/או המשרד להגנת הסביבה בשיתוף עם כל גורם אחר באישור יחידת הסייבר בתעשייה של המשרד להגנת הסביבה.

2. **דרישות סף בנושא ניסיון:**

גיבוש, אפיון ומימוש תפיסות, שיטות ומתודולוגיות להגנת הסייבר בתשתיות הטכנולוגיות ומערכות המידע. הגדרת המתודולוגיות והתהליכים הארגוניים להגנה על תשתיות טכנולוגיות ומערכות המידע (כגון ליווי ובקרה בתהליך הקמת תשתיות ומערכות הגנת סייבר משרדיות, ליווי ובקרה של פרויקטים טכנולוגיים בהיבטי הגנת סייבר, אבטחת שרשרת האספקה בתשתיות מידע מפני איומי סייבר, המשכיות עסקית, התאוששות מאסון (DR) ועוד). בקרה ואכיפה מתודולוגית וטכנולוגית על תפעול הגנת הסייבר במערכות המידע. אחראי על הטמעת היבטי אסדרה ותקינה ישראלית ובין-לאומית והיבטי הגנת הפרטיות במערכות המידע בעסק.

וגם

ניסיון בעבודה ברצפת ייצור במערכות OT (Operation Technology), במסגרת פעילות במערכות ICS (Industrial Control Systems) כולל ניסיון במערכות סקאדה ו-HMI (Human-Machine Interface). תכנות בקרים, תכנון מערכת סקאדה, ביצוע שינויים במערכת HMI, ניטור התראות המתקבלות ממערכות HMI וטיפול בהן.

ניסיון של שש שנים בביצוע המטלות המתוארות בתפקיד, מהן שנתיים לפחות בניהול צוותים טכנולוגיים.

3. **דרישות נוספות בנושא השכלה, ניסיון, כישורים ומיומנויות (אם יש); יתרון:**

א. השכלה על תיכונית בתחום כימיה/הנדסה כימית, או הנדסת תעשייה, או מדעי טבע, או מנהל עסקים.

ב. היכרות מעשית עם מתודולוגיות הגנת סייבר בעולם תעשייתי - יתרון משמעותי.

ג. כתיבת מתודולוגיית הגנה על סייבר בעולם תעשייתי - יתרון משמעותי מאוד.

ד. ניסיון מעשי בתחום התעשייה הכימית - יתרון משמעותי.

ה. ניסיון כאיש מחשבים בתעשייה הכימית, בדגש על ניסיון במערכות בקרת תהליכים.

ו. ניסיון בהגדרת מדיניות ארגונית, כתיבת נהלים. ניסיון ביישום מסמכי מדיניות והנהלים.

ז. ניסיון בביצוע ביקורות אבטחת מידע.

ח. הכרת טכניקות הגנה וכלי אבטחת מידע במערכות SCADA.

## נספח ה' - כתב מינוי ממונה הגנת סייבר בעסק[7]

תאריך: _____

אל: _____ מס' ת"ז: _____

כתובת מייל: _____ מספר טלפון: _____

**הנדון: כתב מינוי ממונה הגנה בסייבר**

בהתאם לחוק חומרים מסוכנים התשנ"ג 1993 (להלן - "החוק"), ודרישות המפורטות בהיתר הרעלים, הריני למנותך לממונה הגנה על סייבר בארגוננו.

ממונה הגנה בסייבר יפעל בכפיפות ישירה לבעל היתר הרעלים.

תפקיד ממונה הגנה בסייבר יכלול:

1. גיבוש מדיניות הגנת סייבר בהתאם לתהליך ניהול סיכונים ארגוני ובהתאם לדרישות המפורטות בהיתר הרעלים ובמסמך ההנחיות.
2. בניית תוכנית עבודה להגנת סייבר על פי המדיניות.
3. בקרה ומעקב אחר ביצוע תוכנית העבודה ועמידה בתנאי היתר הרעלים בנושא הגנת סייבר.
4. פעילות בהיבטי הגנת סייבר בהתאם למסמך ההנחיות ועדכוני האבטחה השוטפים של יחידת הסייבר בתעשייה, המשרד להגנת הסביבה.

בברכה,

| שם מלא | תפקיד | חתימה וחותמת |
|---|---|---|

7 הממונה חייב להיות עובד העסק ולא עובד חיצוני

## נספח ו' - טופס מיפוי ראשוני של חומר מסוכן המנוהל/מבוקר ע"י מערכת ממוחשבת[8]

שם העסק: _____

שם המתקן: _____

| מס' | שם החומר | מס' CAS | מס' בהיתר רעלים | כמות מאושרת בהיתר רעלים | האם החומ"ס נכלל בתהליך המבוקר / משולב באופן מחשובי? | הסבר על התהליך המסוכן (שלבי התהליך, מטרותיו, אופן הביצוע) | פירוט מערכות מחשוב/ תהליך דיגיטלי המעורבים בתהליך המסוכן | פוטנציאל פגיעה בבריאות הציבור או בסביבה[9] |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

8 ימולא רק אם נערך סקר סיכוני סייבר עצמאי ללא ניהול סיכונים משולב

9 בהתאם לטבלת חישוב רמת הנזק במדריך זה

## נספח ז' - תצהיר בעל היתר הרעלים אודות ביצוע הערכת סיכוני סייבר וסיווג העסק

אני החתום מטה _____ , מס' זהות _____ , לאחר שהוזהרתי כי עלי לומר את כל האמת, וכי אם לא אעשה כן אהיה צפוי לעונשים הקבועים בחוק, מצהיר בזה לאמור:

1. הח"מ משמש כ _____ , בעבור _____ (שם העסק), מס' היתר רעלים _____.
2. תהליך סיווג העסק בעניין הגנת סייבר הסתיים ביום _____.
3. מצורף בזאת מסמך המפרט את עיקרי תוצאות הליך הסיווג של העסק והערכת סיכוני הסייבר.
4. ערכתי בעצמי/נעזרתי בשירותי חברת ייעוץ _____ (מחק את המיותר) את הערכת הסיכונים ואת מסמך עיקרי תוצאות הליך סיווג העסק והערכת הסיכונים, ולמיטב ידיעתי והבנתי מסמכים אלה הם מלאים, שלמים ונכונים, ונערכו לפי מסמך ההנחיות, ומציגים תמונת מצב מדויקת של העסק.
5. תהליך הערכת סיכונים ועריכת תוצאותיו בעניין הגנת הסייבר הסתיימו ביום _____ .
6. להלן תקציר תוצאות הערכת סיכונים:

| שם המערכת | רמת החשיפה (1-4) | רמת הנזק (1-4) | רמת הסיכון | חבילת בקרות להטמעה (1-4) |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |

7. ערכתי בעצמי/בדקתי (מחק את המיותר) את טבלת תקציר הערכת סיכונים המוגש למשרד להגנת הסביבה כנדרש בהנחיות, ולמיטב ידיעתי והבנתי התקציר מלא, שלם ונכון ומציג תמונת מצב מדויקת של העסק.
8. הנני מצהיר כי כל האמור אמת. חתימת המצהיר: _____

**אישור עו"ד**

אני החתום מטה _____ עורך דין, מאשר בזה כי ביום _____ הופיע לפני _____ המוכר לי אישית / שזיהיתיו על פי תעודת זהות מס' _____ ולאחר שהזהרתיו כי עליו לומר את האמת כולה ואת האמת בלבד, וכי יהיה צפוי לעונשים הקבועים בחוק אם לא יעשה כן, אישר נכונות הצהרתו לעיל וחתם עליה בפני.

חתימה וחותמת: _____

## נספח ח' - תצהיר בעל היתר רעלים על השלמת תוכנית למזעור סיכוני הסייבר

אני החתום מטה _____ , מס' זהות _____ , לאחר שהוזהרתי כי עלי לומר את כל האמת, וכי אם לא אעשה כן אהיה צפוי לעונשים הקבועים בחוק, מצהיר בזה לאמור:

1. הח"מ משמש כמנהל כללי / בעלים (מחק את המיותר), עבור _____ (שם המפעל), מס' היתר רעלים _____.
2. תהליך יישום תוכנית למניעת הסיכון לבריאות הציבור ולסביבה עקב אירוע סייבר, הושלם ביום _____.
3. להלן תקציר הטמעת בקרות למזעור סיכוני סייבר:

| שם המערכת | חבילת בקרות נדרשת (1-4) | רשימת הבקרות שהוטמעו | הערות |
|---|---|---|---|
| | | | |
| | | | |

4. בדקתי את מסמך הסיכום המוגש למשרד להגנת הסביבה כנדרש בהנחיות, ולמיטב ידיעתי והבנתי המסמך מלא, שלם ונכון.
5. הנני מצהיר כי כל האמור אמת. חתימת המצהיר: _____

### אישור עו"ד

אני החתום מטה _____ עורך דין, מאשר בזה כי ביום _____ הופיע לפני _____ המוכר לי אישית / שזיהיתיו על פי תעודת זהות מס' _____ ולאחר שהזהרתיו כי עליו לומר את האמת כולה ואת האמת בלבד, וכי יהיה צפוי לעונשים הקבועים בחוק אם לא יעשה כן, אישר נכונות הצהרתו לעיל וחתם עליה בפני.

חתימה וחותמת: _____

# נספח ט' - דוח אירוע סייבר[10]

| 1. פרטי איש קשר המדווח על האירוע: | |
|---|---|
| שם: | |
| תפקיד: | |
| טלפון: | |
| כתובת דואר אלקטרוני: | |

| 2. תיאור האירוע |
|---|
| תקציר האירוע: |

| 3. פרטים על האירוע | |
|---|---|
| תאריך ושעה שבה התגלה האירוע: | |
| סטטוס הטיפול באירוע | ☐ לא טופל<br>☐ תחילת טיפול - לא הסתיים<br>☐ הטיפול הסתיים |
| מיקום פיזי של האירוע | |
| מערכות שהושפעו מהאירוע | |
| האם גורמים נוספים מחוץ למפעל הושפעו מהאירוע (אם כן פרט)? | |

| 4. מידת הנזק / פוטנציאל הנזק: (סמן כל מה שנכון) |
|---|
| ☐ פגיעה במערכת מחשוב המנהלת/מבקרת חומרים מסוכנים ללא שחרור חומרים מסוכנים |
| ☐ פגיעה במערכת מחשוב המנהלת/מבקרת חומרים מסוכנים כולל שחרור חומרים מסוכנים שגרם לפגיעה בסביבה |
| ☐ פגיעה במערכת מחשוב המנהלת/מבקרת חומרים מסוכנים כולל שחרור חומרים מסוכנים שגרם לפגיעה בבריאות הציבור |
| ☐ לא ידועה מידת הנזק בשלב זה |
| תיאור מילולי קצר של הפגיעה: |

01 על עסק אשר קיבל תוספת תנאי סייבר בהיתר הרעלים חלה חובת דיווח אירוע בטופס זה.

| 5. אנשים שעודכנו באירוע | | |
|---|---|---|
| רשימת האנשים שעודכנו באירוע: | | |
| שם | תפקיד | טלפון |
| | | |
| | | |
| | | |

| 6. מה הצעדים שננקטו עד כה (מלא כל מה שנכון)? | |
|---|---|
| ☐ לא ננקט שום צעד בשלב זה | ☐ הלוגים של המערכות נשמרו לצורך תחקור |
| ☐ המערכות נותקה מרשת ה-OT | ☐ בוצע שחזור מגיבוי |
| ☐ נעשתה סריקה של המערכת לווירוסים | ☐ נעשתה פעולה אחרת (תאר מה נעשה) |
| תיאור מילולי קצר של הצעדים שננקטו: | |

| 7. נתונים נוספים / מידע נוסף שלדעתך חשוב לציין ולא נמצאים בטופס דוח אירוע |
|---|
| |

| 8. לקחים ומסקנות למניעת הישנות אירוע מסוג זה: | | |
|---|---|---|
| פעולות לביצוע | אחראי | לו"ז |
| | | |
| | | |
| | | |
| שם ומשפחה: | ת"ז: | חתימה: |
| | | |

## נספח י' – תצהיר בעל היתר רעלים על היעדר מערכות ממוחשבות המנהלות/מבקרות חומרים מסוכנים

אני החתום מטה _____ , מס' זהות _____ , לאחר שהוזהרתי כי עלי לומר את כל האמת, וכי אם לא אעשה כן אהיה צפוי לעונשים הקבועים בחוק, מצהיר בזה לאמור:

1. הח"מ משמש כ _____ , בעבור _____ (שם העסק), מס' היתר רעלים _____.
2. בצעתי הליך מיפוי החומרים המסוכנים ומצאתי כי כלל החומרים המסוכנים אינם מנוהלים/מבוקרים ע"י מערכות ממוחשבות, וכי לא קיימות במפעל מערכות ממוחשבות אשר פגיעה בהן עלולה לגרום לאירוע חומרים מסוכנים.
3. הליך המיפוי האמור בסעיף 2 לעיל הסתיים, ביום _____.
4. ידוע לי כי אם תתווסף מערכת ממוחשבת אשר תנהל או תבקר מערכות המכילות חומרים מסוכנים בעסק, אדרש לבצע הליך מיפוי מחודש ולפעול בהתאם לממצאי ההליך על פי תנאי היתר הרעלים.
5. הנני מצהיר כי כל האמור אמת.
חתימת המצהיר: _____

**אישור עו"ד**

אני החתום מטה _____ עורך דין, מאשר בזה כי ביום _____ הופיע לפני _____ המוכר לי אישית / שזיהיתיו על פי תעודת זהות מס' _____ ולאחר שהזהרתיו כי עליו לומר את האמת כולה ואת האמת בלבד, וכי יהיה צפוי לעונשים הקבועים בחוק אם לא יעשה כן, אישר נכונות הצהרתו לעיל וחתם עליה בפני.

תאריך: _____ חתימה וחותמת: _____

## נספח יא' - טופס הצהרת ספק המתחבר אל העסק מרחוק בדבר מחשב מעודכן ונקי מנוזקות

אני החתום מטה _____ מס' זהות _____

מצהיר/ה בזה לאמור:

1. המחשב שממנו אני מבצע/ת התחברות מרחוק אל רשת חברת_____ הוא:

א. מחשב בעל מערכת הפעלה בתוקף, נתמכת ומעודכנת בכל עדכוני האבטחה באופן שוטף.

ב. מחשב המכיל אנטי-וירוס בתוקף ומעודכן בעדכונים שוטפים.

2. המחשב שממנו אני מתחבר/ת אל חברת _____ נסרק ונבדק לגילוי נוזקות ונמצא נקי.

3. מטרת התחברותי מרחוק אל חברת: _____היא לצרכים האלה:

_____

_____

_____

_____

4. משך הזמן המוערך להתחברות הוא:_____

5. בסיום ההתחברות אני מתחייב/ת להודיע לנציג החברה על סיום התחברותי ולוודא ניתוק החיבור.

חתימה וחותמת: _____

# ניהול גרסאות המסמך

| גרסה | כתב | אישר | מהות השינוי | תאריך |
|---|---|---|---|---|
| 1.0 | יוסי שביט<br>ר' יחידת סייבר בתעשייה | גלעד בן ארי<br>ר' אגף חירום וסייבר | מסמך מקורי | 5/11/2019 |
| 1.1 | יוסי שביט<br>ר' יחידת סייבר בתעשייה | גלעד בן ארי<br>ר' אגף חירום וסייבר | שינוי בטבלת הבקרות | 11/12/2019 |
| 1.2 | יוסי שביט<br>ר' יחידת סייבר בתעשייה | גלעד בן ארי<br>ר' אגף חירום וסייבר | הוספת תצהיר, שינוי בטבלת הבקרות, תיקון טעויות סופר | 03/03/2020 |
| 1.3 | יוסי שביט<br>ר' יחידת סייבר בתעשייה | גלעד בן ארי<br>ר' אגף חירום וסייבר | הוספת נספח י"א | 17/5/2020 |
| 1.99 | יוסי שביט<br>ר' יחידת סייבר בתעשייה | לילך פדלון<br>ר' אגף חירום וסייבר | 1. שינוי תהליך המיפוי<br>2. הסרת נספח י"א שינוי וטיוב נספח ג' – רשימת בקרות נדרשות<br>4. הוספת בקרות 7.7, 9.7<br>5. שינוי וטיוב מילון מונחים | 31/5/2021 |
| 2.0 | יוסי שביט<br>ר' יחידת סייבר בתעשייה | לילך פדלון<br>ר' אגף חירום וסייבר | 6. הוספת בקרות 7.8, 18.1, 18.7, 24.5, 24.6<br>7. נספח י"א טופס הצהרת ספק המתחבר אל העסק | 28/11/2021 |

לפמ
נייר אקולוגי FSC
הפקה: אגף תקשורת דוברות והסברה, המשרד להגנת הסביבה

המשרד להגנת הסביבה
الوزارة لحماية البيئة
Israel Ministry of Environmental Protection
רחוב בנק ישראל 7, בניין ג'נרי 2, ירושלים 9195024
cyber_industry@sviva.gov.il 074-7675850/1/4.ט