



## תקנים ורגולציה באבטחת סייבר

מרחב הסייבר, כפי שהתפתח, הינו במידה רבה מרחב אזרחי. יש להגן עליו ולחסנו מפני פגיעה, אולם תוך שמירה על חיוניותו של המרחב כמנוע צמיחה וכמאפשר זרימה חופשית, ככל הניתן, של מידע, שירותים ומסחר.

אחד מצירי הפעולה בהם נוקטות מדינות וארגוני תקינה בינ"ל, הינו ביצירה ומיסוד של סטנדרטים מקצועיים בתחום ההגנה בסייבר והנחלת רגולציה שתכליתה העלאה שיטתית ורציפה של רמת ההגנה בארגונים השונים. זאת על מנת למנוע או לצמצם את פגיעותם לתקיפות סייבר.

בחלק זו קובצו מגוון מתוך הרגולציות, ההנחיות והתקנים הקיימים כיום בתחום אבטחת הסייבר, בדגש על התקנים הקיימים בישראל ובחלוקה למספר משפחות מרכזיות:

### **1. רגולציה, סטנדרטים ותקנים ברמה הארגונית**

מאמץ מרכזי ראשון בתחום הסטנדרטיזציה נוגע לתהליך אבטחת הסייבר בארגון. סטנדרט זה מחייב לרוב את הארגון לבצע תהליך מתודולוגי מוגדר ושקוף לניהול מערכת אבטחת הסייבר אצלו. כך לדוגמה, על הארגון להגדיר מדיניות, לקיים תהליכי הגדרת נכסי מידע, ניהול סיכונים ובניית תכניות עבודה להגנה מתוך גישה הממוקדת בטיפול בפערים ובשיפור תהליכים. העמידה בתקנים ארגוניים גורמת לעתים רבות למצב בו הארגון ממסד ומסדיר את פעילותו בתחום אבטחת הסייבר ובכך מטפלת באופן שיטתי ומוסדר יותר בסיכוני אבטחת המידע ובמענים הארגוניים הנדרשים.

#### **1.1. תקינה ורגולציה בישראל -**

##### **• תורת הגנה בסייבר לארגון**

הרשות הלאומית להגנת הסייבר גיבשה והפיצה טיוטה להתייחסות באפריל 2017. התורה נכתבה למען הארגונים במשק הישראלי, היא אמנם נסמכת במקורותיה על תקינה בינלאומית בנושא הגנה בסייבר, אך היא מהווה גיבוש של תפיסה המושתת ברובה על ניסיון וידע ישראלי ובראיית צרכי ומאפייני הארגונים במשק הישראלי. התורה תופץ בגרסתה הראשונה 1.0 ביולי 2017.

##### **• חוק המחשבים, התשנ"ה – 1995**

במסגרת הדין הפלילי חוק המחשבים מגדיר ומפרט את המושג עבירת מחשב ורף הענישה בגינה (בין 3-5 שנים). החוק מתייחס לעבירות של שיבוש ומחיקת מידע במחשב, חדירה למחשב בהתייחס לפרטיות והאזנת סתר, יצירת נוזקות וכדומה.

##### **• תקנות הגנת הפרטיות (אבטחת מידע) 7809, התשע"ז-2017**

שרת המשפטים במסגרת סמכותה לפי סעיף 36 לחוק הגנת הפרטיות, התשמ"א-1981 חתמה על תקנות הגנת הפרטיות (אבטחת מידע) 7809 המתייחסות למאגרי המידע בישראל, כולל מידע ביומטרי ומגדירות



את פעולות שיהיה על בעלי מאגרי המידע לבצע. **הרשות למשפט, טכנולוגיה ומידע** (רמו"ט) במשרד המשפטים אחראית לאכוף את יישום התקנות

#### • הוראת המפקח על הבנקים

כחלק מהוראות המפקח על ניהול בנקאי תקין אשר חלות על כל תאגיד בנקאי ישראלי ותאגיד שבשליטתו במישרין או בעקיפין, כהגדרתו בחוק הבנקאות, התשמ"א-1981. קיימות הוראות מספר 357 בנושא **"ניהול טכנולוגיית המידע"**, מספר 361 בנושא **"ניהול הגנת הסייבר"** מספר 355 בנושא **"ניהול המשכיות עסקית"**

#### • הוראה לניהול סיכונים אבטחת המידע של הגופים המוסדיים

משרד האוצר - אגף שוק ההון, ביטוח וחיסכון בתוקף סמכותו לפי החוק לפיקוח על שירותים פיננסיים (ביטוח), התשמ"א-1981. פרסם בשנת 2016 חוזר בנושא **"ניהול סיכונים סייבר בגופים מוסדיים"** החל על כל גוף המנהל כספים של הציבור, כגון כספי פנסיה וקרנות נאמנות כאשר הגופים המוסדיים המרכזיים בישראל הם חברות הביטוח ובתי השקעות.

#### • מכון התקנים הישראלי

אימץ חלק ממשפחת תקני 27000 של ארגון ISO (International Organization for Standardization) – ארגון התקינה הבינ"ל ו-IEC (International Electro-technical Commission) הנציבות הבינלאומית לאלקטרו-טכניקה, ארגון תקינה בתחום החשמל והאלקטרוניקה. בנספח א' מפורטים התקנים שאומצו.

### 1.2 תקינה בינלאומית

#### ISO/IEC 27000

משפחת תקנים של **ISO** (ארגון התקינה הבינ"ל) ו-IEC (הנציבות הבינלאומית לאלקטרו-טכניקה) העוסקת בניהול אבטחת המידע בארגון ומהווים מסגרת לבנית תכנית הגנה ושיטות עבודה מומלצות להגנה על המידע, קיימים לפחות 45 תקנים בתתי-תחומים תחת נושא זה. התקנים ברובם בתשלום. תקנים מובילים במשפחה הינם **ISO 27001** – המגדיר את עקרונות הקמת ניהול ותחזוקה של מערכת אבטחת מידע המתאימה לארגון ו-**ISO 27002** – מתכונת מומלצת למילוי דרישות תקן ISO 27001.

#### SOX

**חוק** אמריקני פדרלי (2002) החל על חברות הנתונות לפיקוח של רשות ניירות הערך האמריקאי ואומץ בחלקו גם בישראל. בסעיף 404 לאותו חוק נקבעה החובה להעריך את אפקטיביות הבקורות והנהלים, הן לגבי תפעול החברה והן לגבי הגילוי הנדרש בדוחות. חלק מהבקורות הנ"ל מתייחסות לנושא אבטחת המידע בארגון.



## PCI-DSS

[תקן](#) אבטחת המידע לסליקת כרטיסי אשראי. פורום של חמש חברות האשראי הבינלאומיות, התקן חל על כל גוף המעביר, מאחסן, מעבד או מכבד נתוני אשראי. מטרתו של התקן להגן על המשתמשים בכרטיסי האשראי מפני הונאות, גניבת זהות או גניבת כרטיסי אשראי והגנה על פרטיות המשתמשים.

## CSA

[Cloud Security Alliance](#) ארגון ללא מטרת רווח שמטרתו לקדם תכנית הגנה ושיטות עבודה מומלצות להגנה על שירותי "ענן", הארגון מקיים מעל 25 קבוצות חשיבה ומחקר בתתי-תחומים בנושא ההגנה על שירותי "ענן", לארגון תכנית הסמכה מובילה בשם (Security, Trust and Assurance Registry) [STAR](#) ומטריצת בקורות להגנה על שירותי "ענן" בשם [CCM](#).

## NIST

[The National Institute of Standards and Technology](#), המכון הלאומי (האמריקאי) לתקנים וטכנולוגיה מפרסם [מסגרות עבודה](#) ומפרסם כמות גדולה של [תקנים](#) בתחום הגנת המידע. ניתן לציין את [NIST Special Publication 800-53](#) העוסק בבקורות הגנה על מידע ופרטיות בארגונים ומערכות מידע ו- [NIST Special Publication 800-30](#) העוסק בניהול סיכונים.

## ITIL

[Information Technology Infrastructure Library](#) מתודה לניהול שירותי מערכות מידע, זהו אוסף של הנחיות כיצד יש לנהל את יחידת המחשב (IT) בכל ארגון, וכיצד לספק שירותי מערכות מידע שיעזרו לארגון לעשות עסקים. מתודת ITIL נכתבה על ידי OGC - משרד המסחר הבריטי, ומופצת בעולם על ידי פורום [ITSMF](#).

## CobIT

[Control Objectives for Information and Related Technologies](#) מסגרת עבודה ומערכת כלים התומכת בממשל טכנולוגיות המידע. המסייע ביישום נושא הניהול והבקרה של מערכות מידע ארגוניות, הני"ל במסגרת ארגון [ISACA](#) הפועל בתחומי הבקרה, הביקורת, האבטחה והממשל בסביבה של מערכות מידע וטכנולוגיות המידע.



- בנוסף קיימים תקנים נהלים ורגולציות בעיקר בעולם המערבי ארה"ב ואירופה הנהוגים ע"י הממשל, למשל בארה"ב בתחומי הבריאות [HIPAA-HHS](#) והביטחון [DHS-CYBERSECURITY](#) או במדינות האיחוד האירופי בתחום ההגנה על המידע והפרטיות [GDPR](#)

(The EU General Data Protection Regulation)

תקנים אלו ואחרים חלים גם על ארגונים וחברות הפועלים למשל ביצוא או ייצור מול מדינות בעלות תקינה ורגולציה מעין זאת.

## 2. רגולציה, סטנדרטים ותקנים עבור מוצרים ושירותים בתחום אבטחת הסייבר

מרכיב נוסף בתחום הרגולציה הינם התקנים והסטנדרטים המעידים על איכות מוצרי הגנת הסייבר המוטמעים במערכות הארגון ועל השירותים המסופקים לו.

תקן מקצועי נפוץ בעולם בתחום הינו תקן [Common Criteria](#) (שאומץ גם כתקן ישראלי - ת"י 15408 ISO) העוסק בהסמכת מוצרי אבטחת מידע וסייבר בהתאם לדרישות מקצועיות מוגדרות ולתהליך הכולל בדיקות מעבדה מוסמכת.

הסמכת המוצרים מתבצעת בהתאם למדרג של רמות בדיקה. יצרני תוכנה וחומרה המעוניינים בקבלת התקן נדרשים לפעול בהתאם לתהליך מוסדר ושיטתי מול גורמי הסמכה במדינות בהם קיימת מערכת לטיפול בתקן ומול מעבדות מוסמכות הבודקות את המוצרים בהתאם להגדרת דרישות אבטחה ברורות ובמתודה מוגדרת ומתועדת היטב.

קבלת התקן מעיד כי המעבדה שבדקה את המוצר מאשרת כי תכונות האבטחה הנדרשות במפרט הבדיקה נבדקו בהתאם לשיטה ולפרוטוקול הבדיקה שהוגדרו.

## 3. רגולציה, סטנדרטים ותקנים עבור אנשים (כוח האדם העוסק באבטחת סייבר)

המרכיב האחרון בתחום הרגולציה והסטנדרטים עוסק באנשי המקצוע. איוש אנשי מקצוע ברמה גבוהה בתחום זה ומתן סמכויות ומרחב פעולה מקצועי בתוך הארגונים הינו מרכיב קריטי במימוש ההגנה הארגונית בסייבר.

קיימים מודלים רבים להסמכת אנשי מקצוע בתחומים שונים: בעולם הרפואה נדרש כל רופא לעבור לימודים מקיפים והסמכה בטרם ייגש לטפל בחולים. בתחום עריכת הדין נדרשים אנשי המקצוע לבצע תקופת התמחות (סטאזי) ולעמוד בבחינות לשכה מסודרות. בתחום הסייבר המצב איננו כך, אך עם זאת קיימות הסמכות ידועות לאנשי אבטחת מידע וסייבר הניתנות ע"י גופים בעולם וכן מרכזים בארץ בתחומים כגון:

- הסמכות לגורמים בכירים – כגון מנהלי אבטחת סייבר, מנהלי סיכונים, תכנון מערכות אבטחה וכו'
- הסמכות למיישמים בתחום – העוסקים בהטמעה, התקנת מוצרים, תפעול, טיפול שוטף וכו'.



- הסמכות טכנולוגיות ייעודיות – כגון תחום החקירה הפורנזית, בדיקות חדירות וכו'.

לאחרונה, הוקמה וועדה ציבורית ע"י המטה הקיברנטי הלאומי, ובראשה עמד האלוף (במיל.) עמי שפרן שאמורה להגדיר את מקצועות אבטחת הסייבר ולקבוע הליכי הסכמה מתאימים לעוסקים בהם.

כיום קיימות הסמכות של ארגונים מסחריים כגון [ICS2](#), [SANS](#), או של יצרנים כגון Cisco, Microsoft ואחרים.

**האגף להסדרה והכשרה ברשות הלאומית להגנת הסייבר פועל בימים אלו להגדרת המקצועות בניית תכנית הכשרתם והתעדה שלהם במשק הישראלי.**



נספח א'

תקנים שאומצו על ידי מכון התקנים הישראלי

#	קבוצה	נושא / תת קבוצה	ת"י	שם התקן	התקן המאומץ	מהות התקן
1	השלמת סדרת ISO/IEC 27XXX	ניהול מערכת ארגונית	27010	טכנולוגיית המידע – טכניקות אבטחה – ניהול אבטחת מידע לתקשורת בין-מגזרית ולתקשורת בין-ארגונית  Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications	ISO/IEC 27010: 2012	תקן זה מספק קווים מנחים, בנוסף על ההנחיות המובאות בקבוצת התקנים הישראליים ת"י 27000 ( ISO/IEC 27000 family), ליישום ניהול אבטחת מידע בתוך קהילות שיתוף מידע.  תקן זה מספק בקורות והנחיות שקשורות באופן ספציפי לייזום, ליישום, לתחזוקה ולשיפור אבטחת מידע בתקשורת בין-ארגונית ובתקשורת בין-מגזרית.  תקן זה חל על כל שיטות החילוף והשיתוף של מידע רגיש, הן ציבורי והן פרטי, הן לאומי והן בין-לאומי, באותו ענף בתעשייה או באותו מגזר שוק או בין מגזרים. במיוחד, הוא עשוי לחול על החילוף ועל השיתוף של מידע הנוגע לאספקה, לתחזוקה ולהגנה על התשתיות החיוניות של הארגון או של המדינה.
2			27014	טכנולוגיית המידע – טכניקות אבטחה – ניהול אבטחת מידע  Information technology – Security techniques – Governance of information security	ISO/IEC 27014: 2013	תקן זה מספק הנחיות בנוגע למושגים ולעקרונות של ניהול אבטחת מידע, שבאמצעותם ארגונים יכולים להעריך, להפנות ולנטר את הפעילויות הקשורות לאבטחת המידע בתוך הארגון וליידע (communicate) עליהם.  תקן זה מתאים לארגונים מכל הסוגים והגדלים.
3			27032	טכנולוגיית המידע – טכניקות אבטחה – קווים מנחים לאבטחת סייבר  Information technology – Security techniques – Guidelines for Cybersecurity	ISO/IEC 27032: 2012	תקן זה מספק הנחיות לשיפור מצב אבטחת הסייבר, למעט ההיבטים הייחודיים של פעילות זו ואת התלות שלה בתחומי אבטחה אחרים, במיוחד את המפורט להלן:  - אבטחת מידע; - אבטחת רשת; - אבטחה באינטרנט (internet security); וכן - הגנה על תשתיות מידע קריטיות (CIIP).  תקן זה דן בנוהגי האבטחה הבסיסיים עבור גורמים במרחב הסייבר (Cyberspace). תקן זה מביא את המפורט להלן:  - סקירה כללית של אבטחת סייבר;  - הסבר על היחס בין אבטחת סייבר לבין תחומי אבטחה אחרים;



#	קבוצה	נושא / תת קבוצה	ת"י	שם התקן	התקן המאומץ	מהות התקן
						<p>- הגדרה של מחזיקי עניין ותיאור תפקידם באבטחת סייבר ;</p> <p>- הנחיות לטיפול בבעיות נפוצות באבטחת סייבר ; וכן</p> <p>- מסגרת שתאפשר למחזיקי עניין לשתף פעולה בפתרון בעיות באבטחת סייבר.</p>
4	אבטחת רשתות		2703 3 חלק 1	טכנולוגיית המידע - טכניקות אבטחה - אבטחת רשת : סקירה כללית ומושגים  Information technology -- Security techniques -- Network security: Overview and concepts	ISO/IEC  27033-1: 2009	<p>תקן זה מציג סקירה כללית של נושא אבטחת הרשת ושל ההגדרות הקשורות לכך. התקן מגדיר ומתאר את המושגים הקשורים לאבטחת רשת ומפרט הנחיות לניהול אבטחת רשת [אבטחת רשת ישימה לאבטחה של התקנים, לאבטחת פעילויות ניהול הקשורות להתקנים, ליישומים/שירותים ולמשתמשי קצה, נוסף על אבטחה של מידע המועבר בנתיבי התקשורת (communication links)].</p> <p>תקן זה רלוונטי לכל מי שמעורב בבעלות על רשת, בהפעלת רשת או בשימוש ברשת. אלה כוללים מנהלים בכירים ומנהלים אחרים או משתמשים שאינם טכניים, נוסף על מנהלים ומנהלים (administrators) הנושאים באחריות ספציפית לאבטחת מידע או/וגם לאבטחת רשת, להפעלת רשת, או האחראים על תוכנית האבטחה הארגונית הכוללת ועל פיתוחה של מדיניות האבטחה. התקן רלוונטי גם לכל מי שמעורב בתכנון, בתכן וביישום של ההיבטים הארכיטקטוניים של אבטחת הרשת. כמו כן, תקן זה :</p> <p>- מביא הנחיות כיצד לזהות ולנתח את סיכוני האבטחה ברשת, ומגדיר דרישות לאבטחת הרשת המבוססות על ניתוח זה ;</p> <p>- מביא סקירה של בקורות התומכות בארכיטקטורות אבטחה טכניות של הרשת ובקורות טכניות קשורות, וכן של בקורות שאינן טכניות ובקורות טכניות שישמות לא רק לרשתות ;</p> <p>- מציג דרכים להשגת ארכיטקטורות אבטחה טכניות לרשת באיכות טובה, ואת היבטי הסיכון, התכן והבקרה הקשורים לתרחישי רשת טיפוסיים ולאזורי "טכנולוגיה" ברשת (שנידונים בפירוט בחלקים האחרים של סדרת התקנים הישראליים ת"י 27033) ומתייחס בקצרה לנושאים הקשורים להטמעת בקורות אבטחת רשת והפעלתן, ולניטור ולסקירה רציפים של הטמעתן.</p> <p>באופן כללי, התקן מביא סקירה של סדרת התקנים הישראליים ת"י 27033 ו"מפת דרכים" לשאר חלקי הסדרה.</p>



#	קבוצה	נושא / תת קבוצה	ת"י	שם התקן	התקן המאומץ	מהות התקן
5			2703 3 חלק 2	טכנולוגיית המידע - טכניקות אבטחה - אבטחת רשת: קווים מנחים לתכן וליישום של אבטחת רשת	ISO/IEC 27033-2: 2012	תקן זה מציג קווים מנחים לארגונים לתכנון, ליישום ולתיעוד של אבטחת רשת.
6			2703 3 חלק 3	טכנולוגיית המידע - טכניקות אבטחה - אבטחת רשת: תרחישי רשתות מקושרות – איומים, טכניקות תכן וסוגיות בקרה	ISO/IEC 27033-3: 2010	תקן זה מתאר את האיומים, את טכניקות התכן ואת סוגיות הבקרה הקשורים לתרחישי רשתות מקושרות. עבור כל תרחיש, התקן מביא הנחיות מפורטות בנוגע לאיומי אבטחה, את השיטות לתכן האבטחה ואת הבקורות הנדרשות כדי לאפחת (mitigate) את הסיכונים הכרוכים בה. כאשר הדבר רלוונטי, התקן מאזכר את התקנים הישראליים ת"י 27033 חלקים 4 ו-5 ואת התקן הבין-לאומי ISO/IEC 27033-6, כדי להימנע מחזרה על תוכנם של מסמכים אלה.  המידע בתקן זה מיועד לשימוש בעת סקירת אפשרויות הארכיטקטורה/התכן של אבטחה טכנית ובעת בחירה ותיעוד של הארכיטקטורה/התכן של האבטחה הטכנית המועדפים ובקורות האבטחה הקשורות, לפי התקן הישראלי ת"י 27033 חלק 2. המידע המסוים שנבחר (יחד עם מידע שנבחר מהתקנים הישראליים ת"י 27033 חלקים 4 ו-5 ומהתקן הבין-לאומי ISO/IEC 27033-6) תלוי באופייני סביבת הרשת הנסקרת, כלומר – בתרחישים של הרשת ובנושאים הטכנולוגיים המסוימים הנוגעים בדבר.  בסיכומו של דבר, תקן זה יסייע במידה ניכרת להגדרה מקיפה וליישום של אבטחה עבור כל סביבת רשת של כל ארגון שהוא.
7			2703 3 חלק 4	טכנולוגיית המידע - טכניקות אבטחה - אבטחת רשת: אבטחת תקשורת בין רשתות באמצעות שערי אבטחה (Gateways)	ISO/IEC 27033-4: 2014	תקן זה מציג קווים מנחים לאבטחת תקשורת בין רשתות באמצעות שערי אבטחה (חומת אש, חומת אש של יישומים, מערכת הגנה חדירה וכדומה), בהתאם למדיניות אבטחת המידע המתועדת של שערי האבטחה, לרבות:  (א) זיהוי וניתוח של איומי אבטחה ברשת הקשורים לשערי אבטחה;  (ב) הגדרת דרישות אבטחת רשת ביחס לשערי





#	קבוצה	נושא / תת קבוצה	ת"י	שם התקן	התקן המאומץ	מהות התקן
				gateways		אבטחה המבוססת על ניתוח האיום ; ג) שימוש בטכניקות לתכן וליישום שמטרתם טיפול באיומים ובקרה על היבטים הקשורים לתרחישי רשת טיפוסיים ; וכן ד) טיפול בנושאים הקשורים ליישום, להפעלה, לניטור ולסקירה של בקורות שערי אבטחת רשת.
8			2703 3 חלק 5	טכנולוגיית המידע - טכניקות אבטחה - אבטחת רשת : אבטחת תקשורת בין רשתות באמצעות רשתות פרטיות וירטואליות (VPNs)  Information technology -- Security techniques -- Network security : Securing communications across networks using Virtual Private Networks (VPNs)	ISO/IEC 27033- 5: 2013	תקן זה מציג קווים מנחים לבחירה, ליישום ולניטור של הבקורות הטכניות הדרושות כדי לספק אבטחת רשת באמצעות חיבורי רשת פרטית וירטואלית (VPN) לקישור בין רשתות ולחיבור משתמשים מרוחקים לרשתות.
9	אבטחת יישומים		2703 4 חלק 1	טכנולוגיית המידע – טכניקות אבטחה – אבטחת יישומים : סקירה כללית ומושגים  Information technology – Security techniques – Application Overview and : security concepts	ISO/IEC 27034- 1: 2011	תקן זה מציג הנחיות המיועדות לסייע לארגונים לשלב אבטחה בתהליכים המשמשים לניהול היישומים שלהם.  תקן זה מציג סקירה כללית של אבטחת יישומים, הגדרות, מושגים, עקרונות ותהליכים המעורבים באבטחת היישומים.  תקן זה חל על יישומים שפותחו בתוך הארגון (in-house), על יישומים שנרכשו מצד שלישי וכן על יישומים שהפיתוח שלהם או שהפעלה שלהם נעשו במיקור חוץ.
10			2703 4 חלק 2	טכנולוגיית המידע – טכניקות אבטחה – אבטחת יישומים : מסגרת ארגונית נורמטיבית  Information technology -- Security techniques -- Application security : Organization normative framework	ISO/IEC 27034- 2: 2015	תקן זה מביא תיאור מפורט של מסגרת ארגונית נורמטיבית ומספק הנחיות לארגונים ליישומה.
11	מערכות IDPS		2703 9	טכנולוגיית המידע – טכניקות אבטחה – בחירה, פריסה והפעלה של מערכות מניעה וגילוי מְחַדָּר (IDPS)  Information technology – Security techniques –	ISO/IEC 27039: 2015	תקן זה מציג קווים מנחים המיועדים לסייע לארגונים בהיערכות לפריסה של מערכות מניעה וגילוי מְחַדָּר ( IDPS – intrusion detection and prevention systems). התקן דן במיוחד בבחירה, בפריסה ובהפעלה של מערכות מניעה וגילוי מְחַדָּר.



#	קבוצה	נושא / תת קבוצה	ת"י	שם התקן	התקן המאומץ	מהות התקן
				Selection, deployment and operations of intrusion detection and prevention systems (IDPS)		
12	אבטחת אחסון	27040	טכנולוגיית המידע – טכניקות אבטחה – אבטחת אחסון	Information technology – Security techniques – Storage security	ISO/IEC 27040: 2015	<p>תקן זה מציג הנחיות טכניות מפורטות כיצד יכולים ארגונים להגדיר רמה מתאימה של אפחות סיכונים (risk mitigation), על ידי שימוש בגישה מבוססת ועקבית (consistent) לתכנון, לתכן, לתיעוד ולמימוש של אבטחת אחסון נתונים. אבטחת אחסון חלה הן על הגנת המידע במקום שבו הוא מאוחסן והן על האבטחה של המידע המועבר באמצעות קישורים (communication links) הנוגעים לאחסון.</p> <p>אבטחת אחסון כוללת את האבטחה של ה־תקנים ושל מדיה, את האבטחה של פעילויות הניהול הנוגעות ל־תקנים ולמדיה, את אבטחת היישומים והשירותים ואת האבטחה הרלוונטית למשתמשי קצה במהלך מחזור החיים (lifetime) של ה־תקנים ושל המדיה ואחרי תום השימוש.</p> <p>אבטחת אחסון נוגעת לכל מי שיש בבעלותו התקני אחסון נתונים, מדיה ורשתות או לכל מי שקשור לשימוש ולתפעול שלהם – מנהלים בכירים, קניינים (acquirers) של מוצרי אחסון ושירותי אחסון, ומנהלים או משתמשים אחרים שאינם טכניים וכן מנהלים (managers) ומנהלים (administrators) – שיש להם אחריות ספציפית לאבטחת מידע או לאבטחת אחסון וכן לתפעול אחסון, או שהם אחראים על תוכנית האבטחה הכללית של ארגון ועל פיתוח מדיניות האבטחה בו.</p> <p>אבטחת אחסון גם נוגעת לכל מי שמעורב בתכנון, בתכן וביישום של היבטי הארכיטקטורה של אבטחת רשת אחסון.</p> <p>תקן זה מציג סקירה של מושגים והגדרות בתחום אבטחת אחסון. התקן כולל הנחיות הנוגעות להיבטים של האיום, התכן והשליטה הקשורים לתרחישי אחסון טיפוסיים ולתחומי טכנולוגיית אחסון. נוסף על כך, התקן מאזכר תקנים בין-לאומיים ודוחות טכניים אחרים המתייחסים לנהגים (practices) ולטכניקות הקיימים שניתן ליישם באבטחת אחסון.</p>
13	אבטחת	2703	טכנולוגיית המידע – טכניקות		ISO/IEC	תקן זה הוא חלק המבוא של סדרת התקנים



#	קבוצה	נושא / תת קבוצה	ת"י	שם התקן	התקן המאומץ	מהות התקן
		קשרי ספקים	6 חלק 1	אבטחה – אבטחת מידע לקשרי ספקים : סקירה כללית ומושגים	27036-1: 2014	הישראליים ת"י 27036. התקן מציג סקירה כללית של ההנחיות המיועדות לסייע לארגונים באבטחת המידע ובאבטחת מערכות המידע שלהם בהקשר של קשרי ספקים ( supplier relationships). התקן מציג גם מושגים שמתוארים בפירוט בחלקים האחרים של סדרת התקנים הישראליים ת"י 27036. תקן זה דן בנקודות המבט הן של הרוכשים והן של הספקים.
14			27036 חלק 2	טכנולוגיית המידע – טכניקות אבטחה – אבטחת מידע לקשרי ספקים : דרישות	ISO/IEC 27036-2: 2014	תקן זה מפרט דרישות אבטחת מידע יסודיות להגדרה, ליישום, להפעלה, לניטור, לסקירה, לתחזוקה ולשיפור קשרי ספק ורוכש.  דרישות אלה דנות ברכישה ובאספקה של מוצרים ושל שירותים, כגון ייצור או הרכבה, רכישה של רכיבי תוכנה וחומרה, רכישה של תהליך ידע, בנייה-הפעלה-העברה ושירותי מחשב ענן.  דרישות אלה מיועדות להיות ישימות לכל ארגון, ללא קשר לסוג הארגון, לגודלו ולאופיו.  כדי לעמוד בדרישות אלה, רצוי שהארגון יהיה כבר אחרי תהליך של יישום פנימי של מספר תהליכים יסודיים, או שהארגון יתכונן לעשות זאת באופן פעיל. תהליכים אלה כוללים, בין היתר, ניהול עסקי, ניהול סיכונים, ניהול תפעולי, ניהול משאבי אנוש ואבטחת מידע.
15			27036 חלק 3	טכנולוגיית המידע – טכניקות אבטחה – אבטחת מידע לקשרי ספקים : קווים מנחים לאבטחת שרשרת האספקה בטכנולוגיית המידע והתקשורת	ISO/IEC 27036-3: 2013	תקן זה מספק, לרוכשים ולספקים של מוצרים ושל שירותים לשרשרת האספקה בטכנולוגיית המידע והתקשורת (ICT), הנחיות על המפורט להלן:  (א) השגת נראות וניהול סיכונים אבטחת מידע הנגרמים עקב תפוצה פיזית ( physically dispersed) ורב-שכבתיות של שרשרת האספקה ב-ICT;  (ב) מענה עבור מוצרים ועבור שירותים ב-ICT לסיכונים הנובעים משרשרת האספקה העולמית ב-ICT, שיכולים להשפיע על אבטחת המידע בארגונים המשתמשים במוצרים ובשירותים אלה. סיכונים אלה יכולים להיות קשורים להיבטים ארגוניים וגם טכניים (כגון החדרת קוד זדוני או נוכחות של מוצרי



#	קבוצה	נושא / תת קבוצה	ת"י	שם התקן	התקן המאומץ	מהות התקן
						<p>טכנולוגיית מידע (IT) מזויפים);</p> <p>ג) שילוב תהליכים ונוהגים של אבטחת מידע בתהליכי מחזור החיים של המערכת ושל התוכנה, כמתואר בתקן הישראלי ת"י 15288 ובתקן הישראלי ת"י 12207, תוך תמיכה בבקורות אבטחת מידע, כמתואר בתקן הישראלי ת"י 27002.</p> <p>תקן זה אינו כולל נושאים של ניהול רציפות עסקית או של חוסן רציפות עסקית המעורבים בשרשרת האספקה של ICT. התקן הישראלי ת"י 27031 דן בהמשכיות עסקית.</p>
16		תחקור וראיות דיגיטליות	27037	טכנולוגיית המידע - טכניקות אבטחה - הנחיות לזיהוי, לאיסוף, לרכישה ולשימור של ראיות דיגיטליות	ISO/IEC 27037: 2012	<p>תקן זה מביא קווים מנחים לפעולות ספציפיות של טיפול בראיות דיגיטליות. פעולות אלה הן זיהוי, איסוף, רכישה ושימור של ראיות דיגיטליות (digital evidence) שעשוי להיות להן ערך ראיתי (evidential value). תקן זה מביא הנחיות למשתמשים יחידים בנוגע למצבים נפוצים שנתקלים בהם במשך תהליך הטיפול בראיות דיגיטליות, ומסייע לתהליכים בארגונים.</p> <p>תקן זה מציג הנחיות בנוגע להתקנים אוגם לפונקציות המפורטים להלן, שנעשה בהם שימוש בנסיבות שונות:</p> <ul style="list-style-type: none"> <li>- אמצעי אחסון דיגיטלי המשמשים במחשבים תקינים כגון כוננים קשיחים, תקליטונים, דיסקים אופטיים ומגנטיים-אופטיים, התקני נתונים עם פונקציות דומות;</li> <li>- טלפונים ניידים, סייעים דיגיטליים אישיים (PDA), התקנים אלקטרוניים אישיים (PED), כרטיסי זיכרון;</li> <li>- מערכות ניווט ניידות;</li> <li>- מצלמות תצלומים (סטילס) דיגיטליות ומצלמות וידאו (לרבות טלוויזיה במעגל סגור);</li> <li>- מחשב תקני עם חיבורי רשת;</li> <li>- רשתות מבוססות פרוטוקול TCP / IP ופרוטוקולים דיגיטליים אחרים;</li> <li>- התקנים עם פונקציות דומות לפונקציות הנזכרות לעיל.</li> </ul> <p>הערה 1: רשימת המכשירים שלעיל היא</p>



#	קבוצה	נושא / תת קבוצה	ת"י	שם התקן	התקן המאומץ	מהות התקן
						רשימה חלקית ואינה ממצה.  הערה 2: ישנן נסיבות שבהן ההתקנים המפורטים לעיל מתקיימים יחד בכמה צורות. לדוגמה, מערכת רכב עשויה לכלול מערכת ניווט ניידת, מערכת אחסון נתונים ומערכת חושית.
17		שירותי ענן	2701 7	טכנולוגיית המידע – טכניקות אבטחה – קובץ כללים לבקורות אבטחת מידע לשירותי ענן המבוססות על התקן הישראלי ת"י 27002  Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services	ISO/IEC 27017: 2015	תקן זה מציג קווים מנחים לבקורות אבטחת מידע החלים על התנאים ועל השימוש בשירותי ענן, באמצעות:  - הנחיות יישום נוספות לבקורות רלוונטיות המפורטות בתקן הישראלי ת"י 27002;  - בקורות נוספות עם הנחיות ליישום הנוגעות באופן ספציפי לשירותי ענן.  תקן זה קובע בקורות והנחיות ליישום הן עבור ספקי שירות ענן והן עבור לקוחות שירות ענן.
18			2701 8	טכנולוגיית המידע – טכניקות אבטחה – כללי יישום להגנה על מידע מזהה אישי (PII) בעננים ציבוריים הפועלים כמעבדי מידע מזהה אישי  Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	ISO/IEC 27018: 2014	תקן זה קובע יעדי בקרה, בקורות וקווים מנחים מקובלים נפוצים, עבור אמצעי יישום להגנה על מידע מזהה אישי (PII), בהתאם לעקרונות הפרטיות שבתקן הישראלי ת"י 29100 עבור סביבת מחשוב הענן הציבורי.  תקן זה מציין במיוחד קווים מנחים המבוססים על התקן הישראלי ת"י 27002, תוך התחשבות בדרישות האסֶדְרָה להגנה על מידע מזהה אישי (PII), אשר עשויות לחול בהקשר של סביבה (או סביבות) בעלות סיכוני אבטחת מידע של ספקי שירותי ענן ציבוריים.  תקן זה מתאים לארגונים מכל הסוגים והגדלים, לרבות חברות פרטיות וחברות ציבוריות, גופים ממשלתיים וארגונים ללא כוונת רווח, שמספקים לארגונים אחרים שירותי עיבוד מידע המוסדרים בחוזה, כמעבדי מידע מזהה אישי באמצעות מחשוב ענן.
19	פרטיות		2910 0	טכנולוגיית המידע – טכניקות אבטחה – מסגרת פרטיות  Information technology – Security techniques – Privacy framework	ISO/IEC 29100: 2011	תקן זה מציג מסגרת פרטיות אשר - מפרטת מינוח פרטיות משותף;  - מגדירה את המשתתפים (actors) ואת תפקידם בעיבוד מידע המאפשר זיהוי אישי (PII);  - מתארת שיקולי שמירת פרטיות; וכן



#	קבוצה	נושא / תת קבוצה	ת"י	שם התקן	התקן המאוץ	מהות התקן
						<p>- מביאה אזכורים לעקרונות פרטיות לטכנולוגיית מידע.</p> <p>תקן זה חל על אנשים ועל ארגונים המעורבים ברכישה, בעיצוב, בתכנון, בפיתוח, בבדיקה, בתחזוקה, בניהול ובהפעלה של מערכות או שירותים של טכנולוגיית המידע והתקשורת, שבהם נדרשות בקרות פרטיות לעיבוד מידע המאפשר זיהוי אישי (PII).</p>
20	אישור והסמכת מוצרי הגנה (משלים את Common Criteria (ISO/IEC 15408	1804 5	טכנולוגיית המידע – טכניקות אבטחה – מתודולוגיה להערכת אבטחה לטכנולוגיית המידע	Information technology – Security techniques – Methodology for IT security evaluation	ISO/IEC 18045: 2008	<p>תקן זה מהווה מסמך נלווה לסדרת התקנים הישראליים ת"י 15408 - "קריטריונים להערכת אבטחה לטכנולוגיית המידע". תקן זה מגדיר את הפעולות המינימליות שהמעריך נדרש כדי לבצע הערכה לפי סדרת התקנים הישראליים ת"י 15408, תוך שימוש בקריטריונים ובראיות ההערכה המוגדרים בתקן הישראלי ת"י 15408.</p>
21	הגנת מערכות תעשייתיות / SCADA	6244 3 חלק 1.1	רשתות תקשורת תעשייתיות – אבטחת רשת ומערכת: מונחים, מושגים ומודלים	Industrial communication networks - Network and system security Terminology, concepts and models	IEC/TS 62443-1-1: 2009	<p>תקן זה הוא מפרט טכני המגדיר את המונחים, את המושגים ואת המודלים עבור מערכות אוטומציה ובקרה תעשייתיות (IACS). התקן מניח את הבסיס לשאר התקנים בסדרת התקנים הישראליים ת"י 62443.</p> <p>את מהות התקן זה ניתן לתאר במונחים של טווח הפונקציונליות של מערכות המידע והאוטומציה של הארגון. פונקציונליות זו מתוארת בדרך כלל במונחים של מודל אחד או יותר.</p> <p>תקן זה מתמקד בעיקר באוטומציה ובקרה תעשייתיות. מערכות לוגיסטיות ותכנון עסקי אינן מטופלות באופן מפורש במסגרת תקן זה, אף שקיימת התייחסות לשלמות הנתונים המוחלפים בין המערכות העסקיות והתעשייתיות.</p> <p>אוטומציה ובקרה תעשייתיות כוללות את רכיבי הבקרה המפקחת שענפי התהליך כוללים בדרך כלל. אוטומציה ובקרה תעשייתיות כוללות גם מערכות SCADA (בקרה מפקחת ורכישת נתונים) שלרוב משמשות ארגונים הפועלים בענפי תשתית קריטית, לרבות אלה:</p> <p>(א) הולכת חשמל וחלוקתו ;</p> <p>(ב) רשתות חלוקת גז ומים ;</p> <p>(ג) תפעול הפקת נפט וגז ;</p> <p>(ד) צנרת להולכת גז ונוזלים.</p> <p>רשימה זו אינה רשימה סגורה. ניתן למצוא</p>



#	קבוצה	נושא / תת קבוצה	ת"י	שם התקן	התקן המאומץ	מהות התקן
						<p>מערכות SCADA גם בענפי תשתיות קריטיות ולא קריטיות אחרים.</p> <p>תקן זה מקיף את תחום מערכות האוטומציה והבקרה התעשייתיות (IACS) כולו, וחל על מערכות שביכולתן להשפיע על ההפעלה הבטוחה, המאובטחת והאמינה של תהליכים תעשייתיים. מערכות אלה כוללות, בין השאר:</p> <p>א) מערכות בקרה תעשייתיות ורשתות התקשורת הקשורות בהן, לרבות מערכות בקרה מבוזרות (DCSs), בקרים לוגיים מיתכנתים (PLCs), יחידות מסוף מרוחק (RTUs), התקנים אלקטרוניים חכמים, מערכות SCADA, חישה ובקרה אלקטרונית מרושתת, מערכות מדידה והעברת משמורת (custody) ומערכות ניטור ואבחון. (בהקשר זה, מערכות בקרה תעשייתיות כוללות פונקציות מערכת בקרת תהליך בסיסית ופונקציות מערכת בטיחות ממוכשרת (SIS), בין שהן נפרדות פיזית מהמערכת ובין שהן משולבות פיזית במערכת).</p> <p>ב) מערכות מקושרות - לדוגמה בקרה מתקדמת או רבת משתנים, רכיבי אופטימיזציה מקוונים, צגי ציוד ייעודיים, ממשקים גרפיים, רכיבי ניהול היסטוריה (process historians), מערכות ייצור, מערכות גילוי דליפה בצנרת, מערכות ניהול עבודה, מערכות ניהול הפסקת חשמל, ומערכות ניהול אנרגייה חשמלית.</p> <p>ג) ממשקים קשורים, כגון: ממשקים פנימיים, ממשקי אנוש, ממשקי רשת, ממשקי תוכנה, ממשקי מכונה או ממשקי התקן המאפשרים את הפונקציונליות של הבקרה, הבטיחות, הייצור, או ההפעלה מרחוק לתהליכים מתמשכים, לתהליכי אצווה, לתהליכים בדידים ולתהליכים אחרים.</p>
22			6244 3 חלק 2.1	רשתות תקשורת תעשייתיות – אבטחת רשת ומערכת: הקמת תוכנית אבטחה למערכת אוטומציה ובקרה תעשייתית	IEC 62443- 2-1: 2010	<p>תקן זה מגדיר את האלמנטים הנדרשים להקמת מערכת לניהול אבטחת סייבר (CSMS) למערכות אוטומציה ובקרה תעשייתית (IACS) ומציג הנחיות כיצד יש לפתח אלמנטים אלה. תקן זה משתמש בהגדרה הרחבה ובחלות רחבה של מה שמהווה מערכת אוטומציה ובקרה תעשייתית.</p> <p>אלמנטי המערכת לניהול אבטחת סייבר המתוארים בתקן זה קשורים בעיקר למדיניות, לנוהל, לנוהג ולכוח אדם, המתארים מה צריך להיכלל או מה רצוי שייכלל במערכת הסופית</p>





#	קבוצה	נושא / תת קבוצה	ת"י	שם התקן	התקן המאומץ	מהות התקן
				program		<p>לניהול אבטחת סייבר בארגון.</p> <p>ההנחיות בתקן כיצד לפתח מערכת לניהול אבטחת סייבר מובאות כדוגמה לאופן שבו ארגון עשוי לפעול לפיתוח האלמנטים ועשויות שלא להתאים לכל המקרים. המשתמשים בתקן זה נדרשים לקרוא בקפידה את הדרישות וליישם כראוי את ההנחיות כדי לפתח מערכת לניהול אבטחת סייבר שמתפקדת באופן מלא בארגון. את המדיניות ואת הנהלים שנידונים בתקן יש להתאים ספציפית לארגון.</p> <p>הערה: ייתכנו מקרים שבהם כבר קיימת מערכת לניהול אבטחת סייבר שאליה מוסיפים מערכת אוטומציה ובקרה תעשייתית, או שיתכנו ארגונים מסוימים שמעולם לא יצרו מערכת לניהול אבטחת סייבר באופן רשמי.</p>
23			62443-2-3	<p>רשתות תקשורת תעשייתיות – אבטחת רשת ומערכת: ניהול עדכונים בסביבת IACS</p> <p>Security for industrial automation and control Patch management : systems in the IACS environment</p>	IEC 62443-2-3:2010	<p>תקן זה, שהוא דוח טכני, מתאר דרישות לבעלי הנכס ולספקי מוצרים למערכת אוטומציה ובקרה תעשייתית (IACS) שהקימו תוכנית לניהול עדכונים במערכת אוטומציה ובקרה תעשייתית וכעת מתחזקים אותה.</p> <p>תקן זה ממליץ על תַּסְדִּיר (format) מוגדר להפצת מידע על עדכוני אבטחה מבעלי הנכס לספקי מוצרים למערכת אוטומציה ובקרה תעשייתית, על הגדרה של חלק מהפעילויות הקשורות לפיתוח של עדכוני המידע על ידי ספקי מוצרים למערכת אוטומציה ובקרה תעשייתית, ועל הפריסה וההתקנה של עדכונים על ידי בעלי הנכס.</p> <p>תקן זה אינו מבדיל בין עדכונים הזמינים עבור מערכות הפעלה (OSs), עבור יישומים או עבור הַתְּקָנִים. תקן זה אינו מבדיל בין ספקי המוצרים המספקים את רכיבי התשתית לבין יישומי מערכת אוטומציה ובקרה תעשייתית. תקן זה מביא הנחיות לכל העדכונים הישימים במערכת אוטומציה ובקרה תעשייתית. נוסף על כך, סוג העדכון יכול להיות עבור פתרון תקלים (bugs), עבור בעיות אמינות, עבור בעיות תפעוליות, או עבור פגיעויות אבטחה.</p>
24			62443-2-4	<p>אבטחה למערכות אוטומציה ובקרה תעשייתיות: דרישות לתוכנית אבטחה עבור ספקי שירות IACS</p> <p>Security for industrial automation and control</p>	IEC 62443-2-4:2015	<p>תקן זה מפרט דרישות ליכולות אבטחה עבור ספקי שירות IACS שיכולים להציע לבעל הנכס בזמן פעילויות כילול (integration) ותחזוקה של פתרון אוטומציה (Automation Solution).</p> <p>יכולות האבטחה המוצעות על ידי ספק שירות</p>





#	קבוצה	נושא / תת קבוצה	ת"י	שם התקן	התקן המאומץ	מהות התקן
				Security program : systems requirements for IACS service providers		IACS מאוזכרות כתוכנית האבטחה שלו.
25			62443 3 חלק 3.1	רשתות תקשורת תעשייתיות – אבטחת רשת ומערכת : טכנולוגיות אבטחה למערכות אוטומציה ובקרה תעשייתיות  Industrial communication networks – Network and Security : system security technologies for industrial automation and control systems	IEC 62443-3-1: 2009	<p>תקן זה מביא הערכה נוכחית של כלים שונים באבטחת סייבר, של אמצעי נגד לאפחות (mitigation) ושל טכנולוגיות שניתן להחיל אותן ביעילות על מערכות מודרניות אלקטרוניות המבוססות על מערכות אוטומציה ובקרה תעשייתיות (IACS) שמוסדות ומנטרות תעשיות ותשתיות קריטיות רבות. התקן מתאר מספר קטגוריות של טכנולוגיות אבטחת סייבר ממוקדות- מערכות בקרה, את סוגי המוצרים הזמינים בקטגוריות אלה, את היתרונות והחסרונות של השימוש במוצרים אלה בסביבות מערכות אוטומציה ובקרה תעשייתיות אוטומטיות, בכל הנוגע לאיומים הצפויים ולפגיעויות הסייבר הידועות, והחשוב מכול, את ההמלצות ואת ההנחיות הראשוניות לשימוש במוצרים אלה של טכנולוגיית אבטחת סייבר.</p> <p>המושג של אבטחת סייבר למערכות אוטומציה ובקרה תעשייתיות (IACS), כפי שחל בתקן זה הוא במונח הרחב ביותר, שמקיף את כל סוגי הרכיבים, המפעלים, המתקנים והמערכות בתעשיות ובתשתיות הקריטיות. מערכות אוטומציה ובקרה תעשייתיות כוללות, בין היתר, את המפורט להלן :</p> <p>א. מערכות חומרה (לדוגמה, שרתי נתונים היסטוריים ( data historian servers) ומערכות תוכנה (לדוגמה, מסדות הפעלה, תצורות, יישומים), כגון מערכות בקרה מבוזרת (DCSs), בקרים לוגיים מתכנתים (PLCs), מערכות בקרה לפיקוח ורכישת נתונים (SCADA), מערכות חישה אלקטרוניות מרושתות ומערכות לניטור, לאבחון, ולהערכה. בתחום החומרה והתוכנה נכללים גם רשת תעשייתית חיונית וכל הִתְקַנִי טכנולוגיית מידע (IT) וקישורים (links) המחברים או הקשורים שחיוניים להפעלה מוצלחת של מערכת הבקרה באופן כללי. כשלעצמו, תחום זה כולל, בין היתר : חומות אש, שרתים, נתבים, מתגים, שערים, מערכות שיש ממשק ביניהן ליחידות הקצה (fieldbus systems), מערכות לגילוי פריצות, התקנים אלקטרוניים/התקני קצה חכמים, יחידות מסוף מרוחקות (RTUs), והן</p>



#	קבוצה	נושא / תת קבוצה	ת"י	שם התקן	התקן המאומץ	מהות התקן
						<p>מודמים מרוחקים קוויים והן מודמים מרוחקים אלחוטיים.</p> <p>ב. ממשקים פנימיים, ממשקי אנוש, ממשקי רשת, או ממשקי מכונה קשורים המשמשים לבקרה, לרישום נתונים, לאבחון, לבטיחות, לניטור, לתחזוקה, להבטחת איכות, להתאמה לאסדרה, לביקורת ולטיפוסים אחרים של פונקציונליות תפעולית לתהליכים מתמשכים, לתהליכי אצווה, לתהליכים בדידים, ולתהליכים משולבים.</p> <p>באותו אופן, גם המושג של טכנולוגיות אבטחת סייבר ושל אמצעי נגד, מיושם באופן רחב (broadly applied) בתקן זה והוא כולל, בין היתר, את הטכנולוגיות המפורטות להלן:</p> <p>א. אימות והרשאה;                  ב. סינון, חסימה, ובקרת גישה;                  ג. הצפנה;                  ד. תיקוף נתונים;                  ה. ביקורת;                  ו. מדידה;                  ז. כלי ניטור וכלי גילוי;                  ח. מערכות הפעלה.</p> <p>נוסף על כך, טכנולוגיה שאינה סייבר – בקרת אבטחה פיזית – היא דרישה חיונית להיבטים מסוימים של אבטחת סייבר, והיא נידונה בתקן זה.</p> <p>מטרת תקן זה היא לסווג ולהגדיר טכנולוגיות אבטחת סייבר, אמצעי נגד, וכלים שזמינים כיום כדי לספק בסיס משותף לדוחות ולתקנים טכניים מאוחרים יותר שיופקו. כל טכנולוגיה בתקן זה נידונה במונחים של:</p> <p>א. פגיעויות אבטחה שנידונות על ידי הטכנולוגיה, הכלים, אוווגם אמצעי הנגד;                  ב. פריסה טיפוסית;                  ג. בעיות ידועות וחולשות ידועות;                  ד. הערכת השימוש בסביבת מערכות אוטומציה ובקרה תעשייתיות (IACS);                  ה. כיוונים עתידיים;                  ו. המלצות והנחיות;                  ז. מקורות מידע וחומר עזר.</p> <p>כוונת תקן זה היא לתעד את המצב העכשווי של טכנולוגיות אבטחת סייבר, של הכלים ושל אמצעי הנגד הישימים בסביבת מערכות אוטומציה ובקרה תעשייתיות (IACS), להגדיר בבירור אילו טכנולוגיות ניתן לפרוס כיום בצורה סבירה, ולהגדיר את התחומים שבהם ייתכן שיהיה צורך במחקר נוסף.</p>



#	קבוצה	נושא / תת קבוצה	ת"י	שם התקן	התקן המאומץ	מהות התקן
26			6244 3 חלק 3.3	רשתות תקשורת תעשייתיות – אבטחת רשת ומערכת: דרישות אבטחת מערכת ורמות אבטחה  Industrial communication networks – Network and System : system security security requirements and security levels	IEC  62443-3-3: 2013	<p>תקן זה מציג דרישות מערכת (SRs) טכניות מפורטות לבקרה, הקשורות לשבע דרישות היסוד (FRs) המתוארות בתקן הישראלי ת"י 62443 חלק 1.1, לרבות הגדרת הדרישות לרמות אבטחה וליכולת מערכת הבקרה.</p> <p>כמוגדר בתקן הישראלי ת"י 62443 חלק 1.1, קיימים בסך הכול שבע דרישות יסוד (FRs):</p> <p>(א) בקרת זיהוי ואימות (IAC),</p> <p>(ב) בקרת שימוש (UC),</p> <p>(ג) פְּלִילוּת מערכת (SI),</p> <p>(ד) חיסיון נתונים (DC),</p> <p>(ה) זרימת נתונים מוגבלת (RDF),</p> <p>(ו) זמן תגובה לאירועים (TRE), וגם</p> <p>(ז) זמינות משאב (RA).</p> <p>שבע דרישות אלה הן הבסיס לרמות אבטחה (SLs) ליכולת מערכת הבקרה, SL-C (מערכת בקרה). הגדרת יכולת אבטחה ברמת מערכת הבקרה היא המטרה והיעד של תקן זה.</p>
27	סדרת של 800 NIST	הערכת סיכונים	8003 0	מדריך לביצוע הערכת סיכונים  Guide for Conducting Risk Assessments	NIST SP 800-30: 2012	<p>מטרת תקן זה להציג הנחיות לביצוע הערכות סיכונים של מערכות מידע ארגוניות ושל ארגונים. הערכות סיכונים, המבוצעות בכל שלוש הדרגות שבמדרג ניהול סיכונים, הן חלק מתהליך ניהול סיכונים כולל – המספק לנושאי משרה/למנהלים בכירים את המידע הדרוש כדי לקבוע דרכי פעולה מתאימות כתגובה לסיכונים שזוהו. במיוחד, תקן זה מביא הנחיות לביצוע כל אחד מהשלבים בתהליך הערכת הסיכונים (למשל, בהכנה להערכה, בביצוע ההערכה, בדיווח תוצאות ההערכה, ובשמירה על ההערכה) וכיצד הערכות סיכונים ותהליכי ניהול סיכונים ארגוניים אחרים משלימים ומיישמים את זה. תקן זה גם מציג הנחיות לארגונים לזיהוי גורמי סיכון ספציפיים כדי לנטר באופן שוטף, כך שארגונים יכולים לקבוע האם הסיכונים גדלו לרמות שאינן קבילות (כלומר, הם חורגים מסבולת הסיכון הארגוני) ואילו דרכי פעולה שונות יש לנקוט.</p>
28		ניהול אירועים	8006 1	מדריך לטיפול באירועי אבטחת מחשב  Computer Security Incident	NIST SP 800-61:	<p>תקן זה נועד לסייע לארגונים בהפחתת הסיכונים מאירועי אבטחת מחשב באמצעות הצגת קווים מנחים מעשיים לתגובה אפקטיבית ויעילה לאירועים. התקן כולל</p>



#	קבוצה	נושא / תת קבוצה	ת"י	שם התקן	התקן המאומץ	מהות התקן
				Handling Guide	2012	קווים מנחים לקביעת תוכנית אפקטיבית של מענה לאירוע, אך מתמקד בעיקר בגילוי, בניתוח, בתעדוף ובטיפול באירועים. מומלץ שהארגונים יתאימו את הקווים המנחים ואת הפתרונות המומלצים לדרישות האבטחה ולדרישות המשימות הספציפיות שלהם.
29		מניעת תוכנות זדוניות במחשבים ובלפטופים	8008 3	מדריך לטיפול באירועי נזקה ולמניעתם במחשבים ניידים ובמחשבים ניידים  Guide to Malware Incident Prevention and Handling for Desktops and Laptops	NIST SP 800- 83: 2013	<p>תקן זה נועד לסייע למגוון רחב של ארגונים להבין את האיומים מנוזקות (malware), ולאפחח (mitigate) את הסיכונים הקשורים לאירועי נזקות. נוסף על הצגת הקטגוריות העיקריות של נזקות, התקן מביא הנחיות מעשיות ומציאותיות (real-world) למניעת אירועי נזקה ולמתן מענה לאירועי נזקה באופן אפקטיבי ויעיל. המידע המתואר בתקן זה נועד לשמש כנקודות נתונים (data points) שייכנסו לתהליך ניהול סיכונים גדול יותר.</p> <p>תקן זה מבוסס על ההנחה שלארגון כבר יש תוכנית למתן מענה כללי לאירוע וליכולת לבצע אותה. עבור מידע נוסף בנוגע למתן מענה כללי לאירוע ראו התקן הישראלי ת"י 80061, המשמש כבסיס לתקן זה.</p>
30	ניהול זהויות		2476 0 חלק 1	טכנולוגיית המידע: טכניקות אבטחה – מסגרת עבודה לניהול זהות: מונחים ומושגים  Information technology – Security techniques – A framework for identity management: Terminology and concepts	ISO/IEC 24760- 1: 2011	<p>תקן זה</p> <ul style="list-style-type: none"> <li>– מגדיר מונחים לניהול זהות, וגם מפרט מושגים עיקריים של זהות, של ניהול זהות ושל היחסים ביניהם.</li> <li>– תקן זה מתאים לכל מערכת מידע אשר מעבדת מידע על זהות (identity information).</li> </ul>
31			2476 0 חלק 2	טכנולוגיית המידע: טכניקות אבטחה – מסגרת עבודה לניהול זהות: ארכיטקטורת ייחוס ודרישות  Information technology – Security techniques – A framework for identity management: Reference architecture and requirements	ISO/IEC 24760- 2: 2015	<p>תקן זה</p> <ul style="list-style-type: none"> <li>– מציג קווים מנחים ליישום של מערכות לניהול של מידע על זהות (identity information), וגם מפרט דרישות ליישום והפעלה של מסגרת עבודה לניהול זהות.</li> <li>– תקן זה מתאים לכל מערכת מידע שבה מידע הנוגע לזהות מעובד או מאוחסן.</li> </ul>
32	טיפול בפגיעויות		2914	טכנולוגיית המידע – טכניקות	ISO/IEC	תקן זה מציג קווים מנחים לתהליך גילוי



#	קבוצה	נושא / תת קבוצה	ת"י	שם התקן	התקן המאומץ	מהות התקן
			7	אבטחה – תהליך גילוי פגיעות Information technology – Security techniques – Vulnerability disclosure	29147: 2014	<p>פגיעויות (vulnerabilities) אפשריות בשירותים מקוונים ובמוצרים. תקן זה מפרט את השיטות שבהן הספק (vendor) צריך להשתמש כדי לטפל בנושאים הקשורים לגילוי פגיעות. תקן זה:</p> <p>(א) מציג קווים מנחים עבור ספקים (vendors) המפרטים כיצד לקבל מידע על פגיעויות פוטנציאליות בשירותים המקוונים או במוצרים שלהם,</p> <p>(ב) מציג קווים מנחים עבור ספקים (vendors) כיצד להפיץ מידע המפרט את אופן הטיפול בפגיעויות פוטנציאליות בשירותים המקוונים או במוצרים שלהם,</p> <p>(ג) מציג את פריטי המידע שאמורים להיות מופקים כשהספק (vendor) מיישם את תהליך גילוי הפגיעות, וגם</p> <p>(ד) מציג דוגמאות של התוכן שאמור להיכלל בפריטי המידע.</p>



## נספח ב'

### קישורים ומידע נוסף

[NICCS – US National Initiative for Cybersecurity Careers and Studies](#)

[GIAC – Global Information Assurance Certification](#)

[IACRB – The Information Assurance Certification Review Board](#)

[ISACA – Information Systems Audit and Control Association](#)

[ISC2 – International Information System Security Certification Consortium](#)

[ECCouncil](#)