



## ניהול חוסן ביטחוני - תקן ישראלי



**מאת: ד"ר דן לנדא, מנהל תוכנית הגנת הסביבה של התעשייה האווירית. הוביל פיילוט ליישום התקן, יו"ר ועדת המומחים 181501 - מערכות ניהול ביטחון, במכון התקנים הישראלי**

### הקדמה

תופעת הטרור נגד אנשים ומוסדות קיימת מתקופות קדומות בהיסטוריה האנושית.

המיוחד לתקופתנו הוא זמינות יכולות ההרס בידי ארגונים קטנים ואף אנשים בודדים, היכולים לנצל את הקדמה הטכנולוגית כדי להגיע ליעדיהם ולגרור להם נזק קשה, לפעמים אנוש. התלות של מפעלים וארגונים בשרשרת הספקה מורכבת עשויה ליצור שרשרת נפץ שתגרור נזק רב הרחק מתחומי הארגון.

עקב כך נדרשים ארגונים בעולם להוכיח לבעלי העניין (Stakeholders) את יכולתם להתמודד בצורה סבירה עם איומים ביטחוניים - למניעת התרחשות של פעילות המסכנת את הארגון, ובמקרה של אי מניעת ההתרחשות - צמצום הנזקים וחזרה מהירה לפעילות. בין בעלי העניין ניתן למנות משקיעים, לקוחות, עובדי הארגון, הקהילה השכנה לארגון ועוד.

הצלחתם של תקני מערכות הניהול (ISO 14001, OHSAS 18001 ועוד) הציגה את היתרונות של הגישה המערכתית, המפעילה בצורה אפקטיבית ויעילה כלים ניהוליים להשגת יעדי הארגון. לאור הצלחה זו יזמה הקרן לשיתוף פעולה מדעי וטכנולוגי ארה"ב-ישראל (USISTF) בשיתוף עם מכון התקנים הישראלי (מת"י) תוכנית לכתיבה של תקן לניהול ביטחון ובחינה של יישומו במספר ארגונים. במסגרת פרויקט זה נכתבה טיוטת תקן המבוססת על התקן הבין-לאומי ISO 14001. הטיוטה נכתבה על ידי אנשי מקצוע מארה"ב וישראל. לאחר סיום כתיבת טיוטת התקן נערכו תוכניות פיילוט ליישום התקן בארגונים שונים: מפעלי תעשייה, בתי חולים, נמל נפט ועוד. מסקנות תוכניות הפיילוט עובדו, ולאורן נכתב תקן ישראלי הנמצא כיום בתהליכי אשרור (ת"י 24001).

מכון התקנים מעוניין לשכנע מכוני תקינה זרים לאמץ את התקן הישראלי, ולפיכך נכתב התקן במקורו באנגלית והוא יתורגם לעברית.

ההתבססות על ISO 14001 נבעה מהעובדות, שהוא כולל יסודות של ניהול סיכונים ושהוא יושם במספר גדול של ארגונים בעולם. כאן המקום להדגיש את החשיבות של בניית תקנים חדשים לפי תקנים קיימים, דבר שיקל על ההטמעה שלהם בארגונים.

### 1. יסודות התקן

בהתבסס על לקחי היישום של תקני הניהול קיימים, התקן החדש מדגיש את חשיבותה של מעורבות ומנהיגות מצד הנהלת הארגון. הנהלת הארגון חייבת להפעיל את המערכת, לקבל תמונת מצב על המצוי, הצפוי והרצוי, לקבוע מדיניות, להקצות את המשאבים המתאימים, לפקח על ביצוע תוכניות העבודה ולבחון מעת לעת את עדכניות המידע והתוכניות. הנהלת הארגון יש חשיבות בבניית התקשורת והעבודה המשותפת בין הגורמים המקצועיים בתוך הארגון ובין הארגון לגורמים חיצוניים.

### התקן מכיל את הגורמים האלה:

#### 1.1 ניהול הידע בארגון -

איסוף מידע, מיון המידע, אבטחתו (מפני השמדה או מפני חשיפה לגורמים לא מורשים), הפצתו והבטחת זמינותו לגורמים הזקוקים לו.

המידע כולל:

- תשתיות ונכסי הארגון;
- סיכונים ביטחוניים;
- מערכות הגנה ותגובה הקיימים בארגון ומחוצה לו;
- דרישות על פי דין ודרישות אחרות המוטלות על הארגון;
- דוחות, סיכומי דיון, נהלים והנחיות.

המורכבות של איומים ביטחוניים הולכת וגוברת. האיומים עשויים להיות בעלי אופי קונבנציונלי, כימי (עם אפשרות לשימוש במאגרי החומרים שבמפעל תעשייתי), ביולוגי (שימוש בחומרים הנמצאים בבתי חולים) ואף רדיולוגי. ההתמודדות עם איומים אלו דורשת התייחסות לתחום רחב של פעילויות במפעל בתחום התהליכים, הבינוי, ניהול המערכת הלוגיסטית ועוד. מערכת הידע חייבת לצבור ידע מחוץ למפעל ובתוכו ולהעבירו לכל הגורמים המקצועיים, אשר ביחד יתנו את הפתרון האופטימלי.

קצב איסוף ועיבוד המידע עשוי להיות מתחום של שנים ועד לתחום של זמן קצר ביותר, כאשר מדובר באיומים מידיים הדורשים תגובה.

### 1.2 ניתוח המידע

תוצאות עיבוד המידע יכולות להתבטא בתוכניות עבודה (בינוי, רכש ציוד, הדרכות, מבדקים וכד'), בכתיבה או בעדכון של הנחיות עבודה.

### 1.3 הפעלת המערכת

הפעלת פעילויות אד-הוק או פעילויות מתמשכות, עבודה בהתאם להנחיות, ניטור ומדידה, הפעלת כלי תקשורת בתוך הארגון ובין הארגון לגורמים חיצוניים, זיהוי ותיקון של אי התאמות. הפעלת המערכת יוצרת מידע שוטף, והוא מוזן לאותה מערכת ניהול המידע המתוארת בסעיף 1.1.

### 1.4 ביקורת ותיקון

תהליך בחינה של היעילות והאפקטיביות של המערכת: האם היא מביאה ליעדים שנקבעו על ידי ההנהלה? האם היא עושה זאת בצורה היעילה ביותר, תוך שימוש ותמיכה ביעדים אחרים של הארגון?

### 2. סעיפי התקן

התקן, כאמור, מבוסס על יסודות התקן הבין-לאומי ISO 14001. להלן פירוט סעיפי התקן:

#### 2.1 הגדרות

פרק זה כולל סדרת הגדרות, שחלקן מופיעות בתקן ISO 14001 וחלקן בתקנים לניהול סיכונים.

ההגדרה המשמעותית ביותר היא של המונח "ביטחון":

Security: protection from risks of unintentionally, intentionally, and naturally caused crises and disasters that disrupt and have consequences on the operation, critical assets, and continuity of the organization and its stakeholders.

הגדרה זו מרחיבה את תחולת התקן לטווח רחב של איומים, כולל אסונות טבע. עם זאת, התקן אינו מתייחס לסיכונים עסקיים.

ברקע של הגדרה זו הייתה התלבטות בין הרצון למקד את התקן בנושא מוגדר ובין הרצון לבנות תקן גנרי הניתן לשימוש במגוון איומים. היתרון של תקן גנרי הוא שימוש בשפה אחידה וניצול יעיל של כלי ניהול.



- מיד לאחר האירועים כאשר יש לייצב ולהחזיר לפעולה את המערכות הקריטיות לפעילות העסקית של הארגון;
- שלב השיקום של הארגון במטרה להחזירו לפעילות מלאה במהירות האפשרית.

התקן דורש מהארגון להכין תוכניות, ציוד, כוח אדם, הסכמי שיתוף פעולה, ערוצי תקשורת פנימיים וחיצוניים ועוד, במטרה להגיב בצורה הטובה ביותר לאירועי חירום. הארגונים נדרשים להביא בחשבון שיקולים של הקהילה העולה להיפגע מאירועי החירום, ובכלל זה צמצום ותיקון של פגיעה באיכות הסביבה.

### 2.6 משאבים, תחומי סמכות ואחריות

כדי שתוכניות יתבצעו יש צורך להקצות את המשאבים הנדרשים ולהגדיר את בעלי הסמכות והאחריות לביצוע התוכניות. הנהלת הארגון חייבת למנות נציג הנהלה אשר יקבל סמכויות ואחריות להפעלת המערכת, בחינת פעילותה ודיווח להנהלה על ביצועיה.

### 2.7 כישורים, הדרכות ומודעות

הארגון מזהה את הכישורים הנדרשים מבעלי התפקידים השונים ואת צרכי ההדרכה וההכשרה. תוכניות ההדרכה יתבססו בין השאר על:

- סקרי האיומים;
- תוכניות הפעולה;
- הנחיות להתנהגות ברגיעה ובמצבי חירום;
- הוראות הפעלה של ציוד שנרכש לפעילות שגרתית ולחירום, ועוד.

התקן מחייב להקנות לעובדים מודעות לתפקידם במערכת ניהול הביטחון, לחשיבות העמידה בהנחיות ולתוצאה של התנהגות לא תקינה.

### 2.8 תקשורת והתראה

הארגון מזהה את ערוצי התקשורת הדרושים לפעילות המערכת ובונה את התשתית הדרושה. קיימים מספר סוגי תקשורת הפועלים במערכת ניהול הביטחון:

- תקשורת שוטפת המיועדת להעביר ידע בין הגורמים השונים בארגון ובין הארגון לגורמים מחוצה לו;
  - תקשורת "דחופה" הפועלת במצבים חריגים - התראות, מידע בין כוחות הפועלים במצבי חירום ועוד.
- הארגון קובע את שיטת התקשורת ואת התשתיות הנדרשות. קביעת שיטת התקשורת במצבי חירום חייבת להביא בחשבון את האפשרות של קריסת תשתיות קיימות.

## 2.2 מדיניות

כתיבת המדיניות הינה התוויית הכיוון והיעדים של הארגון בידי ההנהלה. התקן מחייב הכללה של מספר מחויבויות בתקן, ובהן עמידה בדרישות על פי דין וקודים מקובלים לנושאי ביטחון וכן מחויבות לשיפור מתאים.

### 2.3 זיהוי איומים והערכת סיכונים

זיהוי סיכונים לחוסנו של הארגון ולבריאותם וחייהם של עובדיו. במסגרת התהליך ייבחנו תרחישי איום על פעילויות ונכסים קריטיים לארגון. מול כל תרחיש תיבחן ההסתברות למימושו והתוצאות של מימושו. תהליך זה יאפשר לזהות נקודות תורפה של הארגון, לדרג את האיומים ולקבוע דרכי פעולה למניעה או לצמצום של השפעה של האיומים המשמעותיים. התקן דורש להתייחס לתחום רחב של ההשלכות של התממשות תרחיש איום, לדוגמה: פגיעה בצוותי החירום שיפעלו במקרה של אירוע, השפעה של אירועי טבע על מערכות ההגנה והתגובה של הארגון, השפעה של אירוע על שרשרת ההספקה שהארגון מהווה גורם בה, ועוד.

### 2.4 דרישות על פי דין ודרישות אחרות

התקן דורש קיום מערכת המוודאת שהגורמים המתאימים בארגון מודעים לדרישות החוק ולדרישות אחרות (דרישות פנימיות של הארגון, דרישת לקוחות ועוד) מעודכנות, ושהם מקשרים את הדרישות לפעילויות הרלוונטיות של הארגון או לסיכונים שהארגון חשוף להם.

### 2.5 מטרות, יעדים ותוכניות

התקן קובע שרשרת של פעילויות המקשרות בין ההחלטות האסטרטגיות של הנהלת הארגון, לבין זיהוי הסיכונים ופעילויות המנע וצמצום הנזק. השיטה הנדרשת בתקן - של קביעת **מטרות** כלליות המבוססות על סקרי האיומים ומדיניות החברה, מעבר ל**יעדים** ממוקדים יותר ומהם **לפעילויות** - מוודאת שאכן הפעילויות הללו תואמות את האסטרטגיה של החברה והאיומים המשמעותיים על פעילותה. בתהליך הביקורת של האפקטיביות של הפעילויות ניתן לחזור אחורה ולבחון באיזו מידה הן השיגו את המטרות והיעדים ואת המדיניות של הארגון, והאם צמצמו את סיכוני הביטחון שהארגון עומד מולם. תוכניות הפעולה חייבות לכלול הגדרת תחומי סמכויות ביצוע, לוחות זמנים ותקציבים מאושרים על ידי ההנהלה.

### התקן מונה מספר סוגי תוכניות:

#### 2.5.1 תוכניות מניעה וצמצום נזקים

פרק זה בתקן דורש מהארגון לבחון את האפשרויות למניעת ההתממשות של תרחישי האיום המשמעותיים, ולחלופין לצמצם את הנזק שעלול להיגרם אם, למרות פעילויות המניעה, הם אכן יתממשו. בתהליך קביעת דרכי הפעולה ייבחנו אפשרויות שונות. המטרה היא להגיע לפתרון אופטימלי מבחינת רמת השיפור בביטחון, עלויות, התאמה למכלול היעדים של הארגון ועוד. דרכי הפעולה עשויות לכלול רכש והפעלת מערכות, ביצוע תוכניות הדרכה, השבתת פעילויות המהוות סיכון, הרחקת גורמים מסכנים מתחום הארגון ועוד.

#### 2.5.2 תוכניות תגובה והתאוששות

מטרת תוכניות אלה היא להכין את הארגון לאירועי חירום. התוכניות מטפלות בהתפתחות האירועים על ציר הזמן:

- בעת האירועים, כאשר יש לעצור את התפשטות ההרס ולהגן על חיי אדם;