תקן ישראלי
ת"י 1495
חלק 2

תמוז תשנ"ג
יוני 1993

מכון התקנים הישראלי
THE STANDARDS INSTITUTION OF ISRAEL

אבטחת מערכות מידע ממוחשבות - מצעים נושאי מידע

Information processing system security - Data Medium

מלות מפתח: עיבוד נתונים, טיפול במידע, אמצעי בטיחות, מצעים נושאי מידע.
Descriptors: data processing, information handling, safety measures, data media.

מיון עשרוני:
681.3

תוכן העניינים

0. הקדמה

תקן זה הוא חלק מסדרת תקנים הדנה באבטחת מערכות מידע ממוחשבות והכוללת עקרונות אבטחה, סיסמות, מצעים נושאי מידע, בקרת אירועים, התאוששות, ניהול הרשאות גישה, העתד וכדומה[1].

הסדרה דנה, בין היתר, באמצעים המיועדים להגן על מערכות אלה מפני סכנת פגיעה במידע מההיבטים של חשיפת המידע, שלמותו ושרידותו.

מטרת התקן לקבוע כללים לאבטחת מצעים לשם הנחיית הציבור ולהוות בסיס לקביעת נהלים פנימיים בארגון. בין היתר מיועד תקן זה לסייע ביישום הוראות חוק הגנת הפרטיות התשמ"א-1981 והתקנות שעל פיו.

1. תחום התקן

1.1 - תקן זה דן בכללי אבטחה של מצעים נושאי מידע מגנטיים או אופטיים, המכילים בדרך כלל מידע, המחייב התייחסות אבטחתית בכפוף לרמות אבטחה אלה: בסיסית, בינונית וגבוהה.

1.2 - תקן זה קובע אמות מידה אחידות ליישום אמצעי אבטחה של מצעים במערכות מידע ממוחשבות ובמקומות שבהם נמצאים מצעים, כגון: מתקני מחשב ומחשבים אישיים.

1.3 - התקן מיועד ליישום במערכות מידע בכל ארגון במגזרי המשק השונים בישראל.

1.4 - אין תקן זה בא לגרוע מהוראות כל דין.

2. אזכורים

תקנים ומסמכים המוזכרים בתקן זה:

תקנים ישראליים

ת"י 1243[2] - בטיחות אש של מחשבים וציודם ההיקפי

מסמכים ישראליים

חוק הגנת הפרטיות - ספר חוקים מ"א מס' 1011 מיום 11-3-1981.

3. הגדרות

ההגדרות שכוחן יפה בתקן זה:

3.1 - מצע נושא מידע (להלן: מצע) - מצע מגנטי או אופטי כגון: דסקה, דסקית, קלטת וסרט, המשמש להחסנה של מידע ממוחשב, להעברתו ולעיבודו.

3.2 - מצע בתולי - מצע שלא נרשמו עליו נתונים ושאין בו סימני תסדיר.

3.3 - מצע ריק - מצע שלא נרשמו עליו נתונים (המכיל סימני תסדיר בלבד).

3.4 - מצע נייד - מצע שניתן לטלטלו, כגון: דסקית, קלטת, דסקה נתיקה וסרט מגנטי.

3.5 - מצע קבוע - מצע שאינו נייד כשלעצמו.

3.6 - ספריית מצעים (להלן: ספרייה) - אוסף מצעים נושאי מידע, המשמשים קלט או פלט לעיבודים ממוחשבים, המוחסן ומנוהל במקום כלשהו.

---

(1) בעת הכנת תקן זה נמצאת הסדרה בהכנה.

(2) בעת הכנת תקן זה נמצא התקן הישראלי ת"י 1243 ברוויזיה.

3.7 – סימון מצע – רישום חיצוני על גבי המצע המאפשר את זיהויו באופן חד-משמעי. סימון זה מזהה את המצע גם בזמן המעקב.

3.8 – מחיקת מצע – מחיקת מידע מעל גבי מצע נושא מידע, באופן שלא יתאפשר שחזורו על-ידי תוכנה ועל-ידי אמצעי מחשוב רגילים. המחיקה מתבצעת באמצעות רישום של תווים אקראיים על גבי המצע עד סופו, במספר מחזורי כתיבה או באמצעות שימוש באלקטרומגנט.

3.9 – השמדת מצע – הוצאת מצע מכלל שימוש בשיטות כמו גריסה, שרפה או באמצעים פיסיקליים או כימיים אחרים.

4. מבנה התקן וצורת השימוש בו

4.1 – תקן זה כולל טבלות המפרטות כללים והנחיות לאבטחתם של מצעים בהתאם לשלוש רמות אבטחה: בסיסית, בינונית וגבוהה.

4.2 – רשימת הטבלות:

טבלה 1 – קבלת מצעים

טבלה 2 – ניהול מצעים (הקצאה ורישום)

טבלה 3 – טיפול במצעים לפי סיווגם

טבלה 4 – העברת מצעים

טבלה 5 – החסנת מצעים

טבלה 6 – השמדת מצעים

טבלה 7 – תחזוקת מצעים ותיקונם

טבלה 8 – ביקורת

הערה: דרישות לאבטחה פיסית של מצעים ראה התקן הישראלי ת"י 1243[2].

4.3 – בטבלות מופיעים הסימנים "+" (פלוס) או "-" (מינוס), המציינים צורך או העדר צורך לביצוע סעיף מסוים בטבלה כדי ליישם את רמת האבטחה הנדרשת.

4.4 – סיווג מידע או סיווג מערכת מידע ממוחשבת לאחת מבין שלוש רמות האבטחה ייקבע לפי העניין מתוקף הסכם או על-פי הוראת דין.

4.5 – ניתן לקיים בעת ובעונה אחת מספר רמות אבטחה או לקבוע רמת אבטחה אחידה לכלל המצעים בארגון בהתאם לסיווג היישום, שרמת אבטחתו הגבוהה ביותר.

5. <u>טבלות כללים והנחיות לאבטחת מצעים</u>

הארגון יקבע גורמים האחראים לביצוע פעולות ברמות אבטחה שונות כמפורט בטבלות.
בכל מקום בטבלות שיש בו התייחסות לגורם האחראי הכוונה לגורמים אלה.
בטבלות 1 ו-2 קיימת עמודה המתייחסת לסוג המצעים הרלוונטי.
בשאר הטבלות ההתייחסות היא לסוגי המצעים, כהגדרתם בסעיפים 3.4 ו-3.5.

5.1 - <u>טבלה 1 - קבלת מצעים</u>

מספר סעיף	כללים והנחיות	סוג המצע	ביצוע בהתאם לרמת האבטחה		
			בסיסית	בינונית	גבוהה
5.1.1	סימון מצעים בתולים בסימן מזהה של הארגון	נייד	-	+	+
5.1.2	קבלה, קיטלוג ורישום המלאי של מצעים (בתולים ונושאי מידע) למיניהם השונים (ראה סעיף 3.1)	נייד וקבוע	+	+	+
5.1.3	סימון המצעים למיניהם בסימון מזהה חד-ערכי	נייד	+	+	+
5.1.4	בדיקת מצעים נכנסים (ריקים ונושאי מידע) בעת קבלתם, כדי לוודא שאינם מכילים רכיבי תוכנה הרסניים, כגון וירוסים	נייד וקבוע	+	+	+
5.1.5	הפרדה בין מצעים המיועדים לשימוש פנימי לבין מצעים המיועדים להעברת מידע לגורמי חוץ	נייד	-	-	+
5.1.6	הפרדה בין מצעים של גורמי חוץ שונים הנכנסים לארגון	נייד	-	-	+

5.2 - טבלה 2 - ניהול מצעים (הקצאה ורישום)

מספר סעיף	כללים והנחיות	סוג המצע	ביצוע בהתאם לרמת האבטחה		
			בסיסית	בינונית	גבוהה
5.2.1	רישום מצעים ומעקב אחריהם ביומני מעקב בשתי רמות רישום: ברמת הספרייה - (בארגון שקיימת בו ספרייה) ינוהל רישום של הקצאת המצעים ותנועתם ברמת היישום - ינוהל רישום לגבי נושא תכולת המצעים	לגבי דסקיות מספיקה רמת הספרייה	- -	+ +	+ +
5.2.2	רישום ביומן המעקב ברמת היישום יכלול את הנתונים האלה: סוג המצע (ראה סעיף 3.1), זיהויו, מיקומו, נושא תכולתו ורמות סיווגו הערות: א. ביומן המעקב תישמר ההיסטוריה של רמות סיווג המצע ב. אפשר לנהל יומן בצורה ממוכנת	נייד וקבוע	+	+	+
5.2.3	רישום ביומן המעקב (הספרייה) של מצעים המועברים לגורמים מחוץ לארגון יכלול, נוסף על הפרטים המוזכרים בסעיף 5.2.2, גם את הפרטים האלה: הגורם שאליו הועבר המצע, תאריך ההעברה, פרטי המעביר, פרטי המקבל ואישור הקבלה היומן ישקף את מיקום המצע בכל עת	נייד וקבוע	+	+	+
5.2.4	רישום ביומן המעקב (הספרייה) של מצעים המועברים לגורמים אחרים בתוך הארגון יכלול, נוסף על הפרטים המוזכרים בסעיף 5.2.2, גם את הפרטים האלה: הגורם שאליו הועבר המצע, תאריך ההעברה, פרטי המעביר, פרטי המקבל ואישור הקבלה היומן ישקף את מיקום המצע בכל עת	נייד וקבוע	-	-	+
5.2.5	סיווג יומן המעקב ואבטחת הגישה אליו	-	+	+	+
5.2.6	סימון חיצוני של פרטי מצע, באופן שיאפשר את זיהויו	נייד	-	+	+
5.2.7	קביעת נוהל להקצאה מחדש של מצעים (ראה סעיף 5.3)	נייד וקבוע	-	+	+

5.3 - טבלה 3 - טיפול במצעים לפי סיווגם

מספר סעיף	כללים והנחיות	ביצוע בהתאם לרמת האבטחה		
		בסיסית	בינונית	גבוהה
5.3.1	סיווג המצעים בהתאם לרגישות המידע המצוי בהם	+	+	+
5.3.2	הורדת רמת סיווג המצע לרמת סיווג נמוכה יותר באישור הגורם האחראי לכך	-	+	+
5.3.3	שמירת רמת הסיווג של מצע שהתקבל מגורם חוץ באותה רמת סיווג	+	+	+
5.3.4	אישור הקצאה מחדש של מצעים המיועדים לשימוש חוזר בתוך הארגון, בהתאם לרמת סיווגם	-	-	+
5.3.5	איסור הקצאה מחדש של מצעים המיועדים לשימוש חוזר מחוץ לארגון, בהתאם לרמת סיווגם	-	+	+
5.3.6	הקצאת מצע נושא מידע לשימוש חוזר בתוך הארגון מחייבת מחיקת המצע במלואו	-	+	+
הערה: ברמת אבטחה גבוהה אין שימוש חוזר במצע הנושא מידע חסוי.				

5.4 – טבלה 4 – העברת מצעים

מספר סעיף	כללים והנחיות	ביצוע בהתאם לרמת האבטחה		
		בסיסית	בינונית	גבוהה
5.4.1	קביעת נהלים כתובים להעברת מצעים בהתאם לרמות האבטחה. נוהל העברת מצעים יכלול התייחסות לנושאים אלה: 5.4.1.1 – אבחנה בין העברה בתוך הארגון לבין העברה אל מחוץ לארגון 5.4.1.2 – אבחנה לפי רמת רגישות המידע 5.4.1.3 – אבטחת הגעת החומר ליעדו כשהוא תקין (אמצעי ליווי, כגון: נשק) 5.4.1.4 – פירוט אמצעי אריזה להגנת המצע מפני פגיעות, כגון: מכניות, אלקטרומגנטיות, טמפרטורה ולחות 5.4.1.5 – קביעת תחומי אחריות ופעילות לגורמים האחראים לביצוע ההעברה 5.4.1.6 – קבלת אישורים מתאימים 5.4.1.7 – מסירת מצעים לגורם אחראי המוסמך לקבלם ואישורו	–	+	+
5.4.2	רישום העברות ביומני המעקב בהתאם לסעיף 5.2	–	+	+
5.4.3	איסור העברת מצעים שהתקבלו מגורמי חוץ לגורמי חוץ אחרים	+	+	+

5.5 – טבלה 5 – החסנת מצעים

מספר סעיף	כלליים והנחיות	ביצוע בהתאם לרמת האבטחה		
		בסיסית	בינונית	גבוהה
5.5.1	החסנת מצעים בתנאי החסנה התואמים את דרישות היצרן ודרישות ת"י 1243	+	+	+
5.5.2	קביעת הוראות שמירה של מצעים והחסנתם על-פי סיווג המידע שבהם	+	+	+
5.5.3	קביעת הוראות שמירה של מצעי העתד והחסנתם	+	+	+
5.5.4	הפרדה בהחסנה בין מצעים המיועדים לשימוש בארגון לבין מצעים המיועדים להעברה לגורם חוץ	–	–	+

5.6 - טבלה 6 - השמדת מצעים

מידע רשום על גבי מצע אינו ניתן להימחק מחיקה מוחלטת עקב תכונותיו הפיסיות והכימיות של החומר שממנו עשוי המצע. שיטת רישום על רשום אינה מעלימה תמיד את המידע הקיים על מצע. אמצעים טכניים מאפשרים שחזור וקריאה אחורנית כמה דורות של מידע הרשום על המצע.

מספר סעיף	כללים והנחיות	ביצוע בהתאם לרמת האבטחה		
		בסיסית	בינונית	גבוהה
5.6.1	קביעת נוהל השמדת מצעים לסוגים המצויים בשימוש הארגון	-	+	+
5.6.2	קביעת רמת הסיווג של המצע, שמתחתיה אין צורך להשמידו, והשמדת מצעים מעל רמת סיווג זו	-	+	+
5.6.3	השמדת מצע פגום שאינו ניתן לתיקון (ראה סעיף 5.6.2)	-	+	+
5.6.4	השמדת מצע שאין לארגון צורך בו (ראה סעיף 5.6.2)	-	+	+
5.6.5	ההשמדה תלווה בטפסים, ברישום מתאים ביומני מעקב וברישום המלאי	-	+	+
5.6.6	פיקוח על ההשמדה וקביעת אמצעי בקרה, שיבטיחו ביצוע ההשמדה במלואה ובאופן בלתי הפיך	-	+	+

5.7 - טבלה 7 - תחזוקת מצעים ותיקונם

מספר סעיף	כללים והנחיות	ביצוע בהתאם לרמת האבטחה		
		בסיסית	בינונית	גבוהה
5.7.1	קביעת קריטריונים לסיווג המעבדה לתיקון מצעים	-	+	+
5.7.2	קביעת מעבדות מאושרות לתיקון מצעים, שיתאימו לרמת הסיווג של המצע	-	-	+
5.7.3	תיקון מצעים במקומות המאושרים לתיקון בהתאם לרמת הסיווג של המצעים	-	+	+
5.7.4	קביעת הסדר בין ספק לבין ארגון לגבי החזרה או אי-החזרה של מצע שנרשם עליו מידע, בין אם המצע מושכר, מושאל או קנוי ונמצא בתקופת אחריות	-	+	+
5.7.5	מצע אשר יועבר לספק לצורך בדיקתו או תיקונו, יימחק טרם מסירתו הערה: מצע ברמת אבטחה גבוהה לא יועבר לספק בשום מקרה	-	+	+

5.8 – טבלה 8 – ביקורת

מטרת הביקורת להבטיח שמירה על רמת האבטחה שנקבעה למצעים.

מספר סעיף	כללים והנחיות	ביצוע בהתאם לרמת האבטחה		
		בסיסית	בינונית	גבוהה
5.8.1	עריכת ביקורת באופן מחזורי לפחות אחת לשנה	+	+	+
5.8.2	עריכת ביקורת רישום מלאי כדי לוודא התאמת מצעים במתקן בהתאם לרישומים	–	+	+
5.8.3	עריכת ביקורת על עדכנות הנהלים ואופן אבטחת מצעים כדי לבדוק את דרך יישום ההנחיות המפורטות בתקן זה	–	+	+
5.8.4	עריכת ביקורת מעקב לתיקון הליקויים	–	+	+
5.8.5	העברת ממצאי הביקורת לגורמים האחראים בהנהלת הארגון	+	+	+

רשימת מונחים

דסקה	–	(magnetic) disk
דסקית	–	flexible disk
החסנה	–	storage
העתד (גיבוי)	–	back-up
מחיקה	–	erasing
מצע	–	medium
מצע בתולי	–	virgin medium
מצע ריק	–	empty medium
תסדיר	–	format

בהכנת תקן זה השתתפו נציגים אלה:

אוניברסיטת תל-אביב	- א' קפלן
איגוד הבנקים בישראל	- נ' בר-אל
איל"א - איגוד ישראלי לעיבוד אינפורמציה	- א' אבנר, א' הים
איגוד מנתחי מערכות	- י' קורפל
הרשות המרכזית לצרכנות	- ח' נוריאל
התאחדות התעשיינים בישראל	- מ' שפר
התעשייה האווירית לישראל	- ש' רפאל
יבמ ישראל בע"מ	- מ' קורנר
משרד המשפטים	- ש' בר-סלע
משרד ראש הממשלה	- נ' זיגרט
צבא ההגנה לישראל (ממר"ם)	- ז' תמיר

תקן זה הוכן על-ידי ועדת מומחים בהרכב זה:

י' וינר (יו"ר), א' קפלן

כמו כן תרמו להכנת התקן: ל' חורב, ב' תאזיני, מ' דישון, ש' בוגנים, מ' שטנדל, א' רבר, ר' קלדרון-הים, צ' אילני

א' אבנר היה יושב ראש הוועדה הטכנית

מ' אורלובה היתה רכזת הוועדה הטכנית

התקנים הישראליים עומדים לבדיקה מזמן לזמן, ולפחות אחת לחמש שנים, כדי להתאימם להתפתחות המדע, הטכניקה והתעשייה.

המשתמשים בתקנים יוודאו, שבידיהם המהדורה המעודכנת של התקן על גיליונות התיקון שלו.

הצעות לשינויים יש לשלוח לפי כתובת מכון התקנים הישראלי.

מכון התקנים הישראלי

רח' חיים לבנון 42, תל-אביב 69977

SI 1495 part 3

תקן ישראלי ת"י 1495 חלק 3

June 2008

סיוון התשס"ח - יוני 2008

ICS CODE: 13.310

35.020

אבטחת מערכות מידע ממוחשבות - שימוש בסיסמות

Information processing system security - The use of passwords

מכון התקנים הישראלי
The Standards Institution of Israel

רח' חיים לבנון 42, תל-אביב 69977, טל' 03-6465154, פקס' 03-6412762, www.sii.org.il

תקן זה הוכן על ידי ועדת המומחים בהרכב זה:
משה שפר (יו"ר), דורון שקמוני, רחל יעקבי, אורן פז, שי זנדני

תקן זה אושר על ידי הוועדה הטכנית 2114 - אבטחת מידע, בהרכב זה:

איגוד האינטרנט הישראלי	-	דורון שקמוני
איגוד לשכות המסחר בישראל	-	אברהם פרחיה
איגוד תעשיות האלקטרוניקה והמידע	-	מירון קורנר, שמעון סימן טוב
איל"א	-	אורן פז (יו"ר)
בנק ישראל - הפיקוח על הבנקים	-	רחל יעקבי
האיגוד הישראלי לביקורת ואבטחת מידע	-	משה שפר
לשכת מנתחי מערכות מידע	-	נעמי אברמסון, שי זודני
מכון התקנים הישראלי - אגף התעשייה	-	אילן כרמית
רשות ההסתדרות לצרכנות	-	יובל דרורי

דני אילן ריכז את עבודת הכנת התקן.

הודעה על רווידיה

תקן זה בא במקום

התקן הישראלי ת"י 1495 חלק 3 מיוני 1992

מילות מפתח:

עיבוד נתונים, טיפול במידע, בקרת גישה, סיסמות, אמצעי בטיחות.

Descriptors:

data processing, information handling, access, password, safety measures.

עדכניות התקן

התקנים הישראליים עומדים לבדיקה מזמן לזמן, ולפחות אחת לחמש שנים, כדי להתאימם להתפתחות המדע והטכנולוגיה.

המשתמשים בתקנים יוודאו שבידיהם המהדורה המעודכנת של התקן על גיליונות התיקון שלו.

מסמך המתפרסם ברשומות כגיליון תיקון, יכול להיות גיליון תיקון נפרד או תיקון המשולב בתקן.

תוקף התקן

תקן ישראלי על עדכוניו נכנס לתוקף החל ממועד פרסומו ברשומות.

יש לבדוק אם התקן רשמי או אם חלקים ממנו רשמיים. תקן רשמי או גיליון תיקון רשמי (במלואם או בחלקם) נכנסים לתוקף 60 יום מפרסום ההודעה ברשומות, אלא אם בהודעה נקבע מועד מאוחר יותר לכניסה לתוקף.

סימון בתו תקן

כל המייצר מוצר, המתאים לדרישות התקנים הישראליים החלים עליו, רשאי, לפי היתר ממכון התקנים הישראלי, לסמנו בתו תקן:

מכון התקנים הישראלי

תוכן העניינים

הקדמה

תקן זה הוא חלק מסדרת תקנים הדנה באבטחת מערכות מידע ממוחשבות והכוללת עקרונות אבטחה, סיסמות, בקרת אירועים, התאוששות, ניהול הרשאות גישה, העתד וכדומה.

הסדרה דנה, בין היתר, באמצעים המיועדים להגן על מערכות אלה מפני סיכון של פגיעה במידע מההיבטים של חשיפת המידע, שלמותו ושרידותו.

חלקי הסדרה הם אלה:

ת"י 1495 חלק 1 - אבטחת מערכות מידע ממוחשבות - כללי[1]

ת"י 1495 חלק 2 - אבטחת מערכות מידע ממוחשבות - מצעים נושאי מידע[1]

ת"י 1495 חלק 3 - אבטחת מערכות מידע ממוחשבות - סיסמות

ת"י 1495 חלק 4 - אבטחת מערכות מידע ממוחשבות - ניטור ובקרת אירועים

ת"י 1495 חלק 5 - אבטחת מערכות מידע ממוחשבות - חיערכות למצב אסון

ת"י 1495 חלק 6 - אבטחת מערכות מידע ממוחשבות - הרשאות גישה

ת"י 1495 חלק 7 - אבטחת מערכות מידע ממוחשבות - גיבוי מידע ושחזורו

1. תחום התקן

1. 1. תקן זה דן באופן השימוש בסיסמות גישה, בסוגיהן ובמאפייניהן בכפוף לרמות אבטחה אלה:
רמה בסיסית, רמה בינונית ורמה גבוהה.

1. 2. התקן מיועד ליישום במערכות מידע ממוחשבות בכל ארגון במגזרי המשק השונים בישראל, שבו הסיסמה היא השיטה היחידה לאימות הזיהוי של המשתמש.

1. 3. למרות האמור בסעיף 1.2 לעיל, קיימים אמצעים נוספים לזיהוי המשתמש כגון אמצעים ביומטריים, המספקים הגנה חזקה יותר מסיסמה. לכן מומלץ במקרים של רמת סיווג גבוהה לעשות שימוש באמצעים אלה כתחליף לסיסמה או נוסף עליה.

1. 4. אין תקן זה דן בדרישות לאחסנה מאובטחת של סיסמות, אך הוא ממליץ על יישום אמצעים קריפטוגרפיים כגון הצפנה כהגנה על קבצים אלה.

2. סוגי סיסמות והגדרותיהן

להלן מפורטים סוגי סיסמות והגדרותיהן שכוחם יפה בתקן זה:

2. 1. סיסמת עבודה

מחרוזת תווים המיועדת לאימות הזיהוי של משתמש, כדי לאפשר למשתמש גישה מוגבלת או לא-מוגבלת למערכת מידע.

2. 2. סיסמה ראשונית

סיסמה הניתנת למשתמש ברגע שהוא מוגדר כמשתמש מורשה במערכת. הסיסמה מאפשרת למשתמש להיכנס כניסה ראשונה למערכת, שבמהלכה הוא נדרש להחליף אותה לסיסמת עבודה, כתנאי לעבודה במערכת. הסיסמה אינה מאפשרת עבודה רגילה במערכת אלא רק החלפה לסיסמת עבודה.

---

[1] נמצא ברוויזיה בעת כתיבת תקן זה.

2. 3. סיסמה זמנית

סיסמה המשמשת לזמן קצוב ונמסרת למשתמש מסוים, כגון לטכנאים.

2. 4. סיסמת ברירת מחדל

סיסמה מובנית בתוכנה הבסיסית, המתקבלת מהיצרן או ממתחזק המחשב.

2. 5. סיסמת משתמש בעל זכויות יתר

סיסמה של משתמש בעל הרשאות גבוהות במערכת המאפשרות שליטה על סיסמות של משתמשים אחרים.

2. 6. סיסמות תומכות

קיימות כמה סיסמות תומכות, כמפורט להלן:

2. 6. 1 סיסמה הנלוות לאמצעי הזדהות אחר כגון, סיסמה הנלווית להזדהות ביומטרית.

2. 6. 2 סיסמה המגינה על אמצעי הזדהות אחר כגון, סיסמה המגינה על Token (אסימון) המכיל אמצעי הזדהות.

2. 6. 3 סיסמה המגינה על אמצעי חתימה אלקטרונית חומרתי.

2. 6. 4 סיסמה (Passphrase) המגינה על אמצעי הצפנה וחתימה אלקטרונית תוכנתי (כגון מפתח PGP פרטי, מפתח הצפנה תוכנתי).

3. שימוש בסיסמה

3. 1 מאפייני סיסמה הנדרשים בהתאם לרמת האבטחה יהיו כמפורט בטבלה 1.
הדרישות שבטבלה הן דרישות מינימום והמשתמש או הארגון יכול להחמירן לפי שיקוליו.
בגישה ליישומים ולמשאבים, המוגדרים כבעלי רמת אבטחה גבוהה תידרש פעולת אימות זיהוי נוספת.

3. 2 אם המחשב ומערכת הפעלתו אינם כוללים את המאפיינים הנדרשים על-פי תקן זה, אפשר להשלים את החסר על ידי הוספת מוצר אבטחה מסחרי או מוצר אבטחה שפותח בארגון, ואף לנקוט צעדים נוספים לאבטחת המערכת.

3. 3 סיסמת ברירת המחדל תוחלף מיד עם סיום התקנת התוכנה הבסיסית במחשב הארגון, על ידי הגורם המוסמך בארגון, לסיסמה העומדת בדרישות תקן זה.

3. 4 אין להשתמש בסיסמה בעלת משמעות למשתמש, כגון בשמות ובתאריכים.

3. 5 סיסמת המשתמש בעל זכויות היתר ברמת אבטחה מסוימת תהיה גבוהה לפחות ברמה אחת מזו של המערכת. המנהל המוסמך על ידי הארגון רשאי להחליט על הורדת הסיווג של סיסמת המשתמש המיוחד.

טבלה 1

מספר סידורי	מאפייני הסיסמה	דרישות לסיסמה בהתאם לרמת אבטחה			הערות
		נמוכה	בינונית	גבוהה	
1	2	3	4	5	6
1	הגורם המחבר את הסיסמה	משתמש או מחולל ממוחשב	משתמש או מחולל ממוחשב	משתמש	-
2	אורך הסיסמה, מינ'	4 תווים	6 תווים	8 תווים	-
3	הרכב תווים	אותיות וספרות	אותיות קטנות וגדולות וספרות	אותיות קטנות וגדולות, ספרות וסימנים מיוחדים	בסיסמה ישולבו תווים מכל הסוגים המוזכרים
4	תווים זהים	מותרים	אסורים תווים זהים צמודים	אסורים	-
5	תווים עוקבים	מותרים	אסורים	אסורים	-
6	אותיות וספרות הנמצאות בסמיכות על גבי מקלדת	מותרות	אסורות	אסורות	-
7	משך התוקף, מקס'	180 יום	90 יום	30 יום	-
8	מספר ימים, מינ' להחלפת סיסמה אחת לאחרת(א)	60 ימים	45 ימים	30 ימים	למניעת חזרה מהירה לסיסמה הקודמת
9	מספר מחזורים, מינ' להשוואת סיסמות	4 מחזורים	8 מחזורים	12 מחזורים	-
10	מספר ניסיונות כניסה כושלים רצופים עד לנעילת הגישה למערכת ולמסוף	5	4	3	ראו סעיף 3.4
11	משך זמן הנעילה לאחר ניסיונות כושלים להזנת סיסמה עד לשחרור אוטומטי	חצי שעה	3 שעות	נעול עד לשחרור ידני על ידי מורשה. אין שחרור אוטומטי	-
12	משך הזמן שבו נספרות שגיאות הזנת סיסמה	חצי שעה	3 שעות	24שעות	-
13	מס' תווים, מינ' להחלפה	3	4	6	-

הערה לטבלה:

(א) אם נדרש להחליף סיסמה לפני מספר הימים המינימלי הנדרש, יופעל תהליך "איפוס" סיסמה ויצירת סיסמה חדשה במעורבות מנהלן המערכת או אחראי אבטחה או שניהם. במקרים מיוחדים ולפי נוהלי הארגון ניתן לאפשר למשתמש החלפת סיסמה מידית.

4. מאפייני סיסמה ראשונית

4.1 סיסמה ראשונית תאושר ותוקצה על ידי הגורם המוסמך.

4.2 לא תתאפשר עבודה במערכת על ידי שימוש בסיסמה ראשונית, והמשתמש יידרש להחליפה מיד בכניסה הראשונה למערכת.

4.3 מאפייני הסיסמה הראשונית בהתאם לרמות האבטחה יהיו כמפורט בטבלה 2 (בהתאמה).

טבלה 2

מספר סידורי	מאפייני הסיסמה הראשונית	דרישות לסיסמה בהתאם לרמת אבטחה			הערות
		בסיסית	בינונית	גבוהה	
1	משך התוקף, מקס'	45 ימים	7 ימים	תוך יום עבודה אחד	-

5. ניהול סיסמה זמנית

5.1 מתן סיסמה זמנית (ראו הגדרה 2.3) יהיה כאמור בסעיף 4.1.

5.2 כללי השימוש בסיסמה זמנית יהיו זהים לכללי השימוש בסיסמת עבודה (טבלה 1) ובכל מקרה, תוקף הסיסמה יפוג בתום המועד שנקבע לכך.

מכון התקנים הישראלי

The Standards Institution of Israel

תקן ישראלי - ת"י 1495 חלק 6

אדר התשס"א - פברואר 2001

אבטחת מערכות מידע ממוחשבות: הרשאות גישה

Information processing system security: Access permissions

20132 1/5/01 מק/דק/זג

מילות מפתח: עיבוד נתונים, מחשבים, הגנת החסן נתונים, מערכות מידע.

Descriptors: data processing, computers, data storage protection, information systems.

תקן זה הוכן על ידי ועדת מומחים בהרכב זה:
אורה קפלן (יו"ר), מירון קורנר, סרגיו רוזנצוויג, יורם קוהן

תקן זה אושר על ידי הוועדה הטכנית 1114 - אבטחת מידע במערכות מידע, בהרכב זה:

אוניברסיטת תל-אביב	-	אורה קפלן
איגוד הבנקים בישראל	-	ניסים בר-אל
אילי"א - איגוד ישראלי לעיבוד אינפורמציה	-	אהוד אבנר (יו"ר), אברהם הים
היחידה הממשלתית לאבטחת מידע	-	יגאל בצר
המועצה הישראלית לצרכנות	-	ראובן פרדס
הרשות הממשלתית לאבטחת מידע	-	יוסי שני
התאחדות התעשיינים בישראל	-	משה שפר
לשכת מנתחי מערכות מידע	-	נעמי אברמסון
משרד המשפטים	-	יעקב בלסבלג
משרד ראש הממשלה	-	נפתלי זיגרט
צבא ההגנה לישראל - ממר"מ	-	בועז לנדסברגר

כמו כן תרמו להכנת התקן: אהוד אבנר, ניסים בר-אל
עופר עגור ריכז את עבודת הכנת התקן.

תוכן העניינים

הקדמה

תקן זה הוא חלק מסדרת תקנים הדנים באבטחת מערכות מידע ממוחשבות ובאמצעים להגנה עליהן מפני סכנת חשיפת המידע וסכנת פגיעה בשלמותו ובשרידותו, על פי רמת האבטחה ועל פי רגישות המידע וחיוניותו לתפקודו של הארגון.

חלקי הסדרה הם:

ת"י 1495 חלק 1 - אבטחת מערכות מידע ממוחשבות: כללי

ת"י 1495 חלק 2 - אבטחת מערכות מידע ממוחשבות: מצעים נושאי מידע

ת"י 1495 חלק 3 - אבטחת מערכות מידע ממוחשבות: סיסמות

ת"י 1495 חלק 4[1] - אבטחת מערכות מידע ממוחשבות: בקרת אירועים

ת"י 1495 חלק 5 - אבטחת מערכות מידע ממוחשבות: היערכות למצב אסון

ת"י 1495 חלק 6 - אבטחת מערכות מידע ממוחשבות: ניהול הרשאות גישה

ת"י 1495 חלק 7 - אבטחת מערכות מידע ממוחשבות: גיבוי מידע ושחזורו

ת"י 1495 חלק 9[1] - אבטחת מערכות מידע ממוחשבות: ניתוח סיכונים

חיבטים נוספים של שמירת סודיות המידע במערכות התקשורת נידונים בתקנים אלה:

ת"י 1121 - בטיחות ציוד טכנולוגיית מידע

ת"י 1243 - בטיחות אש של מחשבים וציודם ההיקפי

ת"י 1972 חלק 1[1] - אבטחת מערכות תקשורת: עקרונות

ת"י 1972 חלק 3 - אבטחת מערכות תקשורת: היערכות ארגונים לקראת התחברות לתווך תקשורת חיצוני

ת"י 1972 חלק 4[1] - אבטחת מערכות תקשורת: אבטחה פיזית של תשתית התקשורת

מבוא

מטרת תקן זה להנחות את העוסקים בנושא מימוש אבטחה לוגית של מערכת מידע באמצעות שליטה על הגישה למידע. שליטה זו מתבצעת באמצעות מערכת הרשאות גישה לוגית למידע.

1. תחום התקן

תקן זה דן בעקרונות ניהול הרשאות גישה לוגית למידע ולמשאבים, וביישומם באמצעות תוכנה, קושחה ונחלים.

תקן זה מיועד ליישום במערכות מידע של ארגונים במגזרי המשק השונים בישראל.

אין תקן זה בא לגרוע מהוראות כל דין.

---

[1] נמצא בהכנה בעת פרסום תקן זה.

2. אזכורים

תקנים ומסמכים המוזכרים בתקן זה (תקנים ומסמכים לא מתוארכים - מהדורתם האחרונה היא הקובעת):

תקנים ישראליים

ת"י 1495 חלק 1 - אבטחת מערכות מידע ממוחשבות: כללי

ת"י 1495 חלק 3 - אבטחת מערכות מידע ממוחשבות: סיסמות

ת"י 1495 חלק 4[1] - אבטחת מערכות מידע ממוחשבות: בקרת אירועים

ת"י 1495 חלק 7 - אבטחת מערכות מידע ממוחשבות: גיבוי מידע ושחזורו

מסמכים ישראליים

חוק הגנת הפרטיות על תקנותיו וצוויו, לרבות עדכוניהם

3. הגדרות

הגדרות אלה כוחן יפה בתקן זה:

3. 1 משתמש

אדם, מערכת או ישות, המשתמשים במערכת מידע.

3. 2 מזהה משתמש

מאפיין המייחד את המשתמש במערכת מידע, ומשמש לניהול המשתמשים במערכת המידע.

3. 3 אימות זהות משתמש

ביצוע בדיקות המאפשרות למערכת לזהות משתמש, באמצעות מזהים כגון:

- מזהה שהמשתמש יודע, כגון סיסמה;
- מזהה שהמשתמש מחזיק ברשותו, כגון כרטיס חכם;
- מזהה שמאפיין את המשתמש עצמו, כגון: טביעת אצבע, טביעת רקמת קרנית העין.

3. 4 עקרון "הצורך לדעת"

פרטי המידע הדרושים למשתמש לצורך ביצוע תפקידו, ושלפיהם נקבעות הרשאות הגישה שלו.

3. 5 רמת רגישות המידע וחיוניותו

מידת חנזק שיכול להיגרם לאדם או לארגון בשל חשיפת המידע, או בשל פגיעה בשלמותו, באמינותו או בזמינותו, או בשל שימוש לרעה במידע ובמערכות מידע.

3. 6 סיווג מידע

ציון מוסכם בארגון המבטא את רמת רגישות המידע וחיוניותו.

3. 7 מידור מידע

חלוקת המידע לקבוצות שייכות או לקבוצות עניין, כשלכל אחת מהן בקרת אבטחה נפרדת לצורך הפחתת סיכונים.

הערה:

קיימות שלוש שיטות לפחות למידור מידע:

- לפי נושא או תת-נושא;
- לפי רמת רגישות המידע וחיוניותו;
- לפי כמות המידע המרוכז (כמות גדולה של מידע מרוכז תגדיל בדרך כלל את רמת רגישות המידע וחיוניותו).

3. 8. רמת אבטחה

מכלול הפעולות והאמצעים הנדרשים ליישום אבטחה, בהתאם לרמת רגישות המידע וחיוניותו לארגון.

הערה:

תקן זה דן בשלוש רמות אבטחה אלה: רמה בסיסית, רמה בינונית ורמה גבוהה, כמפורט בתקן הישראלי ת"י 1495 חלק 1.

3. 9. משאבי מערכת מידע

משאבים שניתן לגשת אליהם בצורה לוגית, כלומר באמצעות תוכנה, כגון: קובצי מידע במחשב, טבלות, תוכנות תשתית ותוכנות יישומיות, מצעי מידע מגנטיים או אופטיים, מדפסות, תחנות עבודה, שרתים, מסופים, ציוד תקשורת אקטיבי.

3. 10. אבטחת מערכת מידע

מכלול הפעולות והאמצעים הננקטים והמיושמים במערכת מידע המתופעלת באופן עצמאי או במשולב עם מערכות אחרות, כדי להגן עליה מפני פגיעה בזמינותה, בשרידותה ובסודיות המידע שבה, מפני שינוי במזיד או בשוגג, ומפני פגיעה בשלמות המידע ובאמינותו.

3. 11. אבטחה לוגית

שיטות, תוכנות, קושחות ונהלים המאפשרים שליטה ובקרה על הגישה אל משאבי מערכת המידע ועל השימוש בהם, ומניעת הגישה אל משאבי מערכת המידע והשימוש בהם מן הלא מורשים לכך.

3. 12. הרשאות גישה לוגית למידע (להלן: הרשאות גישה)

מכלול זכויות הגישה של משתמש הקובעות לאיזה משאב מותר לו לגשת, לאיזה חלק מהמידע המצוי במשאב מותר לו לגשת ומה סוג הפעילות שהוא מורשה לבצע בו. זכויות הגישה מבוססות על עקרון "הצורך לדעת" וכפופות למדיניות מידור המידע שנקבעה על ידי הנהלת הארגון.

3. 13. ניהול הרשאות גישה

מכלול פעולות הכולל מתן הרשאת גישה, שינויה, הקפאתה, חידושה או ביטולה ותיעוד הפעולות האלה.

3. 14. מערכת הרשאות גישה

מנגנון שבאמצעותו מתבצעת השליטה בכל סוגי הגישה לכל משאב במערכת המידע.

3. 15. בקרת גישה לוגית (להלן: בקרת גישה)

בקרה על פעולת מתן גישה או על פעולת מניעתה, בדיקת תקינות הגישה למידע לפי הרשאות הגישה שנקבעו, ורישום של בקשות לקבלת הרשאות גישה ותוצאותיהן.

3. 16. הממונה על אבטחת מידע

אדם שמונה מטעם הארגון כאחראי ליישום המדיניות של הארגון בתחום אבטחת המידע.

3. 17. אחראי אבטחת מידע

אדם שמונה מטעם הארגון לביצוע פעולות לאבטחת המידע בתחום מסוים, והוא מונחה מבחינה מקצועית על ידי הממונה על אבטחת המידע.

3. 18. בעל מידע

אדם שנקבע על ידי הארגון כאחראי על המידע בתחום מסוים, ובסמכותו להורות על הזנת מידע, עיבודו והפקתו.

3. 19. קובצי אבטחת מידע

כל הקבצים הקשורים בפעילות אבטחת המידע כגון:

3. 19. 1. קובצי מערכות אבטחת המידע;

3. 19. 2. קבצים של הגדרת המשאבים, של הגדרת המשתמשים ושל הגדרת הרשאות הגישה שלהם;

3. 19. 3. קובצי רישום האירועים השוטפים והאירועים החריגים של המשתמשים;

3. 19. 4. קובצי רישום השינויים בהרשאות גישה.

3. 20. אירוע חריג

אירועים העלולים לפגוע באבטחת מערכות המידע, כגון:

- ניסיון של משתמש מורשה להשתמש במערכת המידע שלא במסגרת הרשאות הגישה שלו;
- ניסיון של משתמש שאינו מורשה לחדור למחשב הארגון ולמערכת המידע שלו במטרה לעיין במידע, להעתיקו, לשנותו או לגרום לו נזק;
- תקלה בתפקוד של אחד האמצעים לאבטחת המידע;
- גרימת נזק כתוצאה מפעילות חוקית של משתמש מורשה (לדוגמה: הורדת קובץ נגוע בווירוסים מהאינטרנט).

3. 21. סוג הרשאת גישה

אופן הגישה למידע או למשאב כגון: קריאה, כתיבה, מחיקה, הרצה של תוכניות.

3. 22. סיווג משאב מערכת מידע

סיווג המשאב, לפי סיווג המידע הרגיש ביותר שהוא מכיל.

4. מסגרת להקמת מערכת הרשאות גישה בארגון

4. 1. הארגון יבחן האם המחשב ותכונות אבטחת המידע, המובנות במערכת ההפעלה שלו ובאמצעי אבטחה נוספים שבשימושו, מאפשרים את ביצוע הפעילויות הנדרשות על פי תקן זה, ובהתאם למדיניות האבטחה של הארגון, בהתאם לרמת רגישות המידע וחיוניותו לארגון ובהתאם לרמת האבטחה הנדרשת.
אם פעילויות האבטחה הנדרשות אינן ניתנות לביצוע, ישלים הארגון את החסר על ידי הוספת מוצר אבטחה מסחרי או מוצר אבטחה שפותח בארגון.
התשתית של האבטחה הלוגית תתבסס על מיפוי הישויות בארגון. בסיום המיפוי יתקבל אוסף נתונים, המציג עבור כל משתמש את משאבי מערכת המידע שהוא נדרש לגשת אליהם לצורך עבודתו (על פי עקרון "הצורך לדעת").

4. 2. מערכת הרשאות הגישה תכלול את הרכיבים האלה:

א. תוכנת בקרת גישה הפועלת בזמן אמת, לבקרת בקשות המשתמשים לגישה למידע;

ב. הגדרת הרשאות גישה המציינות את הקשר בין משתמש לבין משאבי מערכת המידע;

ג. חיוויים בזמן אמת על אירועים חריגים ורישומם בקובצי רישום אירועים;

ד. נתוני מיפוי הישויות בארגון (ראו סעיף 5).

4. 3. הרשאות הגישה יתבססו על שלושה מרכיבים:

4. 3. 1. למי נותנים גישה (למי מבין משתמשי מערכות מידע);

4. 3. 2 אל מה נותנים גישה (אל איזה משאב ממשאבי מערכת המידע);

4. 3. 3 הגדרת הקשר בין משאבי מערכת המידע לבין משתמשי מערכת המידע, במונחים של מתן גישה למידע או מניעתה.

4. 4 מערכת בקרת הגישה תתעד את פעולות המשתמשים בקובץ מיוחד לרישום אירועים. קובץ זה מיועד לאיתור אירועים חריגים של משתמשים, לסייע באיתור של נקודות תורפה אבטחתיות במערכת ולסייע בחקירה של אירועים המצריכים חקירה. קובצי רישום האירועים ישמשו כאמצעי עיקרי לפעילות של ביקורת (ראו בתקן ישראלי ת"י 1495 חלק 4[1]).

4. 5 הארגון יקבע סמכויות ותחומי אחריות לצורך יישום הרשאות גישה, כמפורט להלן:

א. גורם מוסמך היוזם הגשת בקשה לקבלת קוד משתמש והענקת הרשאות גישה (לדוגמה, המנהל הממונה על העובד);

ב. גורם המחליט על הענקת הרשאות גישה (לדוגמה בעל המידע);

ג. גורם מבצע המעניק הרשאות גישה (לדוגמה אחראי אבטחת המידע);

ד. גורם מבקר של תהליך הענקת הרשאות הגישה.

4. 6 הארגון יקבע כללים לביצוע הפעילויות האלה:

4. 6. 1 ניהול משתמשים:
רישום פרטי משתמש חדש, שינוי פרטים של משתמש קיים, ביטול משתמש, הקפאת הרשאת גישה של משתמש וביטולה (על פירוט פעולות ניהול מזהי משתמשים, ראו בנספח ב);

4. 6. 2 ניהול משאבי מערכת המידע:
פעילויות רישום עדכני של משאבי מערכות המידע (על פירוט פעולות אלה ראו בנספח ג);

4. 6. 3 ניהול הרשאות גישה:
הגורמים המשפיעים על ניהול הרשאות הגישה הם אלה: מדיניות אבטחת המידע, תהליכי עבודה, הגדרת תפקידים ומשוב (פידבק) מבדיקת קובץ רישום אירועי המשתמשים (על פירוט הפעולות הקשורות לניהול הרשאות גישה ראו בסעיף 6);

4. 6. 4 תגובה לאירועים חריגים וטיפול בהם;

4. 6. 5 יישום לקחים מממצאי ביקורת אבטחת מידע, וטיפול בחריגות בגישה למידע;

4. 6. 6 טיפול בתקלות במערכת הרשאות הגישה;

4. 6. 7 הטמעת נוהלי הרשאות גישה:
- הדרכת המשתמשים ליישום נכון של נוהלי הרשאות הגישה;
- ביצוע ביקורת על יישום נוהלי הרשאות הגישה;
- ייזום תגובות על אירועים חריגים ועל חריגות מנוהלי הרשאות הגישה של משתמשים ובעלי תפקידים;

4. 6. 8 שמירת רשימת הפעילויות השוטפות הקשורות למערכת האבטחה בקובצי רישום האירועים, ביחידות של ימים או נפחי דיסק, עד למועד העברתה לשמירה ארוכת טווח.
משך השמירה לטווח קצר ולטווח ארוך יהיה לפי קביעת הארגון.

5. מיפוי ישויות בארגון

5. 1 כללי

פרק זה מטרתו להנחות את העוסקים בהקמת תשתית למערכת הרשאות גישה. מנחל הארגון ימנה צוות היגוי בין-תחומי למיפוי הישויות המרכיבות את מערכות המידע הממוחשבות שלו ולעדכונו מפעם לפעם. הנתונים שיתקבלו לאחר מיפוי הישויות ולאחר קביעת רמת הרגישות והחיוניות של כל ישות בארגון (לפי נספח א) ישמשו בסיס לתכנונה והקמתה של מערכת הרשאות גישה בארגון.

5. 2 תיאור המבנה הארגוני

יוכן תיאור סכמתי של מבנה הארגון. בתיאור הסכמתי ייכללו הפרטים האלה: שמות היחידות בארגון, מיקומן בהיררכיה הארגונית, מיקומן הפיזי, שמות בעלי התפקידים הניהוליים העיקריים.

5. 3 מיפוי המשאבים הפיזיים

הארגון יערוך מיפוי של המשאבים הפיזיים המשמשים את המערכות הממוחשבות ואת המשתמשים, לדוגמה: מחשבים, שרתים, תחנות עבודה, יחידות קלט-פלט ומצעי מידע. לגבי כל משאב פיזי יכלול המיפוי את הפרטים האלה: שם המשאב, סוג המשאב, שם היצרן שלו, מיקומו, ייעודו, בעל המשאב, חיבור לרשתות תקשורת, חיבור למחשבים אחרים בארגון.

5. 4 מיפוי פריסת משאבי התקשורת

הארגון יערוך מיפוי של פריסת משאבי התקשורת בתחומו, המשרתים את המערכות הממוחשבות שלו, כגון: בקרים, נתבים, ממירים, מודמים, קווי תקשורת. לגבי כל אחד ממשאבי התקשורת יכלול המיפוי את הפרטים האלה: שם המשאב, סוג המשאב, מיקומו, ייעודו, בעל המשאב, חיבור למחשבים, סוג התקשורת.

5. 5 מיפוי תהליכי עבודה

הארגון יערוך מיפוי של תהליכי העבודה הקיימים בתוכו, ושל מהלך זרימת המידע בין בעלי התפקידים המשתתפים בכל שלבי התהליך. לגבי כל תהליך, יכלול המיפוי את הפרטים האלה: שם התהליך, מטרתו, הממונה על התהליך, היחידות התפקודיות בארגון שאותן הוא משרת, בעלי התפקידים הנוטלים בו חלק, הפעילות המתבצעת בכל אחד משלבי התהליך, המערכות הממוחשבות המשרתות את התהליך וזרימת המידע אל הארגון או מן הארגון החוצה.

5. 6 מיפוי בעלי התפקידים

הארגון יערוך מיפוי של כל בעלי התפקידים בתוכו. בעלי התפקידים יחולקו ל-3 קבוצות לפי מידת מעורבותם בכל תהליך עבודה:

5. 6. 1 בעלי המידע;

5. 6. 2 בעלי תפקידים המשתתפים בתהליך העבודה עצמו;

5. 6. 3 בעלי תפקידים אחרים שאינם קשורים ישירות לביצוע תהליך העבודה, אך נוטלים חלק בתפעולו התקין.

מיפוי בעלי התפקידים יכלול את הפרטים האלה: שם התפקיד, תיאור התפקיד, תחומי האחריות של בעל התפקיד, סמכויותיו לאישור ולביצוע פעילויות, המשאבים שבאחריותו, התהליכים שהוא קשור אליהם, המערכות היישומיות[2] שבתחום אחריותו, התוכנות שביחידתו.

---

[2] application systems

5. 7 מיפוי מערכות המידע

5. 7. 1 מיפוי תוכנות

הארגון יערוך מיפוי של התוכנות האלה:

א. תוכנות תשתית;

ב. תוכנות תקשורת;

ג. תוכנות יישומיות.

מיפוי התוכנות יכלול את הפרטים של כל תוכנה, כמפורט להלן: שם התוכנה, מטרת פעולתה, שם היצרן שלה, המשאבים הפיזיים שהיא מותקנת בהם, המערכות הממוחשבות העושות בה שימוש, בעלי התפקידים שהם בעלי הרשאת גישה לתוכנה.

5. 7. 2 מיפוי חומרות וקושחות

5. 7. 3 מיפוי קבצים

הארגון יערוך מיפוי של כל סוגי הקבצים הקיימים. המיפוי יכלול קבצים שהם בסיסי נתונים, תיקיות, טבלות, קובצי נתונים של מערכות יישומיות, קובצי LOG, קובצי גיבוי וכו'. לגבי כל קובץ יצוינו במיפוי הפרטים האלה: שם הקובץ, תוכנו, מטרתו, מיקומו (במשאב פיזי), התוכנות העושות בו שימוש, המערכות היישומיות העושות בו שימוש, בעל הקובץ, בעלי התפקידים העושים שימוש בקובץ ומהות העבודה שלהם. כמו כן יצוין אם הקובץ מכיל מידע המוגן בחוק הגנת הפרטיות, על תקנותיו וצוויו, לרבות עדכוניהם.

5. 7. 4 מיפוי רשומות ושדות

הארגון יערוך מיפוי של קובצי המידע לרשומות ולשדות. לגבי כל רשומה או שדה תצוין רמת רגישות המידע וחיוניותו.

5. 7. 5 מיפוי פלטים

הארגון יערוך מיפוי של כל התוצרים המופקים בעיבוד במערכות המידע כגון: הדפסות, תצוגות על מסך ומידע מעובד הנרשם על גבי מצעי מידע.

5. 8 מיפוי המשתמשים

הארגון יערוך מיפוי של המשתמשים במערכות המידע (פנימיים וחיצוניים), וירשום ליד כל משתמש את הפרטים האלה: שם המשתמש, תפקידו, שייכותו הארגונית, תהליכי העבודה שבהם הוא נוטל חלק, הפעילויות שאותן הוא מבצע, המערכות היישומיות[2] והתוכנות שהוא משתמש בהן.

ניתן לרכז מספר משתמשים בעלי מאפייני הרשאות גישה זהים לקבוצת משתמשים אחת, ולהעניק הרשאות גישה משותפות לכל חברי הקבוצה.

5. 9 מיפוי המידע

הארגון יערוך מיפוי של המידע שברשותו לפי קבוצות מידע, באופן שיאפשר לו את מידור המידע ואת ריכוז הטיפול בקבוצות המידע השונות, שייתכן שהן בעלות רמת רגישות וחיוניות שונה, ואת אבטחתן בהתאם.

כמו כן יצוין עבור כל פריט מידע בקבוצת מידע אם הוא כפוף לתקנות או הסכמים כלשהם.

להלן דוגמה לחלוקה לקבוצות מידע:

5. 9. 1 חלוקה על פי תהליכי עבודה;

5. 9. 2 חלוקה על פי שייכות ארגונית של המידע. כלומר, חלוקה לפי היחידה הארגונית האוספת את המידע או מייצרת אותו;

5. 9. 3. חלוקה על פי פריסה גאוגרפית, בעיקר בארגונים המבוזרים בכמה אתרים;

5. 9. 4. חלוקה על פי סביבות מחשוב;

5. 9. 5. חלוקה על פי דרישות חוק, תקנות והסכמים:

א. מידע המוגן על פי חוק, לדוגמה: חוק הגנת הפרטיות;

ב. מידע המוחזק ומטופל בארגון, אך כפוף לכללים שנקבעו על ידי גורמים חיצוניים לארגון, כגון: רשות שלטונית, מוסד מחקר;

ג. מידע הנמצא בארגון במסגרת הסכם או שיתוף פעולה בין ארגונים.

5. 10. מיפוי רמות רגישות המידע וחיוניותו

הענקת הרשאת גישה מתאימה למשתמש אל המידע מותנית גם ברמת רגישות המידע וחיוניותו. קיימים כמה גורמים המשפיעים על קביעת רמת רגישות המידע וחיוניותו כגון: רגישות המידע, חיוניות המידע, הוראות חוק (כגון חוק הגנת הפרטיות), תקנות, הסכמים.

הרמה תיקבע עבור כל אחד ממשאבי מערכות המידע של הארגון.

תהליך קביעת רמת רגישות המידע וחיוניותו יתבסס על כמה שלבים:

א. קביעת קריטריונים לבחינת רגישות המידע וחיוניותו;

ב. קביעת סולם ציונים לרגישות המידע וחיוניותו;

ג. קביעת רמת רגישות המידע וחיוניותו.

פירוט מלא של התהליך ואופן קביעת רמת רגישות המידע וחיוניותו, ראו בנספח א.

6. ניהול הרשאות גישה

ניהול הרשאות גישה מורכב מארבעה שלבים:

6. 1. הגשת בקשה להרשאת גישה

הגשת בקשה אל בעל המידע תיעשה על ידי גורם מוסמך.

הבקשה תתייחס לאחת מן הפעילויות האלה: הענקת הרשאות גישה, שינוין, הקפאתן או ביטולן.

הבקשה תכלול את הנתונים האלה:

א. פרטי העובד אשר עבורו נדרשת הרשאת הגישה (שם, מספר תעודת זהות או מספר עובד של הארגון, תפקידו והקשר שלו לארגון, לדוגמה: ספק שירותים, מנוי שירות);

ב. מהות הבקשה להרשאת גישה (הענקה, שינוי, הקפאה, ביטול);

ג. נימוקים לצורך בהרשאת גישה (לדוגמה, תפקיד העובד);

ד. מזהה המשתמש;

ה. שם משאב מערכת המידע;

ו. סיווג המידע (נתון זה אינו חיוני בבקשת הקפאה או ביטול);

ז. רמת הרשאת הגישה (נתון זה אינו חיוני בבקשת הקפאה או ביטול);

ח. מועד פקיעת תוקף הרשאת הגישה, או משך תוקף הרשאת הגישה;

ט. פרמטרים והתניות הנוגעים להרשאות גישה.

להלן דוגמה לפרמטרים ולהתניות המובאים בחשבון לצורך הענקת הרשאות גישה:

- סוג הרשאת הגישה (קריאה, כתיבה, שינוי, ביטול, הרצה של תוכניות);
- המידע המותר (רשומות, שדות);
- תחומי גישה לשדות לפי ערכים;

- ימי פעילות ושעות פעילות;
- תפריטים מונחים, תוכנות שירות.

הערה:
יש לציין פרטים אלה עבור כל משאב מערכת מידע אשר נדרשת הרשאת גישה אליו.

6. 2. אישור הבקשה להרשאת גישה

6. 2. 1 בעל המידע יקבע את הרשאת הגישה של המשתמש למשאב מערכת המידע, על פי עקרון "הצורך לדעת". בעל המידע יוכל לבצע פעולות אלה:

א. לאשר את הבקשה במלואה;
ב. לדחות את הבקשה תוך ציון הנימוקים לכך;
ג. לאשר את הבקשה עם סייגים ולציין את הנימוקים לכך.

6. 2. 2 לצורך אישור קבלת הרשאת גישה למשאבי מערכת מידע בעלי רמת אבטחה גבוהה, כגון תיקיות מקור, תוכניות מערכת הפעלה, משאבי מערכת אבטחת מידע, למשל: קובצי אבטחת מידע או קבצים המכילים מידע רגיש לארגון, ייקבעו התניות נוספות כגון אלה:

א. גורם מאשר נוסף, למשל: הממונה על אבטחת מידע, ועדה להרשאות גישה, מנהל תשתיות;
ב. הגבלת הגישה לטווחי זמן מוגדרים כגון: שעות גישה, ימי גישה, ימי גישה לפרק זמן מוקצב;
ג. הגבלת הגישה על ידי שימוש באמצעי אבטחה נוספים כגון: אימות חוזר של זהות המשתמש, שימוש בקווים מאובטחים בתקשורת, גישה דרך תפריטים מונחים מראש.

6. 3. ביצוע הבקשה להרשאת גישה

6. 3. 1 הענקת הרשאת גישה למשתמש, שינויה, הקפאתה או ביטולה יבוצעו בהתאם לבקשה המאושרת.

6. 3. 2 הרשאות גישה יבוטלו או יוקפאו בשל סיבות כגון אלה:

א. חריגות מכללי אבטחת המידע הנובעות מתהליך בקרה אוטומטי (לדוגמה הקפאת קוד משתמש כתוצאה ממספר מסוים של ניסיונות רצופים כושלים להקלדת סיסמה);
ב. תפוגת ההרשאה, שמועדה הוגדר במערכת האבטחה והיא מתבצעת באופן אוטומטי בהתאם להגדרות;
ג. יציאת עובד לחופשה ממושכת;
ד. התפטרות או פיטורין של עובד;
ה. שינוי תפקיד העובד בארגון.

6. 4. בקרת הרשאות גישה

6. 4. 1 תיעוד הבקשה למתן הרשאות גישה למידע או לביטולן יישמר כאסמכתא לביקורת תקופתית ושוטפת.

6. 4. 2 תיערך בדיקה תקופתית של הרשאות גישה הכוללת בדיקות אלה:

א. בדיקת תקפות מרחב ההרשאות של משתמשים;
ב. בדיקה של הרשאות שניתנו לפרק זמן מוגבל;
ג. בדיקת פעילות משתמשים בעלי הרשאות נרחבות.

7. יישום הרשאות גישה

7.1 על מנת להבטיח יישום של הרשאות גישה בהתאם למדיניות אבטחת המידע, יש להתייחס מצד אחד לרמות רגישות המידע וחיוניותו שקבע הארגון (ראו נספח א), ומצד שני לבחור מתוך שלוש רמות האבטחה: בסיסית, בינונית וגבוהה, כמפורט בתקן הישראלי ת"י 1495 חלק 1, את הרמה המתאימה לצורכי הארגון. על פי רמה זו תיבנה טבלת הפעילויות ליישום הרשאות הגישה.

7.2 טבלה 1 מפרטת את הפעילויות שיתבצעו על ידי מערכת הרשאות הגישה ועל ידי אחראי אבטחת המידע בארגון, בהתאם לשלוש רמות האבטחה.
ביישום הרשאות הגישה ניתן גם לשלב פעילויות השייכות לרמת אבטחה גבוהה יותר מזו שנקבעה למערכת המידע. לדוגמה, אם עבור מערכת מידע מסוימת נקבעה רמת אבטחה בסיסית ניתן לבחור בפעילויות מסוימות מרמת אבטחה גבוהה יותר.

טבלה 1 - פעילויות ליישום הרשאות גישה(א)

הסעיף	הפעילות	תכיפות הביצוע בהתאם לרמת אבטחה (בימים)		
		בסיסית	בינונית	גבוהה
7.2.1	**ניהול מזהי משתמשים**			
7.2.1.1	ביטול מזהה של משתמש שמתנתק מהארגון. (לפי נספח ב, סעיף ב-5) לדוגמה: עובד שעוזב את הארגון או משתמש שמנתק את הקשר עם הארגון	מידי	מידי	מידי
7.2.1.2	בדיקת ביטול מזהה של משתמש שהתנתק מהארגון. בדיקה זו היא בקרה על ביצוע הפעולה בסעיף 7.2.1.1 לעיל.	90	30	7
7.2.1.3	בדיקת תוקף מזהה משתמש (ראו נספח ב' סעיף ב-5)	360	180	60
7.2.1.4	הקפאת מזהה משתמש שאינו פעיל יותר מכמה ימים	90	60	15
7.2.1.5	הקפאת הקוד של עובד, שידוע שהוא עומד להיעדר מהעבודה לתקופה מסוימת, החל ביום ההעדרות המתוכנן	מידי	מידי	מידי
7.2.1.6	הקפאת מזהה משתמש או ביטולו בשל אירוע חריג	מידי	מידי	מידי
7.2.2	**ניהול הרשאות גישה**			
7.2.2.1	בדיקה תקופתית של תוקף הרשאות הגישה של כל משתמש	360	180	90

(המשך הטבלה בעמוד הבא)

טבלה 1 - פעילויות ליישום הרשאות גישה[א] (סוף הטבלה)

הסעיף	הפעילות	תכיפות הביצוע בהתאם לרמת אבטחה (בימים)		
		בסיסית	בינונית	גבוהה
7.2.2.2	בדיקה תקופתית של הרשאות גישה הניתנות לפרק זמן מוגבל	60	30	1
7.2.2.3	שינוי הרשאות הגישה בעת מעבר עובד מתפקיד לתפקיד	מידי	מידי	מידי
7.2.2.4	שינוי הרשאות הגישה בעקבות אירוע חריג	מידי	מידי	מידי
7.2.3	**ניהול משאבי מערכת מידע**			
7.2.3.1	בדיקת משאבי מערכת מידע הקיימים בפועל מול משאבים המוגדרים במערכת אבטחת המידע	360	180	90
7.2.4	**רישום האירועים** (ראו גם התקן הישראלי ת"י 1495 חלק 4)[1]			
7.2.4.1	רישום כל פעולה שמתבצעת במערכת	לא	לא	כן
7.2.4.2	רישום אירועים חריגים	כן	כן	כן
7.2.4.3	רישום גישות למשאבים המוגדרים כרגישים	כן	כן	כן
7.2.4.4	רישום גישות משתמשים בעלי הרשאות גישה רחבות ומיוחדות	לא	כן	כן
7.2.4.5	רישום שינויים בהרשאות גישה	כן	כן	כן
7.2.4.6	רישום שינויים בקובצי אבטחת המידע	כן	כן	כן
7.2.5	**טיפול באירועים חריגים**			
7.2.5.1	בירור סיבת האירוע החריג שנרשם למשתמש	כן	כן	כן

הערה לטבלה:

(א) יש לתכנן את שמירת הגיבויים במשך פרקי הזמן שיאפשרו את ביצוע הפעילויות הנדרשות, בהתאם לתקן הישראלי ת"י 1495 חלק 4[1] וחלק 7.

נספח א - רגישות המידע וחיוניותו

(נורמטיבי)

א-1. תהליך קביעת רמת רגישות המידע וחיוניותו

א-1.1. כללי

קביעת רמת רגישות המידע וחיוניותו משמשת לציון הצרכים וסדרי העדיפויות של ההגנה על המידע, ולקביעת רמת אבטחה מתאימה, והיא מבטאת את הצורך בנקיטת אמצעי אבטחה נוספים או מיוחדים לפריטי מידע מסוימים. רמת רגישות המידע וחיוניותו תיקבע לפי רגישות המידע וחיוניותו לארגון ולפי הוראות חוק, תקנות והסכמים.

א-1.2. שלבי התהליך

תהליך קביעת רמת רגישות המידע וחיוניותו יכלול שלושה שלבים:

- קביעת קריטריונים לבחינת רגישות המידע וחיוניותו, כמפורט בסעיף א-2;
- קביעת סולם ציונים לרגישות המידע וחיוניותו, כמפורט בסעיפים א-3 עד א-5;
- מתן ציון רגישות לכל קריטריון המפורט בטבלה א-1 וסיכום ציוני הרגישות לציון רגישות כולל אחד, הנקרא רמת רגישות קבוצת המידע וחיוניותה, כמפורט בסעיף א-6 ובסעיף א-7.

א-2. קריטריונים לבחינת רגישות המידע וחיוניותו

הארגון יקבע קריטריונים לבחינת רגישות המידע וחיוניותו, ועל פיהם תיבחן הערכת הנזק שעלול להיגרם לארגון כתוצאה מהעדר אבטחה מתאימה.

להלן דוגמה לרשימת קריטריונים אפשריים לבחינה:

א-2.1. פגיעה בחיי אדם;

א-2.2. אי-עמידה בחוקים, תקנות והסכמים;

א-2.3. נזק כלכלי;

א-2.4. פגיעה במוניטין;

א-2.5. פגיעה בתהליכי ייצור (למשל, בתפעול שוטף, במתן שירותים ללקוחות);

א-2.6. פגיעה בעמידה בהתחייבויות;

א-2.7. הפסד שווקים;

א-2.8. פגיעה במחקר ובפיתוח (הפסד זכויות יוצרים או אי-רישום פטנט או אי-עמידה בלו"ז לסיום הפיתוח).

א-3. קביעת משקל לקריטריונים

הארגון ייתן משקל יחסי לכל אחד מהקריטריונים שנקבעו. המשקל יהיה לדוגמה מספר בין 1 ל-10, כאשר כל קריטריון מקבל משקל יחסי סובייקטיבי, בהתאם לחשיבותו בתהליך בחינת הערכת הנזק שייגרם לארגון (אפשר שלכמה קריטריונים יהיה משקל זהה).

א-4. קביעת סולם ערכים

הארגון יקבע סולם ערכים לציון הגורמים האלה (משקלים): סודיות, זמינות ושרידות. הגורמים: פגיעה באמינות הנתונים ופגיעה בשלמות הנתונים יקבלו תמיד את המשקל או הציון הגבוה ביותר. פגיעות אלה בנתונים פוגעות בפעולה התקינה של מערכת המידע עצמה (מסיבה זו אין גורמים אלה כלולים בטבלה א-1).

א-5. קביעת סולם ציונים

הארגון יגדיר סולם ציונים שישקף את מידת רגישות המידע וחיוניותו לארגון. כלומר ככל שהנזק שייגרם לארגון או לפרט מפגיעה בקבוצת מידע מסוימת יהיה גדול יותר - ציון הרגישות של הקבוצה יהיה גבוה יותר. לדוגמה: סולם ציוני רגישות שערכיו הם מ-0 עד 3, כש-1 מייצג את הציון הנמוך ביותר ו-3 את הציון הגבוה ביותר, ו-0 מציין: "לא רלוונטי".

קביעת ציוני הרגישות מבוססת על הערכה איכותית סובייקטיבית של המעריך בארגון ולא על פי מדידה כמותית.

א-6. רמת רגישות המידע וחיוניותו

ציוני הרגישות שהתקבלו יקובצו לקבוצות. קבוצות אלו יהיו רמות רגישות המידע וחיוניותו, כמפורט בסעיף א-7.2, הנחיה ה.

מספר רמות רגישות המידע וחיוניותו יהיה שלוש. רמות רגישות המידע וחיוניותו משפיעות על רמת האבטחה שעל הארגון ליישם.

(לעניין רמת אבטחה, ראו בתקן הישראלי ת"י 1495 חלק 1).

א-7. קביעת ציון רגישות כולל

א-7.1. לחלן דוגמה של טבלה למתן ציוני רגישות לקבוצות המידע, לפי הגורמים: סודיות, זמינות ושרידות. מתן ציוני הרגישות, סיכומם והכפלתם במשקל הקריטריון מסייעים בקביעת רמת רגישות המידע וחיוניותו.

יש למלא טבלה זו עבור כל קבוצת מידע.

טבלה א-1 - ציון רגישות כולל לקבוצת המידע: "שם קבוצת המידע"(א)

קריטריונים	ציוני רגישות לקבוצת מידע				
	מ ש ק ל	ס ו ד י ו ת	ז מ י נ ו ת	ש ר י ד ו ת	ש ק ל ו ל
א. פגיעה בחיי אדם					
ב. נזק כלכלי					
ג. פגיעה במוניטין					
ד. פגיעה בתהליכי ייצור					
ה. פגיעה בעמידה בהתחייבויות					
ו. הפסד שווקים					
ז. פגיעה במחקר ופיתוח					
ח. אי-עמידה בחוקים, תקנות והסכמים					
ציון רגישות כולל					
רמת אבטחה כמפורט בסעיף א-7.2, הנחיה ה					

הערה לטבלה:

(א) במקום המילים "שם קבוצת המידע", ייכתב השם הספציפי של קבוצת המידע.

א-7.2 הנחיות למילוי הטבלה:

א. יינתן משקל לכל אחד מהקריטריונים בטבלה, בהתאם למשקלים שיקבע הארגון (סעיף א-3).

ב. ציוני הרגישות בטבלה יינתנו בהתאם לסולם הציונים שיקבע הארגון (סעיף א-5).
הציון מבטא את מידת ההשפעה שיש לפגיעה בקבוצת מידע מסוימת על הקריטריון הנבחן.

ג. לאחר מילוי ציוני הרגישות בכל הקריטריונים עבור קבוצת מידע מסוימת, יסוכמו כל ציוני הרגישות בכל שורת קריטריון, וסיכומם יוכפל במשקל הקריטריון. המכפלה תירשם בטור "שקלול".
כלומר: שקלול = משקל קריטריון × (ציון שרידות + ציון זמינות + ציון סודיות).
הציון שיתקבל לאחר השקלול יהיה ציון הרגישות של קבוצת המידע לקריטריון מסוים.

ד. ציון הרגישות הכולל לקבוצת מידע יתקבל מהסכום של טור "השקלול" שלה, כלומר, מסכום כל הערכים הרשומים בטור "שקלול" בכל הקריטריונים.
ציון זה הוא רמת הרגישות והחיוניות של אותה קבוצת מידע.

ה. רמת רגישות המידע וחיוניותו של כל קבוצת מידע קובעת את רמת האבטחה הנדרשת עבורה.
בהתאם לרמת רגישות המידע וחיוניותו ייגזרו 3 רמות אבטחה באופן הזה:
- רמת ציון שבשליש התחתון תיקבע כרמת אבטחה נמוכה;

- רמת ציון שבשליש התיכון תיקבע כרמת אבטחה בינונית;
- רמת ציון שבשליש העליון תיקבע כרמת אבטחה גבוהה.

א-7.3 הגנה בהתאם לרמת אבטחה

הארגון יגן על כל קבוצת מידע בהתאם לרמת האבטחה שנקבעה עבורה.

הארגון יקבץ קבוצות מידע בעלות רמות אבטחה זהות, על מנת לאפשר הגנה ברמות אבטחה שונות על קבוצות מידע שונות.

נספח ב - ניהול מזהי המשתמשים

(נורמטיבי)

ב-1. פעילות מזהה משתמש

כחלק בלתי נפרד מתהליך קביעת הרשאות הגישה למידע, ינוהלו מזהי המשתמשים במערכות המידע של הארגון.

הניהול יבוא לידי ביטוי בעת ביצוע הפעילויות האלה: הקצאת מזהה למשתמש חדש, ביטול מזהה משתמש, השעיית מזהה משתמש וביטול השעיית מזהה משתמש.

ב-1.1. הארגון יקבע בעלי תפקידים לביצוע הפעילויות שלהלן במזהה משתמש:

- ייזום הבקשה;
- אישור הבקשה;
- ביצוע הבקשה.

ב-1.2. בעלי התפקידים שלעיל יבדקו ויאמתו את תקינות הבקשות המופנות אליהם לפני ביצוע הפעילות המבוקשת.

ב-2. תיעוד הבקשות להרשאה

תיעוד הבקשות יישמר כאסמכתא לביקורת תקופתית ושוטפת. תקופת שמירת המסמכים תיקבע בנהלים להקצאת מזהה משתמש, להשעייתו, לביטול ההשעיה ולביטול מזהה המשתמש.

ב-3. קביעת נוהל להקצאת מזהה משתמש חדש

הנוהל יכלול את הפעילויות האלה:

ב-3.1. הגשת בקשה על ידי גורם מוסמך לקבלת מזהה משתמש. הבקשה תכיל פרטים כגון: פרטי זיהוי של המשתמש (שם פרטי או שם משפחה או שניהם ומספר תעודת זהות), תפקידו, המחלקה שהוא שייך אליה, משאבי מחשב נדרשים על פי עקרון "הצורך לדעת", חתימת הגורם המוסמך המבקש;

ב-3.2. הקצאת מזהה משתמש על פי שיטה שתיקבע בארגון.

ב-3.3. העברת סיסמה ראשונית על פי התקן הישראלי 1495 חלק 3.

ב-3.4. בארגונים שבהם לא נהוג להחתים עובד חדש על טופס הצהרת סודיות לשמירה על סודיות המידע של הארגון, ניתן במעמד זה להחתימו על טופס זה.

ב-4. קביעת נהלים להשעיית מזהה משתמש או לביטול ההשעיה

השעיית מזהה משתמש או ביטול ההשעיה יכולים להתבצע בשני אופנים: באופן יזום, לפי בקשת גורם מוסמך, או באופן ממוחשב על פי פרמטרים שנקבעו על ידי הארגון והוגדרו במערכת אבטחת המידע.

ב-5. קביעת נהלים לביטול מזהה משתמש

מזהה משתמש יבוטל במקרים האלה:

א. עזיבת המשתמש את הארגון;

ב. מעבר העובד מתפקיד לתפקיד במקרים שהמזהה מתבסס על שיוך ארגוני;

ג. במקרה שמזהה משתמש אינו פעיל מעל לפרק זמן מסוים;

ד. על פי הוראה של גורם מוסמך בארגון.

הערה:

לפני ביטול מזהה משתמש יש לוודא שבוטלו הרשאותיו.

ב-6. קביעת נהלים לביקורת פעילויות משתמשים

ב-6.1. ייקבעו נהלים להוספת משתמשים בעלי הרשאות רחבות לרשימת המשתמשים בקבוצות בקרה מיוחדות.

ב-6.2. תיערך בקרה תקופתית על ידי הגורמים האחראיים, על המשך הצורך בשימוש במזהי המשתמשים שבאחריותם.

נספח ג - ניהול משאבי מערכות המידע

(נורמטיבי)

ג-1. כללי

כחלק בלתי נפרד מתהליך קביעת הרשאות הגישה, ינוהלו משאבי מערכות המידע של הארגון. הניהול יבוא לידי ביטוי בעת ביצוע הפעילויות האלה: הוספת משאב חדש, שינוי בייעודו של משאב קיים או בתכולתו, הסרת המשאב ממצבת משאבי מערכת המידע של הארגון.

הארגון יקבע את בעלי התפקידים לביצוע הפעילויות המפורטות להלן.

ג-2. הוספת משאב חדש למערכת מידע

בעת הוספת משאב חדש למצבת משאבי מערכות המידע של הארגון יש לנקוט את הפעולות האלה:

ג-2.1. שיוך פיזי - קביעת מיקומו של המשאב בחצרי הארגון;

ג-2.2. שיוך לוגי - קישור המשאב למערכות המידע של הארגון;

ג-2.3. סיווג - סיווג המשאב על פי המידע הרגיש ביותר שהוא מכיל;

ג-2.4. קביעת בעלות על המשאב;

ג-2.5. רישום המשאב ברשימת מצאי משאבי המידע של הארגון, וברשומות המיפוי השונות;

ג-2.6. קביעת הרשאות הגישה למשאב;

ג-2.7. נקיטת אמצעי האבטחה הנדרשים;

ג-2.8. הוספת משאבים שהוגדרו כרגישים לקובץ רישום אירועים.

ג-3. שינוי בתכולת משאב מערכת המידע או בייעודו

בעת שינוי תכולתו של משאב מערכת מידע או שינוי בייעודו, ייתכן שיחולו שינויים המשפיעים על מערכת הרשאות הגישה למשאב.

השינויים יכולים לנבוע מכמה סיבות:

ג-3.1. שינוי בסיווג המידע;

ג-3.2. שינוי ברמת רגישות המידע וחיוניותו;

ג-3.3. שינוי בקישוריות המשאב למערכות המידע של הארגון;

ג-3.4. שינוי בבעלות על המשאב.

ג-4. הסרת משאב מערכת מידע ממצבת משאבי מערכת המידע של הארגון

הארגון יגדיר תהליך מסודר של הסרת משאב מערכת מידע ממצבת משאבי מערכת המידע של הארגון, כך שיימנע כל נזק לארגון. במסגרת תהליך זה יינקטו פעולות כגון: מחיקת המידע מהמשאב, עדכון קטלוגים, עדכון מערכת הרשאות הגישה, עדכון מצבת משאבי מערכת המידע.

התקנים הישראליים עומדים לבדיקה מזמן לזמן, ולפחות אחת לחמש שנים,
כדי להתאימם להתפתחות המדע, הטכניקה והתעשייה.
המשתמשים בתקנים יוודאו, שבידיהם המהדורה המעודכנת של התקן על גיליונות התיקון שלו.

הצעות לשינויים יש לשלוח לפי כתובת מכון התקנים הישראלי:

מכון התקנים הישראלי
רח' חיים לבנון 42, תל-אביב 69977, טל' 03-6465154, פקס' 03-6412762
להזמנת תקנים: טל' 03-6465191/2 פקס' 03-6426762 library@sii.org.il
ובאתר מכון התקנים הישראלי:
WWW.SII.ORG.IL

מכון התקנים הישראלי

The Standards Institution of Israel

תקן ישראלי - ת"י 1495 חלק 7

אב תשנ"ח - אוגוסט 1998

אבטחת מערכות מידע ממוחשבות: גיבוי מידע ושחזורו

Information processing system security: Information backup and restoration

ח.פ.מק.דק /זג 15/03/01

מילות מפתח: טכנולוגיית מידע, מערכות מידע, עיבוד נתונים, טיפול בנתונים, אבטחת נתונים, בטיחות.

Descriptors: information technology, information systems, data processing, data handling, data security, safety.

תקן זה הוכן ואושר על ידי הוועדה הטכנית 1114 - אבטחת מידע במערכות מידע, בהרכב זה:

אוניברסיטת תל-אביב	-	א' קפלן
איגוד הבנקים בישראל	-	נ' בר-אל
אי.ל.א - איגוד ישראלי לעיבוד אינפורמציה	-	א' אבנר (יו"ר), א' הים
התאחדות התעשיינים בישראל	-	מ' שפר
לשכת מנתחי מערכות מידע	-	נ' אברמסון
משרד המשפטים	-	ש' בר סלע
משרד ראש הממשלה	-	נ' זיגרט
צבא ההגנה לישראל - ממר"מ	-	מ' מגירא

כמו כן תרמו להכנת התקן: י' בצר, א' גגין, י' וינר, י' שני

רכז הוועדה - ע' עגור

תוכן העניינים

הקדמה

תקן זה הוא חלק מסדרת תקנים הדנים באבטחת מערכות מידע ממוחשבות ובאמצעים להגנה עליהן מפני סכנת חשיפת המידע, פגיעה בשלמותו והגנה על שרידותו, על פי רמת האבטחה וחיוניות המידע לתפקודו של הארגון.

חלקי הסדרה הם:

ת"י 1495 חלק 1 - אבטחת מערכות מידע ממוחשבות: כללי

ת"י 1495 חלק 2 - אבטחת מערכות מידע ממוחשבות: מצעים נושאי מידע

ת"י 1495 חלק 3 - אבטחת מערכות מידע ממוחשבות: סיסמות

ת"י 1495 חלק 4[1] - אבטחת מערכות מידע ממוחשבות: בקרת אירועים

ת"י 1495 חלק 5 - אבטחת מערכות מידע ממוחשבות: היערכות למצב אסון

ת"י 1495 חלק 6[1] - אבטחת מערכות מידע ממוחשבות: ניהול הרשאות גישה

ת"י 1495 חלק 7 - אבטחת מערכות מידע ממוחשבות: גיבוי מידע ושחזורו

היבטים נוספים של שמירת סודיות המידע במערכות התקשורת נידונים בתקנים אלה:

ת"י 1121 - בטיחות ציוד טכנולוגיות מידע, לרבות ציוד חשמלי לשימוש משרדי

ת"י 1243 - בטיחות אש של מחשבים וציודם ההיקפי

ת"י 1972 על חלקיו - אבטחת מערכות תקשורת

מבוא

מטרתו של תקן זה היא יצירת שיטה לגיבוי מידע, המאפשרת את שחזור המידע במקרה של תקלה שבעקבותיה נמנעת הגישה למידע או בשל נסיבות מיוחדות. תקן זה מיועד ליישום במערכות מידע של ארגונים במגזרי המשק השונים בישראל.

1. תחום התקן

1.1. תקן זה דן בתכנון ובביצוע של פעולות גיבוי המידע, החיוניות לצורך שרידות המידע, זמינותו והיכולת לשחזרו.

1.2. תקן זה קובע אמות מידה אחידות לגיבוי מערכות מידע ממוחשבות, על בסיס 3 רמות אבטחה: בסיסית, בינונית וגבוהה. התקן ישמש קו מנחה לקביעת נהלים פנימיים בארגון.

1.3. לתקן זה זיקה לתקן הישראלי ת"י 1495 חלק 5, הדן בהיערכות למצב אסון, וכן לתקן הישראלי ת"י 1495 חלק 2, הדן באבטחת מצעים נושאי מידע.

1.4. תקן זה חל על מרכיבי המידע הנכללים בהגדרת "מידע" כמפורט בסעיף 3.1.

1.5. אין תקן זה בא לגרוע מהוראות כל דין.

---

[1] נמצא בהכנה בעת פרסום תקן זה.

2. אזכורים

תקנים ומסמכים המוזכרים בתקן זה (תקנים ומסמכים לא מתוארכים - המהדורה האחרונה שלהם היא הקובעת):

תקנים ישראליים

ת"י 1243 - בטיחות אש של מחשבים וציודם ההיקפי

ת"י 1495 חלק 1 - אבטחת מערכות מידע ממוחשבות: כללי

ת"י 1495 חלק 2 - אבטחת מערכות מידע ממוחשבות: מצעים נושאי מידע

ת"י 1495 חלק 5 - אבטחת מערכות מידע ממוחשבות: היערכות למצב אסון

ת"י 1972 חלק 1[1] - אבטחת מערכות תקשורת: עקרונות

ת"י 1972 חלק 2[1] - אבטחת מערכות תקשורת: מערכות עיבוד נתונים - התחברות מערכות פתוחות - מודל ייחוס בסיסי: ארכיטקטורת אבטחה

ת"י 1972 חלק 3[1] - אבטחת מערכות תקשורת: היערכות ארגונים לקראת התחברות לתווך תקשורת חיצוני

ת"י 1972 חלק 4[1] - אבטחת מערכות תקשורת: אבטחת גישה לתשתית תקשורת

מסמכים ישראליים

חוק הגנת הפרטיות - ספר החוקים מ"א מס' 1011 מיום 1981-03-11, ותקנות הגנת הפרטיות התשמ"ו-1986

3. הגדרות

הגדרות אלה כוחן יפה בתקן זה:

3.1 מידע

מרכיבי המידע הם (כולם או חלקם):

- נתונים[2];
- תוכנות למיניהן. לדוגמה: מערכת הפעלה, תוכנות עזר, תוכנות יישומיות;
- תיעוד ממוחשב.

3.2 גיבוי

א. עותק זהה של המידע, שנכתב על מצע נוסף;

ב. פעולת ההעתקה של המידע למצע נוסף.

3.3 תכולת גיבוי

רשימת פריטי המידע הכלולים בגיבוי מסוים.

3.4 תדירות פעולות הגיבוי

מרווחי הזמן הקבועים שבין פעולות הגיבוי.

3.5 דור גיבוי[2]

מקומו הסידורי של הגיבוי בסדרת גיבויים עוקבים של אותו סוג גיבוי.

3.6 מחזור גיבוי

מספר דורות הגיבוי שנקבע לסוג גיבוי מסוים בארגון.

---

[2] ראו רשימת מונחים בסוף התקן.

3. 7 סבב דורות גיבוי

החלפת דור הגיבוי הקדום ביותר שבסדרה, המחווה מחזור גיבוי, בדור גיבוי חדש.

3. 8 גיבוי מלא

גיבוי של כל מרכיבי המידע בארגון (ראו הגדרה 3.1), או גיבוי של כל מרכיבי המידע של מערכת מסוימת.

3. 9 גיבוי חלקי

גיבוי של אחד או יותר ממרכיבי המידע.

3. 10 גיבוי שינויים ("גיבוי אינקרמנטלי")

גיבוי השינויים במידע מאז עריכת הגיבוי האחרון (ראו ציור 1).

3. 11 גיבוי שינויים מצטבר ("גיבוי דיפרנציאלי"):

גיבוי השינויים במידע מאז עריכת הגיבוי המלא האחרון.

3. 12 גיבוי רגיל

גיבוי מידע הנערך כשגרה למערכות הצוברות שינויים במידע באופן שוטף.

3. 13 גיבוי מיוחד

גיבוי מידע, הנערך בנוסף על הגיבוי הרגיל שהארגון מפעיל כשגרה והמבוצע בשל נסיבות מיוחדות, לדוגמה: החלפת מערכת הפעלה, גיבוי לאחר שחזור, החלפת דיסקים, גיבוי המשקף מצב נתונים לסוף שנת העסקים.

3. 14 גיבוי חם

עותק גיבוי הנרשם בגישה ישירה בו-זמנית עם מועד יצירת השינויים במידע.

3. 15 גיבוי חם קרוב לזמן אמיתי

עותק גיבוי הנרשם בגישה ישירה, בזמנים קצובים, בסמוך למועד יצירת השינויים במידע.

3. 16 גיבוי חם באתר המחשב

גיבוי חם הנערך על מצע מידע הנמצא באתר המחשב.

3. 17 גיבוי חם מחוץ לאתר המחשב

גיבוי חם הנערך על מצע מידע הנמצא מחוץ לאתר המחשב.

3. 18 שחזור מידע

העתקה של מידע מהמצע שבו נשמר הגיבוי אל מצע אחר המיועד לשימוש המערכת.

3. 19 שחזור מידע מלא

שחזור של כל מרכיבי המידע בארגון (ראו הגדרה 3.1), או שחזור של כל מרכיבי המידע של מערכת מסוימת.

3. 20 שחזור מידע חלקי

שחזור של אחד או יותר ממרכיבי המידע.

3. 21 רענון מצעים

שיטה להבטחת תקינות המידע במצעי גיבוי מגנטיים המיועדים לשמירה לתקופות ארוכות.

4. עקרונות לגיבוי

4.1 כל ארגון יערוך גיבוי של כל המידע שברשותו, באופן שיאפשר את שחזור המידע בעת הצורך.

4.2 כל ארגון יקבע נהלים לעריכת גיבוי עבור כל מערכת מחשב שברשותו, וימנה אחראי לעריכת הגיבויים על פי הנהלים.

4.3 כל ארגון יערוך גיבויים על גבי מצעים; עותק אחד יישמר בסמוך למחשב, והעותקים האחרים יישמרו באזורי סיכון השונים מאזור הסיכון של המחשב.
ארגון, שעל פי צרכיו התפעוליים ואופי עבודתו נדרש לספק שירותי מידע רצופים, ישקול גם יישום גיבוי חם. השיקול העיקרי ליישום גיבוי חם הוא מתן האפשרות לארגון להמשיך במתן שירותי המידע גם במצב של תקלה, ללא השהיה ברצף השירותים הנגרמת מפעולת שחזור המידע.

4.4 הארגון יבצע גיבויים מיוחדים לפי צרכיו.

4.5 בנוהלי הארגון ייקבעו עבור כל גיבוי הפרטים האלה:

- תכולת הגיבוי;
- היקף הגיבוי (גיבוי מלא או גיבוי חלקי);
- מצעי הגיבוי, מחזור הגיבוי, תדירות פעולת הגיבוי, מספר דורות הגיבוי, מספר עותקי הגיבוי;
- מקום אחסון עותקי הגיבוי ושיטת שינוע עותקי הגיבוי.

נוסף על אלה, ייקבעו תהליכי בדיקת האמינות והשלמות של:

- הגיבוי;
- יומן הגיבויים, כמפורט בטבלת ניהול מצעים שבתקן הישראלי ת"י 1495 חלק 2;
- סימון המצעים, כמפורט בטבלת ניהול מצעים שבתקן הישראלי ת"י 1495 חלק 2.

בעת הכנת הנוהל יש להתחשב בשיקולים אלה:

4.5.1 רמת אבטחת המידע, בהתאמה לתקן הישראלי ת"י 1495 חלק 1;

4.5.2 תדירות השינויים במידע;

4.5.3 הדרישות לזמינות המידע;

4.5.4 הסיכון באובדן המידע והנזק התוצאתי;

4.5.5 נפח המידע, שטח האחסון הנדרש ומצעי הגיבוי;

4.5.6 משך זמן פעולת הגיבוי;

4.5.7 הוראות החוק, כגון: חוק הגנת הפרטיות, הוראות רשויות המס.

4.6 בתכנון היישום של פעולות גיבוי יובא בחשבון זמן השמירה של המידע שהארגון מחויב בו על פי חוקים ותקנות או על פי צרכים תפעוליים של הארגון.

4.7 במצעים מגנטיים הנשמרים ללא שינוי תיעשה פעולת רענון באמצעות כתיבה מחדש לאחר 24 חודש מיום הכתיבה האחרון בהם.

5. תכנון גיבוי

5. 1 תכנון גיבוי רגיל

תכנון הגיבוי ייעשה בהתאם לטבלה 1.

טבלה 1 - תכנון גיבוי לגיבויים רגילים[א]

מס'	תכונה	סוג גיבוי	רמת אבטחה		
			בסיסית	בינונית	גבוהה
1	תדירות גיבוי	מלא	אחת לחודש	אחת לשבועיים	אחת לשבוע
		שינויים[ב]	אחת לשבוע	אחת ליום[ג]	אחת ליום[ג]
		שינויים מצטבר[ב]	אחת לשבוע	אחת ליום[ג]	אחת ליום[ג]
2	מחזור הגיבוי[ד]	מלא	2	4	8
		שינויים[ה]	3	13	6
		שינויים מצטבר[ו]	3	3	3
3	בדיקת תקינות תוך כדי ביצוע גיבוי ("Verify")	מלא	לא חובה	כן	כן
		שינויים			
		שינויים מצטבר			
4	בדיקת תקינות חודשית - קריאת גיבוי מדגמית[ז]	מלא	2%	5%	8%
		שינויים			
		שינויים מצטבר			
5	בדיקת שחזור מדגמית מגיבוי	מלא	שנתית 2%	חצי-שנתית 5%	תלת-חודשית 8%
		שינויים			
		שינויים מצטבר			
6	מספר העותקים הנדרש	מלא	1	2 עותקים של גיבוי אתרון[ח]	3 עותקים של גיבוי אתרון[ט]
		שינויים			
		שינויים מצטבר			

הערות לטבלה:

(א) הטבלה מחושבת לפי מודל סכמתי, הכולל מ-7 ימי עבודה בשבוע ו-4 שבועות בחודש.
כל ארגון יערוך התאמות של הערכים בטבלה לפי מספר ימי העבודה בשבוע ומספר השבועות בחודש.

(ב) הארגון יבחר אם לערוך גיבוי שינויים או לחלופין לערוך גיבוי שינויים מצטבר.

(ג) אחת ליום - הכוונה לימי עבודה.

(ד) המספרים הנמצאים ב-3 העמודות; בסיסית, בינונית וגבוהה, מייצגים את מספר דורות הגיבוי הנדרש במחזורי הגיבוי (מלא, שינויים ושינויים מצטבר).

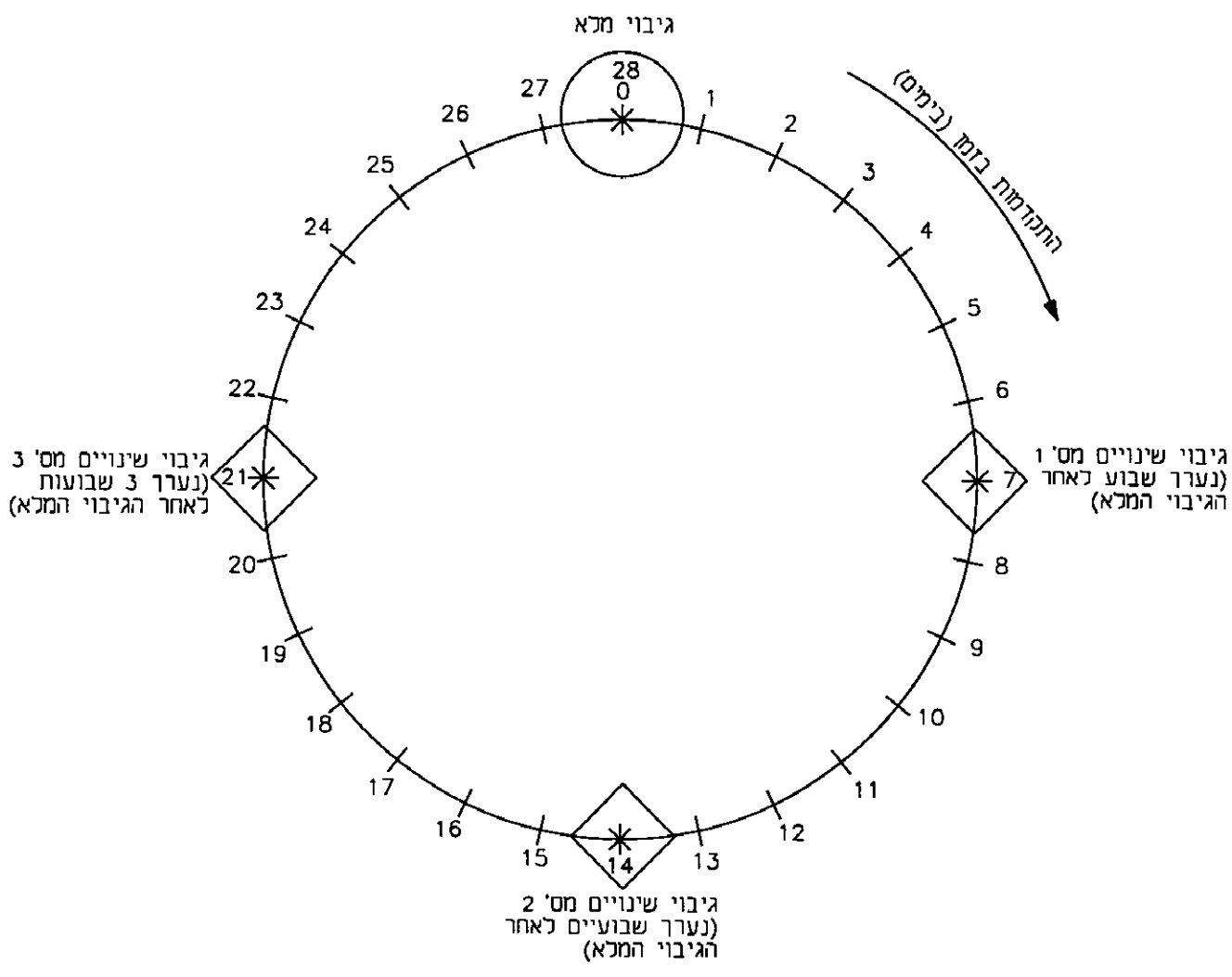
(ה) מספר דורות גיבוי השינויים הנדרש מושפע מתדירות הביצוע (בהתאמה לרמת האבטחה), ולפיכך מספר דורות גיבוי השינויים במחזור מושפע ממספר השבועות שבין גיבוי מלא אחד לגיבוי המלא שאחריו.
לדוגמה: ברמת אבטחה בסיסית, פרק הזמן בין גיבוי מלא אחד למשנהו הוא חודש וגיבוי שינויים נערך אחת לשבוע; לכן בחודש בן 4 שבועות יבוצעו 3 גיבויי שינויים (הגיבוי המלא הבא יהיה במקום גיבוי השינויים הרביעי).
ראו ציור 1.

(ו) מספר דורות הגיבוי נקבע ל-3, כדי לא להתבסס על עותק יחיד של גיבוי שינויים מצטבר.

(ז) לכל הפחות קריאת האינדקס הפנימי במצע.

(ח) 2 עותקים, שיאוחסנו האחד בסמוך למחשב והשני באזור סיכון השונה מאזור הסיכון של המחשב.

(ט) 3 עותקים, שיאוחסנו האחד בסמוך למחשב והשניים האחרים ב-2 אזורי סיכון נפרדים, השונים מאזור הסיכון של המחשב.



ציור 1 - מחזור גיבוי מלא ברמת אבטחה בסיסית

5. 2 תכנון גיבוי מיוחד

תכנון של גיבוי מיוחד ייעשה בדומה לעקרונות התכנון של גיבוי רגיל, תוך התחשבות במאפיינים המיוחדים שמהם נובע הצורך בגיבוי מיוחד.

6. ניהול יומן גיבויים

6. 1. עבור כל פעולת גיבוי ייערך רישום ביומן הגיבויים, והוא יכלול פרטים אלה:

א. סוג הגיבוי (ראו הגדרות 3.8 עד 3.17);

ב. תכולת הגיבוי (ראו הגדרה 3.3);

ג. מועד ביצוע הגיבוי;

ד. פרטי המצעים:

- סוג;
- כמות;
- תוויות[2] זיהוי המצעים;
- מספר העותקים.

ה. תוצאות ביצוע הגיבוי (הצלחה או כישלון, ותיאור הגורם לתקלה);
ו. מקום אחסון מצעי הגיבוי;
ז. זהות מבצע פעולת הגיבוי;
ח. זהות מבצע השינוע.

6. 2. ביומן הגיבויים יירשמו פרטי בדיקת הגיבוי האלה:
א. עותק הגיבוי שנבדק;
ב. סוג הבדיקה שבוצעה (סעיפים 3 עד 5 בטבלה 1);
ג. תוצאות הבדיקה;
ד. הגורם המבצע;
ה. מועד הביצוע.

6. 3. בכל אתר שמוחזקים בו מצעי גיבוי, תנוהל רשימת מצאי[2] מעודכנת, בהתאם לסעיף הדן בניהול מצעים שבתקן הישראלי ת"י 1495 חלק 2.

6. 4. ניתן לנהל יומן גיבויים ממוחשב או ידני או שילוב שלהם.

7. אחסון הגיבוי ושינועו

7. 1. אחסון הגיבוי ושינועו יהיו בהתאם לסעיפים הדנים בהחסנת מצעים ובהעברת מצעים שבתקן הישראלי ת"י 1495 חלק 2.

7. 2. תנאי האחסון והאבטחה הפיזית של מצעי הגיבוי יהיו בהתאם לסעיף הדן במצעים נושאי מידע והגנתם שבתקן הישראלי ת"י 1243.

8. בדיקת הגיבוי וניסוי שחזור

8. 1. הארגון יקבע מסגרת לבדיקת תקינות הגיבוי בהתאם לסעיפים 3 ו-4 בטבלה 1, במגמה לאמת את אמינותו של הגיבוי (זהות ההעתק למקור) ואת שלמותו (כל המידע האמור להיכלל בגיבוי אכן כלול בו).

8. 2. נוסף על כך ייעשה ניסוי שחזור, כדי לוודא שאפשר לשחזר את המידע באמצעות הגיבויים.

8. 3. הבדיקות והניסויים יבוצעו במועדים קבועים כנקוב בטבלה 1, וכן באופן אקראי.

8. 4. פרטי הבדיקות והניסויים ותוצאותיהם יתועדו ביומן הגיבויים או ביומן אחר.

8. 5. לקחים ומסקנות מן הבדיקות והניסויים ישמשו לעדכון ולשיפור של נוהלי הגיבויים.

9. שחזור המידע

9. 1. הארגון יקבע נוהל לביצוע מהיר ואמין של שחזור המידע, תוך שמירה על כללי הרשאות הגישה למידע הקיימים בארגון ולפי התקן הישראלי ת"י 1495 חלק 6[1].

9. 2. בנוהל תהיה חלוקה ל-2 סוגי שחזור מידע:

9. 2. 1. שחזור מלא, נכון למועד מסוים;

9. 2. 2. שחזור חלקי, נכון למועד מסוים.

9.3. בנוהל יפורטו עניינים אלה:

9.3.1. המידע הנדרש לשחזור;

9.3.2. מצעי הגיבוי הנדרשים ומקום אחסונם, בהתאם לרישום ביומן הגיבויים;

9.3.3. אופן שינוע מצעי הגיבוי בהתאם לתקן הישראלי ת"י 1495 חלק 2;

9.3.4. הכלים (תוכנות או פקודות מערכת) שבאמצעותם ייערך השחזור.

10. גיבוי חם

10.1. ארגון שעל פי צרכיו התפעוליים ואופי עבודתו נדרש לספק שירותי מידע רציפים, יערוך גיבוי חם בנוסף על הגיבויים הרגילים או כתחליף לחלק ממחזורי הגיבוי.

10.2. הבחירה באופן היישום של גיבוי חם מותנית ברמת השרידות והזמינות של שירותי המידע הנדרשים מן המערכת. אפשרויות הביצוע של גיבוי חם בהתאם לשיקולי זמן ומקום יהיו בהתאם לטבלה 2.

טבלה 2 - אפשרויות הביצוע של גיבוי חם בהתאם לשיקולי זמן ומקום

שיקולי מקום	שיקולי זמן	
	חם	חם קרוב לזמן אמיתי
באתר המחשב	ביצוע גיבוי חם בהתאם להגדרות 3.14 ו-3.16	ביצוע גיבוי חם בהתאם להגדרות 3.15 ו-3.16
מחוץ לאתר המחשב	ביצוע גיבוי חם בהתאם להגדרות 3.14 ו-3.17	ביצוע גיבוי חם בהתאם להגדרות 3.15 ו-3.17

10.3. גיבוי באמצעות תקשורת

10.3.1. בעת עריכת גיבוי באמצעות תקשורת יש לוודא, שרמת אבטחת המידע במתקן מאחסן הגיבוי ובמערכת המחשב שלו אינה פחותה מרמת האבטחה במתקן המקור.

10.3.2. תקשורת המחשבים תאובטח כנדרש בתקנים ישראליים אלה לאבטחת מערכות תקשורת[1]: ת"י 1972 חלק 1, חלק 2, חלק 3 וחלק 4.

10.4. בכל אפשרויות העריכה של גיבוי חם יש לנהל יומן גיבויים ממוחשב.

10.5. הארגון יקבע שיטה לבדיקת אמינותו ושלמותו של המידע הכלול בכל גיבוי חם.

רשימת מונחים

גיבוי (עותק גיבוי, פעולת גיבוי)	-	backup
דור גיבוי	-	backup generation
מצאי	-	inventory
נתונים	-	data
תווית	-	lable

כל המייצר מצרך, המתאים לדרישות התקנים הישראליים החלים עליו,
רשאי, לפי היתר ממכון התקנים הישראלי, לסמנו בתו תקן:

התקנים הישראליים עומדים לבדיקה מזמן לזמן, ולפחות אחת לחמש שנים,
כדי להתאימם להתפתחות המדע, הטכניקה והתעשייה.
המשתמשים בתקנים יוודאו, שבידיהם המהדורה המעודכנת של התקן על גיליונות התיקון שלו.

הצעות לשינויים יש לשלוח לפי כתובת מכון התקנים הישראלי:

מכון התקנים הישראלי
רח' חיים לבנון 42, תל-אביב 69977, טל' 03-6465154, פקס' 03-6412762
להזמנת תקנים: טל' 03-6465191/2 פקס' 03-6426762 library@sii.org.il
ובאתר מכון התקנים הישראלי:
WWW.SII.ORG.IL