ד.4 בדיקה בנושא הרשאות למתן הנחות

אבטחה ושמירת מידע מחויבים מכח החוקים:

1. סעיף 7א לחוק יסוד כבוד האדם וחירותי סעיף, התשנ"ב 1992 7א אשר קובע כי "כל אדם זכאי לפרטיות ולצנעת חייו".
2. חוק הגנת הפרטיות תשמ"א-1981 ותקנות (תנאי להחזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים) תשמ"ו – 1986 שהותקנו מכוחו.
3. חוק חופש המידע, תשנ"ח - 1998.
4. חוק המחשבים, התשנ"ה – 1995.

חוקים אלה מגדירים כללים הקובעים את חובות הרשות המקומית כמוסד ציבור בשמירה על מאגרי המידע הנתונים בידיה והאופן בו על הרשות המקומית לפעול על מנת להבטיח את ההגנה על פרטיות המידע מחד ואת זכויות האזרח לחופש המידע מאידך.

בכלל הסיכונים הכרוכים בניהול מערכות מידע ניתן למנות:

1. חשיפה של מידע אישי עליו חלה חובת החיסיון והסודיות.
2. זליגת מידע לגורמים בלתי רלוונטיים ו/או בלתי רצויים מחוץ לרשות המקומית.
3. שיבוש מידע האגור במערכות המידע על ידי הזנת נתונים שגויים למערכת, שינוי נתונים קיימים או מחיקתם
4. פעילות בלתי מורשית של עובדים, העלולה לסייע לגורמי חוץ לפגוע ברשות המקומית.

קיימים שני תקני ISO מרכזיים בתחום אבטחת מידע:

1. ISO –27001 תקן לניהול אבטחת מידע

התקן לניהול אבטחת מידע מגדיר עקרונות שיטתיים ותכליתיים להקמה, ניהול ותחזוקה של מערכת אבטחת מידע בהתאם לדרישות הארגון. התקן מתייחס למגוון נושאים, בין היתר: זיהוי וניהול הסיכונים למידע, בחירת הבקרות הנחוצות לארגון, הגדרת יעדים לניהול אבטחת מידע, התאמה לדרישות החוק והתקנות הרלוונטיות, תהליכים לשיפור ופיתוח, המשכיות עסקית ומניעת הונאות.

2. ISO – 27032 אבטחת מידע בתחום הסייבר

התקן נועד לסייע לארגונים להתמודד עם תופעת הסייבר וכולל מערך הנחיות והמלצות המסייעים לארגון להתמודד עם איומי סייבר.

מערך הרשאות תקין, המתאים למבנה הארגוני ולנוהלי הארגון, הכרחי ומהווה בסיס לניהול אבטחת מידע תקין.

מטרת הביקורת

מטרת הביקורת לבדוק האם קיימות הרשאות למתן הנחות לעובדים או לגורמים בלתי מורשים.

היקף הביקורת

הביקורת תתייחס להרשאה עבור "**מתן הנחה**".

קבצים ומסמכים נדרשים

פירוט מורשים לביצוע **עדכון** במסך מתן הנחה.

תוכנית הבדיקה

1. בדוק האם קיימות הרשאות לגורמים בלתי מורשים שאינם נדרשים להרשאה לצורך תפקידם.
2. בדוק האם קיימים בעלי הרשאות שכבר אינם מועסקים ברשות.
3. ככל שאותרו בעלי הרשאות לא תקינים – יש לציין את מספר הפעמים שבהם בוצעה כניסה למערכת החל מהמועד שבו ההרשאה היתה אמורה להתבטל או החל מ 01/01/2025 לפי המאוחר.
4. בריכוז ממצאי הדוח, יש להתייחס למצב ברשות המקומית לאחר תיקונים שביצעה, אם עשתה זאת. יחד עם זאת, יש לציין בשדה הייעודי בקובץ האקסל את מספר בעלי ההרשאות הלא מורשים (סעיפים 1 ו 2 לעיל) כפי שהיה בתחילת הבדיקה.
5. בקובץ האקסל, יש למלא את טבלת הנתונים בגיליון "בדיקת הרשאות הנחות":

- טור C "כן/לא" – בשדה C5 יש להשיב האם קיימת הרשאה למתן הנחות לגורמים לא מורשים כמוסבר בסעיפים 1 ו 2 לעיל. בשדה C6 יש לציין האם היו בעלי הרשאה שאינם מורשים בתחילת הבדיקה.
- טור D – אם התשובה בטור C "כן", היינו נמצאו בעלי הרשאות שאינם מורשים, יש לציין את מספרם. בשדה D5 יש לציין את מספר בעלי ההרשאות שאינם מורשים בסיום הבדיקה ובשדה D6 יש לציין את מספרם בתחילת הבדיקה.
- טור E – יש לציין את מספר הכניסות הכולל למסך מתן הנחה על ידי בעלי הרשאות שאינם מורשים; בסיום הבדיקה ובתחילתה.
- בדוח המפורט יש להוסיף טבלת פירוט של מספר הכניסות על ידי בעלי הרשאות שאינם מורשים:

כמות כניסות למסך מתן הנחה	מספר בעלי הרשאות
גורמים לא מורשים שביצעו כניסה 1	
גורמים לא מורשים שביצעו 2-5 כניסות	
גורמים לא מורשים שביצעו 5-10 כניסות	
גורמים לא מורשים שביצעו מעל 10 כניסות	

- בטורים F עד I קיימים שדות בקרה מחושבים:

יש לא מורשים ולא נרשם מספרם או מספר הכניסות – ערך בטור זה מציין כי חסרים נתונים בטורים D ו E, ויש להשלים.

יש לא מורשים בסיום הבדיקה ולא לפני תחילת הבדיקה או שמספרם בתחילת הבדיקה נמוך מהמצב בסיום הבדיקה – ערך בשדה G6 מציין כי קיימת טעות במספר הגורמים שאינם מורשים בטור D. לא יתכן שבסיום הבדיקה יהיו בעלי הרשאות שאינם מורשים, אך אין כאלה בתחילת הבדיקה. כמו כן, לא יתכן שמספרם בתחילת הבדיקה יהיה נמוך ממספרם בסיום הבדיקה. התראה תופיע בשדה זה גם במקרה שבו צוינו בטור D מספר ההרשאות הלא תקינות, אולם התשובה בשדה C6 נותרה "לא" במקום התשובה "כן".

אין לא מורשים ונרשם מספר לא מורשים או מספר כניסות לא מורשים – ערך בטור זה מציין כי נקלטו נתונים סותרים, ויש לתקן. אם התשובה בטור C היא לא, אין למלא נתונים בטורים D ו E.

לא מולאו התאים – ערך בטור זה מציין כי חסרים נתונים בטור C, ויש להשלים.