תמצית דוח ביקורת בנושא יישום התקנות להגנת הפרטיות - אבטחת מידע.

1. תמצית:

1.1 כללי:

תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז–2017 (להלן: "התקנות"), מפרטות את אופן יישומה של חובת אבטחת המידע המוטלת בחוק הגנת הפרטיות על כל גורם המנהל או מעבד מאגר של מידע אישי.

תקנות אלו נדרשות ליישום במועצה מתוקף היותה גוף ציבורי, התקנות מגדירות כי רמת האבטחה הנדרשת ברשת מקומית הינה בינונית.

בדוח הביקורת שערכתי, בחנתי את עמידת המועצה בדרישות המופיעות בתקנות.

הדרישות המופיעות בתקנות מפורטות ומנחות את המועצה כיצד עליה לפעול, יישומן של התקנות נדרש לא רק בשל הדרישה החוקית, אלא כהליך בסיסי הקיים בכל גוף שאבטחת המידע חשובה לו.

2.2 עיקרי הממצאים:

א. בניגוד לסעיף 17ב. לחוק הגנת הפרטיות המחייב מינוי ממונה על אבטחת מידע, **במועצה לא הוגדר ממונה על אבטחת מידע, מנהל מערכות המידע לא הוכשר כמנהל אבטחת מידע.**

ב. בניגוד לסעיף 3 לתקנות, לא קיים במועצה, נוהל אבטחת מידע, או תכנית בקרה שוטפת לעמידה בדרישות החוקיות.

ג. הוצג לביקורת סקר סיכונים שנערך במועצה בשנת 2013 בתחום תשתיות המיחשוב, סקר זה מצביע על סיכונים בתחום אבטחת המידע במועצה.

1. לא הוצג לביקורת מסמך המעיד על תיקון הליקויים ויישום ההמלצות בתחום אבטחת המידע שעלו בסקר.

2. למרות הזמן שחלף ממועד עריכת הסקר, לא נערך עדכון לסקר ולא נערכו בקרות תקופתיות.

ד. קיים שימוש במועצה במכשירים המאפשרים חיבור לרשת המחשבים ומאגרי המידע באופן אלחוטי וללא בקרה, כמו כן, ישנו שימוש במועצה בכתובות דואר אלקטרוני פרטיות לצורך עבודה.

ה. בקרת הגישה למערכת המחשב במועצה מבוססת על סיסמה ולא על אמצעי פיזי, ולמרות שאמצעי הגישה הינו סיסמה, לא קיימת דרישה לשינוי או הקשחת הסיסמאות במערכת מידי תקופה.

ו. שרתי מערכות המחשב במועצה נמצאים במקום נעול, אולם ללא מערכת התראת גישה, מערכת גילוי או כיבוי אש. וכן לא קיימים אמצעים לתיעוד הכניסה והיציאה מהאתר שבו נשמרות מערכות המחשב של המועצה, כנדרש בתקנות.

2.3 <u>המלצות</u>

א. בהתאם להנחיות החוק להגנת הפרטיות יש להגדיר במועצה ממונה על אבטחת מידע שלא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים, ואשר יוקצו לו "המשאבים הדרושים לו לשם מילוי תפקידו" (כלשון התקנות).

ב. בהתאם לתקנות, יש להגדיר במועצה נוהל אבטחת מידע ותכנית בקרה שוטפת לביצוע בקרות ולעמידה בדרישות החוקיות.

ג. על נוהל אבטחת המידע לכלול בין השאר התייחסות לנושא הסיסמאות: חוזק הסיסמה, מספר ניסיונות שגויים, תדירות החלפת הסיסמאות.

ד. מומלץ כי נוהל אבטחת המידע הנדרש בתקנות יופץ לאחר הכנתו ואישורו בין עובדי המועצה לצורך הטמעתו ויישומו.

ה. בהתאם לתקנות, יש לוודא כי סיסמת הגישה למחשבי המועצה תוחלף אחת לחצי שנה לפחות.

ו. יש למנוע גישה לרשת המחשבים במועצה באמצעים המאפשרים גישה אלחוטית ללא חיבור פיזי (כבל) לרשת.

ז. מומלץ כי השימוש בדואר האלקטרוני במועצה יבוצע באמצעות כתובות הדואר האלקטרוני של שרת המועצה בלבד.

ח. מומלץ למועצה כי הגישה לשרתי המחשב במועצה תוגן באמצעות מערכת התראת גישה, ובאמצעות מערכת גילוי וכיבוי אש.

ט. מומלץ למועצה ליישם את ההמלצות בתחום אבטחת המידע, שעלו בסקר הסיכונים בשנת 2013, ולעדכן את הסקר.

י. יש לוודא כי ההנחיות החלות על המועצה בתקנות הגנת הפרטיות (אבטחת מידע), ייושמו במלואן.

<u>תגובת מנהל מערכות המידע במועצה:</u>

אני מודה לביקורת על עריכתה ועל העלאת נושא אבטחת המידע לסדר היום, הפעולות שיבוצעו בקרוב:

א. הקשחת הסיסמאות לכל מחשבי המועצה.
ב. עריכת מסמך הגדרות למאגרי המידע.