דוח ביקורת אבטחת מידע

יוני 2024

עקרונות מדיניות אבטחת מידע

א- **ניתוח סיכונים** - בחינת תשתיות ופעילויות המועצה, תוך זיהוי איומים, הערכת חשיפות וקביעת מוקדי סיכון.

הביקורת מציינת כי, לא קיים ניתוח סיכונים מקצועי.

א- **עקרון "הצורך לדעת"** (Need to Know)- הגבלת תפוצת המידע לבעלי התפקידים הזקוקים לו.– **לא קיימת וועדה במועצה.**

ב- **זיהוי "בעלי המידע"** (Owners of Data)- הגורמים המאשרים שימוש במידע מסוים על ידי אנשים במועצה או מחוצה לו.

הביקורת מציינת כי, נדרשת פעילות במסגרת הדרכות מודעות לכלל עובדי המועצה.

א- **הגדרת הגורמים האחראים** על יישום מדיניות אבטחת המידע ומערכת הרשאות.

הביקורת מציינת כי, מוגדר חלקית באמצעות הרשאות מערכתיות.

א- סיווג המידע מבחינת רגישותו וחשיבותו למועצה, באופן בלתי תלוי במשתמשים. **הביקורת מציינת כי, לא מונה ממונה על אבטחת מידע.**

ב- **עיצוב מערכת הרשאות** - עקרון "הצורך לדעת" קובע את הרשאות הגישה והשימוש במידע. רמת רגישות המידע קובעת את כללי הגישה ואמצעי ההגנה והבקרה הנדרשים עבור כל הרשאת גישה.- **הביקורת מציינת כי, יש צורך להגדיר בכל מחלקה הרשאות למידע ומענה לכל גורם.**

אבטחת מידע ממוחשב

א- חסימת כל הכניסות החיצוניות למחשבי המועצה. נמצא כי, קיימים מספר מחשבים משרדיים עם כניסות חיצוניות. הביקורת ממליצה לחסום כל הכניסות.

ב- הביקורת ממליצה להגדיר עמדת "הלבנה" אחת באחריות מנהל המחשוב. רק בעמדה זו ניתן יהיה להשתמש באמצעים חיצוניים.

ג- הביקורת מציינת כי, לא נכתבו נהלי עבודה למחשבים ניידים בעבודה מרחוק, אבטחה והחלפת סיסמאות.(משחקי ילדים, שעות עבודה, הפרדת סיסמאות).

ד- נמצא כי, קיימת גישה לחיבור מרחוק לכ-39 עובדים. נדרש להגדיר רשימת מורשים לעבודה מרחוק, צריכה להיבחן מעת לעת.

נוהל קבלת/ עזיבת עובדים

א- הביקורת מציינת כי, לא קיים נוהל קבלת/ עזיבת עובדים:

- פתיחה/ סגירת יוזר.
- הגדרת/ סגירת הרשאות.
- החתמה על שמירת סודיות.
- תיבת המייל - ביטול וחסימת מייל.
- אישורים/ ביטול עבודה מרחוק.

מיפוי ואבחון מערכת המחשוב והאבטחה

א- מיפוי – תוואי הרשת, תוכנות בשימוש, הסכמים עם ספקי תוכנה.

ב- סקרי סיכונים- איתור נקודות תורפה במערכת המחשוב- לא קיים .

ג- מיגון מערכת המחשוב המועצתית (רשתות, שרתים, מחשבים ניידים וטלפונים).

ד- הגדרת תנאי סף לכניסת משתמשים למערכת המידע במועצה.

ה- מבחני חדירת גורמים עוינים.

אבטחת מידע ממוחשב

א- אין תכנית אב למחשוב .

ב- לא הוגדרה מדיניות אבטחת המידע במועצה.

ג- טרם בוצעה בחינת איומי סייבר ודרכי הגנה ומניעה .

ד- טרם הוקמה וועדת היגוי לטיפול בסייבר.

ה- לא קיימות בקרות מקצועיות תקופתיות.

ו- לא הוגדרו תפקידים ותחומי אחריות באבטחת מידע .

ז- טרם נכתבו נהלים בנושא אבטחת המידע במועצה.

ח- נדרשת פעילות הסברה ואכיפה בקרב העובדים.

ממונה אבטחת מידע

- אחראי על יישום מדיניות אבטחת המידע.
  - זיהוי נקודות תורפה וסיכונים במערכות.
  - המלצה לאפיון ומענה למערכות.
  - אחראי על בקרת אבטחת המידע בארגון.
  - אחראי על החדרה והטמעה של פתרונות אבטחת מידע בכל הרמות (תשתית ויישומים, נהלי אבטחת מידע) בארגון.
  - אחראי להנחות מקצועית את הארגון בהובלת נושאי אבטחת מידע.
- ***המועצה לא מינתה ממונה אבטחת המידע.***

מנהל מאגר מידע

א- ***לא נקבעו נהלים לאבטחת המידע ולהגנת הפרטיות למחשבים מנותקי רשת; לרבות טלפונים חכמים וכוננים נתיקים.***

ב- ***נדרש להגדיר נוהל המסדיר את דרכי ההגנה על המידע הנאגר במחשבים, כדי לצמצם את הסיכון שבגנבת הציוד - חשיפת המידע השמור בו ונגישות לרשת.***

ג- הביקורת ממליצה, לתקף האכיפה על הנהלים בתחומים: עבודה של גורמי חוץ, הסברה לעובדים, למנהלים, ובקרות ביצוע.

הערכת סיכונים

א- המועצה לא ביצעה הערכת סיכונים במערכות המידע.

ב- יש לקבוע תדירות סקירה בהתאם לרגישות המערך, ולקיים דיונים על תוצאות סקרי אבטחת המידע ומבחני החדירה ולפעול למימוש המלצותיהם תוך פרק זמן סביר. שש

- יש לקיים סקרי אבטחת המידע ומבחני החדירה תקופתיים -ע"י גורם מקצועי, עצמאי, בלתי תלוי וחיצוני לארגון.

א- נדרש ליישם את ממצאי סקר הסיכונים בתכנית העבודה .

שיקום מאסון

א- במועצה לא קיימת תכנית שיקום מאסון ותוכניות להמשכיות עסקית.

ב- יש לציין כי קיימים פתרונות חלקיים להתמודדות במקרה שריפה, הצפה, פגיעת טילים.

ג- נדרשת הגדרה וביצוע יזום של תהליך שחזור מגיבוי אחת לחצי שנה.

המלצות

א- למנות ממונה לאבטחת המידע.

ב- לבצע מיפוי ואבחון מערכות המידע במועצה.

ג- לבצע מבחני חדירה .

ד- לבחון תהליך התאוששות מאסון והמשכיות תפקודית.

ה- לקיים תיקוף לנהלים הקיימים: למנהלים, עובדים, מנהלי מערכות המידע.

ו- לקיים פעולות בקרה שגרתיות בתחום אבטחת המידע והגנת הפרטיות.