דוח הביקורת לשנת הביקורת

2020-2021

1. מוכנות למתקפות סייבר

2.מעקב אחר תיקון הליקויים באבטחת המידע

1. נתונים כללים על מועצה אזורית גלבוע

1.1 מעמד מוניציפאלי ושטח שיפוט:

מועצה אזורית הגלבוע היא מועצה אזורית במחוז צפון, השוכנת בחלקו המזרחי והדרומי של הגלבוע והסביבה למרגלות הר הגלבוע.

- בצפון: מועצה אזורית עמק יזרעאל.
- במערב: מועצה אזורית מגידו.
- בדרום: מועצה אזורית שומרון.
- במזרח: מועצה אזורית עמק המעיינות.

1.2 סה"כ 33 ישובים. שמות הישובים:

- קיבוצים: בית אלפא, בית השיטה, גבע, חפציבה, יזרעאל, עין חרוד איחוד, עין חרוד מאוחד, תל יוסף.
- מושבים: אביטל, אדירים, ברק, גדיש, דבורה, כפר יחזקאל, מגן שאול, מולדת, מיטב, מלאה ,פרזון, רם און, רמת צבי.
- ישובים קהילתיים: גדעונה, גן נר, מרכז אומן, מרכז יעל, מרכז חבר, ניר יפה, נורית.
- כפרים ערביים: טייבה, טמרה, נאעורה, סנדלה, מוקיבלה.

1.3 שם ראש המועצה ותחילת כהונתו :

ראש המועצה הנבחר מר עובד נור החל את כהונתו בשנת 2015

1.4 מספר חברי מועצה

37 חברים במליאת מועצה אזורית גלבוע עפ"י בחירות 2018.

1.5 מספר תושבי המועצה ומספר בתי אב.

- *מספר תושבי המועצה כ- 32,000 תושבים*
- *קצב גידול שנתי של האוכלוסייה 1.8% (עפ"י הלמ"ס נכון לסוף 2017)*
- הדרוג הסוציואקונומי (חברתי כלכלי) 5.

ביקורת בנושא מוכנות למתקפת סייבר

תקציר מנהלים

להלן עיקרי ממצאים, מסקנות והמלצות מדו"ח ביקורת שנערך במועצה אזורית גלבוע בנושא: מוכנות למתקפת סייבר :

*** לשם קבלות החלטות רצוי לעיין בדו"ח המלא ולהמלצות שבסופו.**

1. רקע

1.1 הזכות לפרטיות היא אחת מזכויות האדם החשובות בישראל. עניינה של הזכות לפרטיות הוא בשמירה על האוטונומיה של האדם, בשמירה על צנעת חייו ועניניו האישיים ואף בהגנה על האדם מפני שימוש לרעה במידע על אודותיו. מאגרי מידע מסכנים בעצם קיומם את הפרטיות, ועל כן יש צורך בקביעת מנגנונים ייחודיים להגנה על המידע הנאגר בו.

1.2. איסוף המידע כיום פשוט יותר מהעבר, וניתן לאסוף מידע על אדם אגב שימוש שהוא עושה בשירותים רבים.

מתקפות הסייבר הפכו תדירות יותר ומהוות את אחד הסיכונים הגדולים לארגונים ולמאגרי המידע שבאחריותם , כאשר המתקפות משמשות מצד אחד כנשק בידי מדינות כחלק מהלוחמה הכוללת ובין המלחמות , ומצד שני כחלק מניסיונות של האקרים (פצחנים) לחדור למערכות המידע ולבצע פשעים כלכליים. בשנים האחרונות ישראל בפרט יחסית לגודל אוכלוסייתה , משמשת כיעד מועדף למתקפות בעלות אפיון לאומי ואף ניסיון פגיעה בנפש, כחלק מהמערכה בין המלחמות מול אירן בין השאר, בניסיון להתקיף תשתיות מים והגדלת רמת הכלור בתוכם (ביצוע ניסיון הרעלת האוכלוסייה) המוסף להם בשגרה , באמצעות שימוש במערכות מידע. בנוסף לאחרונה בוצעו הפעלות יזומות חיצוניות למערכות האתראה לחירום מרחוק (אזעקות) - כאתראות שווא על מנת לזרוע פאניקה באוכלוסייה, בכמה ערים בישראל . וכן בניסיונות גוברים לבצע פשעים כלכליים. מכאן נגזרים הסיכונים הגבוהים לארגונים במגזר הציבורי בארץ ביניהן גם המועצה האזורית הגלבוע.

בעת חקיקתו, נועד חוק הגנת הפרטיות להתמודד עם מציאות של מאות מאגרי מידע שחייבים ברישום. בשנת 1981 נחקק חוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות), במטרה "לשריין את ההגנה של האדם לזכותו לפרטיות". כיום אנו נמצאים במציאות של קיום מיליוני מאגרי מידע ומכאן הסיכון לחשיפת הנתונים , אשר העלה בצורה משמעותית את היכולת לפרוץ למאגרי המידע. הסיכון תלוי גם משמעותית בפעולות ההגנה , אשר ננקטות על מנת לאיין ולהקטין את היכולת לפרוץ למאגרי המידע.

1.3. במועצה אזורית גלבוע ישנם 9 מאגרי מידע.

1.4. יחידת מערכות המידע במועצה אזורית גלבוע אמונה על מתן שירותי מחשב לעובדי המועצה, ניהול המשתמשים, אבטחת המידע ותפעול שוטף של מערכות המחשב במועצה. דובר המועצה האזורית

גלבוע אמון על מאגרי המידע, חובת הרישום בפנקס רשם מאגרי מידע שבמשרד המשפטים, פרסום שמות המאגרים לציבור באתר המועצה, שימוש במשאבי מערכות מידע של המועצה וספקים חיצוניים של מאגרי המידע לאבטחת המידע, שמירת סודיות המידע הנגשת המידע רק למורשים וגיבוי המידע לצרכים המשפטיים ואחרים העתידיים של המועצה .

1.5. בכל גוף ארגוני במרוצת השנים נפתחים מאגרי מידע חדשים והקיימים גדלים בנפחם, חוק הגנת הפרטיות נועד להתמודדות עם גידול זה ומהווה את הדגשים בטיפול מאגרי מידע.

1.6. נדרש זיהוי מאגרים קיימים חדשים ושינוי התייחסות אליהם באמצעות הגדרתם , כמאגר מידע רשמי הנדרש להיות כפוף תחת תקנות הגנת הפרטיות. לפיכך יש לערוך בקרה באמצעות ממונה אבטחת המידע והאחראי על המאגרים , לבדיקת השינויים במאגרי המידע (תוספת , גריעה).

3. <u>מדיניות אבטחת מידע ותוכנית עבודה</u>

3.1. בניגוד לנוהל המסגרת, לא קיים במחלקה מסמך מדיניות ונוהל אשר מפרט כיצד על המחלקה ועל המשתמשים המועצה להתנהל בתחום המחשוב בכלל ובתחום אבטחת המידע בפרט. על הנוהל לכלול פרטים נדרשים , כגון: הוראות בעניין האבטחה הפיזית והסביבתית של אתרי המאגר, הרשאות גישה למאגר המידע ולמערכות המאגר, תיאור של אמצעים שמטרתם הגנה על מערכות המאגר ואופן הפעלתם לצורך כך, הוראות למורשה הגישה למאגר המידע ולמערכות המאגר לצורך הגנה על המידע במאגר, הסיכונים שחשוף להם המידע שבמאגר במסגרת הפעילות השוטפת של בעל מאגר המידע, לרבות אלה הנובעים ממבנה מערכות המאגר, אופן קביעת סיכונים אלה, ואופן הטיפול בהם, לרבות על ידי מנגנוני הצפנה מקובלים להגנה על המידע , השמור במאגר או במערכות המאגר; אופן התמודדות עם אירועי אבטחת מידע לפי חומרת האירוע ומידת רגישות המידע; הוראות לעניין ניהול של התקנים ניידים ושימוש בהם.

3.2. **הממונה על אבטחת מידע לא הכין תכנית לבקרה שוטפת אך בוצע מיפוי וסקר סיכונים באמצעות מטה הסייבר הלאומי בעבר וכן בשנה האחרונה על ידי ממונה אבטחת המידע ברשות , אך טרם הועברו הממצאים על ידו בדוח כתוב.**

4. <u>טיפול באירועי אבטחת מידע</u>

4.1. **קיים נוהל פנימי וחיצוני במחלקת מחשוב במועצה , משנת 2021 אשר מנחה מהו הטיפול הנדרש באירועי אבטחת מידע.** הנוהל נשלח במייל לכל העובדים אשר מחוברים לרשת והתבקשו לקרוא את המסמך , לחתום ולהחזיר במייל חוזר למנהל מערכות המידע.

4.2. במחלקת מחשוב של המועצה **קיימים כלי ניטור על פעילות המשתמשים בצורה חלקית** , זאת מאחר והמלצות הממונה על אבטחת המידע לרכישת ציוד EDR לא יושמו בשל העובדה שהמועצה החליטה לקבל תוכנה הגנה מפני מתקפת סייבר שהוצעה למחלקת מחשוב, אשר ניתנה לשימוש המועצה במסגרת פיילוט , ללא תשלום מחודש יוני 2021 ועד לחודש דצמבר 2022 (לאחר הארכת המועד המקורי יוני 2022). **במקביל טרם נמסרו תוצאות המבדק הפנימי שנערך על ידי הממונה על אבטחת המידע וטרם בוצע מבדק חיצוני למערכת התוכנה , שהתקבלה כאמור כפיילוט ברשות.**

5. <u>בעל הרשאה</u>

5.1. לא התקבל מידע מלא האם כל 9 חברות החיצוניות שעובדות עם המועצה ושקיבלו הרשאה להחזיק במידע , חתמו על הסכם סודיות.

5.2 נמצא כי המועצה לא הגדירה לבעלי ההרשאה מסמך הגדרות ובכך , הגדילה את הסיכוי לפגיעה במאגרי המידע המוניציפאליים.

6. מיקור חוץ

ב 9 החברות שנמסר שמם , לא התקבל מידע האם החברות חתמו על טופס התחייבות לשמירת סודיות וכן האם בטרם ביצוע ההתקשרות בוצע סקר סיכונים לצורך אבטחת המידע.

7. שקיפות

במועצה ישנם 9 מאגרי מידע כפי שמצאה הביקורת , אולם בדוח לתושב לא נכללים שמותיהם של מאגרי המידע ובאתר האינטרנט של מועצה אזורית גלבוע לא מצוינים מספרם ושמותיהם של מאגרי המידע ולכן הביקורת מעירה כי יש לפרסם באתר המועצה ובדוח לתושב את כלל מאגרי המידע הקיימים , לאחר תהליך הרישום מול משרד המשפטים.

8. מעקב אחר דו"ח ביקורת מבקר המועצה בנושא אבטחת מידע שבוצע בשנת 2014

בשנת 2014 בוצעה ביקורת בתחום אבטחת מידע ע"י מבקר המועצה מר אייל פייגנבאום. ממצאי המעקב מעלים, כי המועצה פעלה לתיקון הליקויים הקריטיים והעיקרי שבהם היה שימוש בשרת המועצה לצורך שירותי ה- wi-fi שהמועצה מספקת לעובדים , לתושבים ולכל אדם שביקר במתחם המבנה הראשי של המועצה , כך שהמועצה הייתה חשופה בעבר לפריצה מרחוק וכניסה למערכות המידע שבשימושה.

תיקון הליקוי העיקרי בדוח הביקורת בתחום אבטחת המידע לשנת 2014:

שירותי האינטרנט האלחוטי במועצה האזורית הגלבוע, שסופקו בעבר על ידי המועצה , ניתנים כיום על ידי ספק חיצוני למערכת המועצה, השינוי התבצע לפני כ- 7 שנים. השינוי המבורך הקטין בצורה משמעותי פריצות ופגיעה במערכות המידע של המועצה.

היות והשימוש באינטרנט האלחוטי לא מאפשר כניסה דרך מערכות המידע של המועצה כבעבר.

שינוי השימוש בשרת המועצה לאינטרנט האלחוטי במועצה - לרשת אלחוטית חיצונית ע"י מחלקת מחשוב , הקטין בצורה משמעותית את הסיכון לחדירות למחשבי המועצה , מפני שהפרדת הרשתות ביטלה את האפשרות לכניסה לא מורשית דרך רשתות אלחוטיות לרשת המועצה.

בעקבות ההחלטה על השינוי , הוסב קו בזק לחיבור אינטרנט אלחוטי ע"מ שכל אורח / עובד אשר זקוק לחיבור אינטרנט , יוכל לעשות זאת ברשת מנותקת לחלוטין מרשת המועצה.

יחד עם זאת, הביקורת מוצאת כי יש להמשיך לפעול לתיקון הליקויים בשלמותם.

מבקר המדינה פרסם דוח שבוצע בשנת 2017 בעיריית באר שבע, דו"ח זה מקיף את נושא אבטחת המידע ומביא דרך לוגית פשוטה לבחינת אבטחת המידע בעיריות ומועצות להלן בראשי פרקים עיקרי ההמלצות :

- **נהלים לאבטחה לוגית.**
- **בקרה ופיקוח לוגים.**
- **אבטחת חומרה.**
- **הדרכה והסברה.**

1 רקע כללי

1.1 מרחב הסייבר הוא תולדה של קדמה טכנולוגית, קישוריות וחיבור גלובלי לרשת האינטרנט.

1.2 התלות הגוברת במרחב הסייבר מביאה עמה בשורות של חדשנות טכנולוגית ופיתוחים אדירים לאדם ולסביבתו.

1.3 לצד אלה מתפתח מרחב איומים, המשפיע על הרציפות התפקודית הארגונית, על שלמות תהליכי הייצור ועל סודיות המידע הארגוני.

1.4 מתקפות סייבר עלולות לפגוע בארגונים ואף להביא להפסקת תהליכי ייצור, לנזק כלכלי ולפגיעה במוניטין של הארגון.

1.5 מדינת ישראל עושה מאמץ לאומי בהגנת הסייבר במרחב האזרחי , כחלק מתפיסה הולכת וגוברת שהסייבר הופך לנשק אשר משתמשים בו בפועל כחלק ממערכה בין מדינות בשילוב עם מלחמות פיזיות ובמבם (מערכה שבין המלחמות).

1.6 תורת ההגנה הארגונית הינה נדבך בתפיסת ההגנה הלאומית, המורכבת מרבדים שונים של הגנה על המשק הישראלי ועל הרציפות התפקודית שלו. כך שניתן כיום ביתר שאת לסווג את המוכנות לסייבר , כחלק מההערכות למצבי חירום.

1.7 תורת ההגנה הלאומית רואה את הארגון כמכלול שלם ומאפשרת את העלאת רמת החוסן הארגוני באמצעות הטמעה רציפה של תהליכים, שיטות ומוצרי הגנה.

יישום תורת ההגנה הארגונית ישפר את החוסן הארגוני ואת העמידות הארגונית בפני

1.8 לטובת בניית תכנית העבודה, הארגון יגדיר תחילה על מה הוא נדרש להגן, מהי רמת ההגנה הנדרשת, מהם פערי ההגנה אל מול המצב הרצוי ולבסוף יבנה תכנית עבודה לצמצום הפערים.

1.9 הזכות לפרטיות היא אחת מזכויות האדם החשובות בישראל. עניינה של הזכות לפרטיות הוא בשמירה על האוטונומיה של האדם, בשמירה על צנעת חייו ועניניו האישיים ואף בהגנה על האדם מפני שימוש לרעה במידע על אודותיו. עם חקיקת חוק יסוד: כבוד האדם וחירותו אף הוקנה לה מעמד חוקתי על חוקי. סעיף 11 לחוק היסוד קובע כי "כל רשות מרשויות השלטון חייבת לכבד את הזכויות שלפי חוק יסוד זה". כמו כן, הזכויות החוקתיות לכבוד ולפרטיות מטילות על המדינה חובה להגשימן באמצעים העומדים לרשותה.

2.0 מידע פרטי הוא בעל ערך רב, לרבות ערך כלכלי, ולכן לחברות מסחריות ולגופים אחרים אינטרס ברור באיסופו ובשמירתו במאגרי מידע. בנוסף, בידי רשויות המדינה מידע רב על בני אדם, הנוגע לכל היבטי חייהם, וקיים חשש שייעשה בו שימוש שלא למטרה שלשמה הוסמכו הרשויות לאוספו. מאגרי מידע מסכנים בעצם קיומם את הפרטיות , ועל כן יש צורך בקביעת מנגנונים ייחודיים להגנה על המידע הנאגר בו.

2.1 צורך זה מתעצם בשל ההתפתחות הטכנולוגית מרחיקת הלכת של העשורים האחרונים, שהביאה עמה שינויים באופן שבו מידע נאסף ומעובד ובשימושים הנעשים בו. איסוף המידע כיום

פשוט מאשר בעבר, וניתן לאסוף מידע על אדם אגב שימוש שהוא עושה בשירותים רבים, כגון גלישה באינטרנט או תשלום בכרטיס אשראי, תוך הצלבת נתונים אלה עם נתונים אחרים וביצוע חיתוכים במידע שנאסף. כתוצאה מכך, נוצרו איומים חדשים על הזכות לפרטיות במידע. בהתייחס לכך ציין בית המשפט העליון 1 כי "אמצעי המחשוב המודרניים והטכנולוגיה המתקדמת בתחום התקשורת מביאים עמם ברכה רבה בצד סכנות גוברות לפגיעה בזכותו של האדם לפרטיות".

1.9 בשנת 1981 נחקק חוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות), במטרה "לשריין את ההגנה של האדם לזכותו לפרטיות"1. בשל הפגיעה הפוטנציאלית הגלומה במאגרי מידע יוחד בחוק פרק לנושא זה, ונקבעה בו חובה לרשום מאגרי מידע 2. לפני ניהולם והחזקתם, בפנקס המנוהל על ידי רשם מאגרי המידע. במרוצת השנים הוטלו אגרה עבור רישום מאגרי מידע ואגרה תקופתית על מאגרי מידע רשומים. מטרת הרישום היא לאפשר בקרה ופיקוח על המאגרים, להביא להגנה על פרטיות המידע ולאפשר לציבור לדעת על קיומו של מידע על אודותיו במאגרי המידע. לצד חובת הרישום, מטיל החוק חובות מהותיות על בעל מאגר מידע והמחזיק בו, בהן אחריות לאבטחת המידע האגור במאגר, שמירת סודיות המידע והימנעות משימוש בו שלא למטרה שלשמה נמסר.

1.10 בעת חקיקתו, נועד חוק הגנת הפרטיות להתמודד עם מציאות של מאות מאגרי מידע שחייבים ברישום. במהלך השנים השתנתה מציאות זו לחלוטין, ובשנים האחרונות רווחת ההערכה כי ישנם בישראל מיליוני מאגרי מידע החייבים, על פי הוראות החוק, ברישום. כמעט לכל בית עסק לפחות מאגר מידע אחד החייב ברישום, ואף רבים מהטלפונים החכמים שבידי אנשים פרטיים מכילים מאגרי מידע החייבים, לכאורה, ברישום .

1.11 איסוף המידע כיום פשוט מאשר בעבר וניתן לאסוף מידע על אדם אגב שימוש שהוא עושה בשירותים רבים. כאמור בעת חקיקתו, נועד חוק הגנת הפרטיות להתמודד עם מציאות של מאות מאגרי מידע שחייבים ברישום שנת 1981 נחקק חוק הגנת הפרטיות, התשמ"א-1981 (להלן חוק הגנת הפרטיות), במטרה "לשריין את ההגנה של האדם לזכותו לפרטיות" .

2. <u>רקע ייחודי</u>

2.1 מאחר וארגונים פועלים בסביבה דינאמית, שינויים בטכנולוגיה, באופי החברה ובתחומי פעילותה משפיעים על האופן בו הארגון נדרש להגן על עצמו במרחב הסייבר.

2.2 תורה זו נבנתה באופן שלוקח בחשבון את העובדה, כי על הארגון לבצע תהליך הערכת סיכונים באופן תקופתי.

2.3 הערכת סיכונים זו, היא הבסיס לבניית תכנית עבודה רב שנתית למזעור הפערים (מימוש בקרות נדרשות).

---

[1] ה"ח 1453 התש"ם, 206.

[2] סעיף 8(ג) לחוק קובע שבעל מאגר מידע חייב ברישומו בפנקס אם מתקיימת בו אחת מהנסיבות המנויות בסעיף, בהן שמספר האנשים שמידע עליהם נמצא במאגר עולה על 10,000 ; המאגר מכיל מידע רגיש כהגדרתו בחוק ; המאגר משמש לשירותי דיוור ישיר.

2.4 יחידת מערכות המידע במועצה אמונה על שרותי מחשב ל כ- 200 עובדי המועצה, ניהול משתמשים, אבטחת המידע ותפעול שותף של מערכות המחשב במועצה.

במועצה פועלות מערכות מידע ממוחשבות רבות החיוניות להבטחת תקינות פעילותה השוטפת בתחומים האלה: כספים (גבייה, שכר, תשלומים לספקים ועוד); תכנון ובנייה; חינוך (שירות פסיכולוגי חינוכי, גני ילדים, קייטנות ועוד); רווחה; כוח אדם; רישוי עסקים תחבורה וחניה; תברואה ועוד. מאגרים אלה הם הבסיס לעבודתם של הרשויות.

2.5 שמירה על עדכניות ההגנה לאור דינאמיות מרחב הסייבר בארגון. התהליכים והטכנולוגיות המוטמעים בארגונים משתנים כל הזמן - מחשבים ורשתות חדשים מותקנים, תוכנות מתקדמות נרכשות, רכיבים חדשים מקושרים למרחב הסייבר (למשל Things of Internet)
מוצעים שירותים חדשים כגון מחשוב ענן ועוד. מנגד, גם האיומים ושיטות התקיפה האפשריות על הארגון משתנים, ועקב כך – גם כלי ההגנה הנדרשים.

3. חוקים, הוראות ונהלים

a. **צו המועצות המקומיות (מועצות אזוריות), תשי"ח-1958**
b. **חוק יסוד כבוד האדם וחירותו על פיו "כל אדם זכאי לפרטיות ולצנעת חיו".**
c. **חוק הגנת הפרטיות, תשמ"א- 1981 (להלן: "חוק הגנת הפרטיות")**
d. **תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבורים), תשמ"ו- 1986**
e. **חוק המחשבים, התשנ"ה- 1995.**
f. **חוק העונשין, תשל"ז-1977 הקובע את העונשים החלים על עובדי ציבור שמוסרים מידע שלא כחוק.**
g. **חוק להסדרת ביטחון בגופים ציבוריים, התשנ"ח- 1998, הקובע את דרכי הפעולה והניהול של הביטחון ובכלל זה אבטחת מידע ממוחשב ומידע פיזי רשומות בגופים ציבוריים.**
h. **תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017.**
i. **נהלי מסגרת לאבטחת מידע משרד ראש הממשלה של אגף בכיר לביקורת המדינה והביקורת הפנימית המועצה המייעצת לביקורת ואבטחת מידע, הרשות הלאומית להגנת הסייבר, ספטמבר 2005 .**

4. מטרות הביקורת

a. **איתור חריגות מחוקים, הוראות ונוהלי עבודה.**
b. **איתור חריגות מסמכויות.**
c. **איתור סיכונים עסקיים ותפעוליים.**
d. **איתור ליקויים מערכתיים (כגון: חסר או ליקוי בנהלים, ליקויי תוכנה).**
e. **איתור מקרים בהם קיים חשד לפגיעה בטוהר מידות מצד עובדי המועצה.**
f. **איתור מקרים בהם קיימת פגיעה בחיסכון, בשמירה על הרכוש וביעילות העבודה.**
g. **הביקורת בחנה את ההיבטים השונים הקשורים לנושא ההגנה מפני מתקפת סייבר.**
h. **כמו כן, הביקורת בדקה האם פעילות המועצה בתחום הגנת הסייבר , מתבצעת תוך שמירה על חוקיות, סדירות, עקרון השוויון, חסכון, יעילות שקיפות ומניעת פגיעה בטוהר המידות.**

5. **היקף הביקורת ואופן הבדיקה :**

a. **במהלך החודשים נובמבר 2020 ועד דצמבר 2021 בוצעה ביקורת במועצה אזורית גלבוע.**

b. **הביקורת בוצעה בהתאם לתוכנית העבודה של מבקר המועצה לשנת 2020. הנושא נכלל בתוכנית העבודה השנתית, בשל הסיכונים הכרוכים בו ובהתאם לסמכותו בחוק.**

c. **הביקורת הסתמכה על הוראות החוק כפי שמופיעות בסעיף 3 בדו"ח זה.**

d. **מבקר המועצה השתתף כחלק מהצורך בעדכונים בתחום מוגנות ממתקפות סייבר , באירועי שבוע הסייבר , המתרחשים כל שנה ומאורגנים על ידי מטה הסייבר הלאומי בישראל.**

e. **הביקורת בחנה את ההתנהלות המועצה ביחס לניהול מאגרי מידע במועצה האזורית גלבוע בין השנים 2017-2022 וכללה את ההיבטים הבאים: רישום מאגרי מידע, שקיפות המידע, הסכמי סודיות עם חברות הפועלות על מאגרי המידע והאמצעים הטכנולוגיים להתמודדות עם מתקפות סייבר ועוד.**

f. **לצורך ביצוע הביקורת נעזרה בדוחות ביקורת נוספים וביניהם:**
דוח מבקר המדינה מספר 64ג', משנת 2014 בנושא רישום מאגרי מידע בישראל.
כחלק מהתובנות מהשתתפותי באירועי שבוע הסייבר, בחרתי להיעזר במסמך שפותח ע"י מערך הסייבר הלאומי לטובת הציבור. המסמך מהווה המלצה לכלל הארגונים במשק הישראלי. ניתן להשתמש בו לטובת העלאת החוסן בסייבר במשק באופן חופשי. מסמך זה נכתב עבור דירקטוריונים והנהלות של חברות, מנהלי הגנה בסייבר ומיישמים וספקי IT .
המסמך מציג את דרישות ההגנה המינימאליות הנדרשות בהתאם לפוטנציאל הנזק. תכנית ההגנה לארגון הנגזרת ממסמך זה מותאמת למידת התלות של הארגון בסייבר. ארגונים נדרשים לבצע תהליך הערכת הסיכונים ויכולים לבנות תכנית הגנה מחמירה מדרישות מסמך זה. המסמך פונה לכלל המשק ונכתב בלשון זכר.

1. **הגדרות**

1.1. **"מאגר מידע" - אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט –**
(1) אוסף לשימוש אישי שאינו למטרות עסק; או
(2) אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר איפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף;

1.2. **"מידע" - נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו.**

1.3. **"מנהל מאגר" - מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לעניין זה;**

להלן ממצאי הביקורת

1. כללי

יחידת מערכות המידע במועצה אמונה על מתן שירותי מחשב לעובדי המועצה, ניהול המשתמשים, אבטחת המידע ותפעול שוטף של מערכות המחשב במועצה.
היחידה מטפלת במאות מחשבים / שרתים. לצורך ביצוע חלק ממשימותיהם, על היחידה לעבור פיזית בין אתרים שונים בהם נמצאים מחשבי ושרתי המועצה.

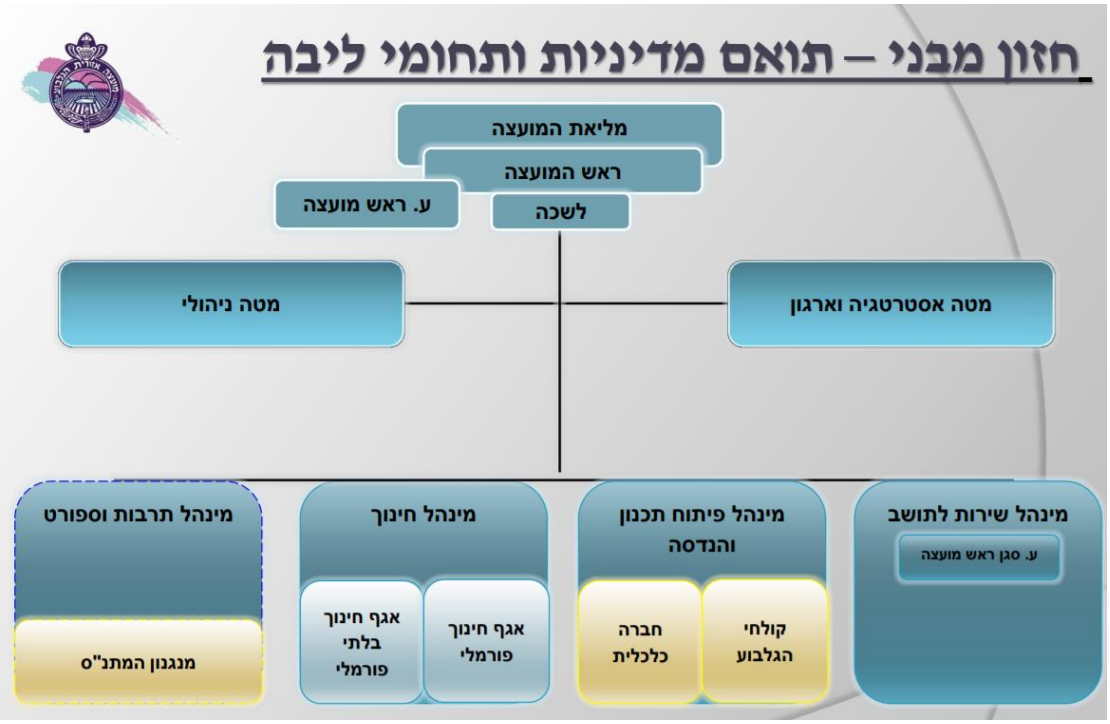
2. פרק 3- מבנה ארגוני וכתב מינוי

2.1. האגף לכח אדם ושכר ברשויות מקומיות במשרד הפנים קובע כי יש למנות מנהל מערכות מידע ראשי (מנמ"ר), אשר יתכנן וינהל את מערכות המידע הניהוליות של הרשות המקומית. בין היתר, נקבע כי ברשות מקומית ברמה א' המנמ"ר יהיה כפוף למנכ"ל או סמנכ"ל הרשות, וכי ברשות מקומית ברמה ב' או ג', המנמ"ר יהיה כפוף למנכ"ל או מזכ"ל הרשות.

2.2. נמצא כי בהתאם להנחיות אגף משאבי אנוש במשרד הפנים הקובעות כי המנמ"ר יהיה כפוף מנהלתית למנכ"ל המועצה, המנמ"ר כפוף למנכ"לית המועצה.

2.3. במועצה התמנה ממונה על אבטחת מידע , עם כתב הסמכה מהמועצה.

להלן המבנה הארגוני של המועצה:



3. ועדת היגוי לאבטחת מידע

3.1. נוהל מס' 5 לנהלי המסגרת בנושא "ועדות היגוי למחשוב ואבטחת מידע" קובע כי ועדת ההיגוי תתכנס לפחות פעמיים בשנה ותורכב מנושאי המשרה הבאים:

- **סמנכ"ל בכיר**
- **מנהל אגף מחשוב**
- **חשב/ גזבר**
- **המבקר הפנימי**
- **נציג היועץ המשפטי**
- **קצין הביטחון**
- **הממונה על אבטחת מידע**

<u>הנוהל קובע כי הועדה תעסוק, בין היתר, בנושאים הבאים:</u>

- **קביעת מדיניות המחשוב ואבטחת מידע.**
- **אישור תוכנית עבודה שנתית בתחום אבטחת המידע, לרבות תקציבים, לוחות זמנים ותחומי אחריות.**
- **קבלת דיווחים ומעקב ביצוע בנושאי אבטחת מידע.**

- **סיווג המידע (רגיש/ סודי/ אישי/ פומבי).**

3.2. כנדרש בנוהל מסגרת מס' 5. קיים במועצה נוהל העוסק בפעילות וועדת היגוי לאבטחת מידע בהשתתפות מנכ"לית, מנמ"ר, דובר והיועץ המשפטי של המועצה .

4. פרוטוקול הוועדה לא מפורסם באתר המועצה.

5. <u>פרק 5 – מדיניות אבטחת מידע ותוכנית עבודה</u>

5.1. <u>מסמך מדיניות</u>

נוהל מספר 1 לנוהלי המסגרת בנושא "קביעת מדיניות אבטחת 'מידע רגיש' ומערכי מידע בממשלה ומוסדותיה" קובע כי יש להכין מסמך "מדיניות אבטחת המידע הרגיש ומערכי המידע" ולהטמיעו בקרב כל העובדים. במסמך מדיניות אבטחת מידע טיפוסי נהוג להעלות, בין היתר, את הנושאים הבאים:

- **אבטחת מידע בניהול משאבי אנוש**
- **אבטחה פיזית וסביבתית**
- **ניהול תקשורת ותפעול**
- **קיום בקרות גישה לוגיות**
- **ניהול סיסמאות**
- **קיום בקרות ומנגנוני הצפנה**
- **פיתוח ותחזוקה של מערכות**
- **המשכיות עסקית**

5.2. בניגוד לנוהל המסגרת, לא קיים במחלקה מסמך מדיניות אשר מפרט כיצד על המחלקה ועל המשתמשים במועצה להתנהל בתחום המחשוב בכלל ובתחום אבטחת המידע בפרט.

5.3. בהתאם לסעיף 3(2) לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז – 2017
" הממונה על אבטחה יכין נוהל אבטחת מידע ויביאו לאישור בעל המאגר".

5.4. בביקורת הנוכחית נמצא כי הממונה על אבטחת מידע הכין נוהל אבטחת מידע. על הנוהל לכלול בין היתר את הפרטים הבאים:

5.4.1. **הוראות בעניין האבטחה הפיזית והסביבתית של אתרי המאגר כאמור בתקנה 6;**

5.4.2. **הרשאות גישה למאגר המידע ולמערכות המאגר בהתאם לתקנה 8;**

5.4.3. **תיאור של אמצעים שמטרתם הגנה על מערכות המאגר ואופן הפעלתם לצורך כך;**

5.4.4. **הוראות למורשה הגישה למאגר המידע ולמערכות המאגר לצורך הגנה על המידע במאגר;**

5.4.5. **הסיכונים שחשוף להם המידע שבמאגר במסגרת הפעילות השוטפת של בעל מאגר המידע, לרבות אלה הנובעים ממבנה מערכות המאגר כמפורט בתקנה 5א, אופן קביעת סיכונים אלה,**

ואופן הטיפול בהם, לרבות על ידי מנגנוני הצפנה מקובלים להגנה על המידע השמור במאגר או במערכות המאגר;

5.4.6. **אופן התמודדות עם אירועי אבטחת מידע כאמור בתקנה 11 , לפי חומרת האירוע ומידת רגישות המידע;**

5.4.7. **הוראות לעניין ניהול של התקנים ניידים ושימוש בהם כאמור בתקנה 12 .**

5.4.8. **אופן קביעת הסיכונים אלה, ואופן הטיפול בהם, לרבות על ידי מנגנוני הצפנה מקובלים להגנה על המידע השמור במאגר או במערכות המאגר, אופן ההתמודדות עם אירועי אבטחת מידע לפי חומרת האירוע ומידת רגישות המידע והוראות לעניין ניהול של התקנים ניידים ושימוש בהם.**

5.5. **בהתאם לסעיף 3(3) לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז – 2017**

"הממונה יכין תכנית לבקרה שוטפת על העמידה בדרישות תקנות אלה, יבצע אותה ויודיע לבעל מאגר המידע ולמנהל המאגר על ממצאיו"

בביקורת נמצא כי הממונה על אבטחת מידע לא הכין תכנית לבקרה שוטפת.

5.6. **בהתאם לסעיף 5(א) לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז – 2017 על מנהל מאגר המידע לבצע מיפוי מערכות המאגר וביצוע סקר סיכונים. הסעיף קובע כי:**

"בעל מאגר מידע יחזיק מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי

מעודכנת של מערכות המאגר, ובכלל זה:

(1) תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע;

(2) מערכות התוכנה המשמשות להפעלת מאגר המידע, לניהול המאגר ולתחזוקתו, לתמיכה בפעילותו, לניטור שלו ולאבטחתו;

(3) תוכנות וממשקים המשמשים לתקשורת אל מערכות המאגר ומהן;

(4) תרשים הרשת שפועל בה המאגר, הכולל תיאור הקשרים בין רכיבי המערכת השונים ומיקומם הפיזי של רכיבים אלה;

(5) תאריך העדכון האחרון של המסמך ושל רשימת המצאי."

בביקורת הנוכחית העדכנית לינואר 2022 נמצא כי בוצעו מיפוי וסקר סיכונים.

4.8 נהלים פנימיים: הביקורת כן מציינת כי דווח שכל עובד בכיר חדש במועצה חותם על הסכם סודיות, לא צוין אם בוצע החתמה של כלל העובדים הבכירים המכהנים בתפקידם קודם להחלטה זאת וחתומים על הסכם סודיות. מאגר מידע של פרטים אישים של עובדי המועצה המגויסים נשמר במאגר פנימי על שרתי המועצה עם גישה מוגבלת למחלקת משאבי אנוש ומנהל מערכות מידע.

4.9 הממונה על אבטחת מידע לא הכין תכנית מלאה לבקרה שוטפת ולכן לא הוצגה תכנית בקרה בביקורת זו. אך נמצא כי בוצע מיפוי וסקר סיכונים בידי המטה הלאומי ללוחמה בסייבר וכן הממונה על אבטחת המידע ביצע סקר סיכונים בשנה האחרונה אך טרם הועברו הממצאים בכתב.

6. <u>פרק 6 – טיפול באירועי אבטחת מידע</u>

6.1. "אירוע אבטחת מידע" – הוא כל מקרה בו קיים חשד לפגיעה בסודיות, אמינות או זמינות במערכות המועצה, מידע המועצה או כל אמצעי אחר אשר שייך למועצה.

6.2. לטיפול באירועי אבטחת מידע חשיבות רבה, במספר מישורים: מניעה, תגובה בזמן אמת, ותחקור אירועים לצורך הפקת לקחים.

6.3. אירועי אבטחת מידע יכולים לכלול תקיפה מכוונת על מערכות המועצה הן על ידי גורמים חיצוניים והן על ידי גורמים פנימיים וכן נזקים הנגרמים מרשלנות או טעויות.

6.4. נוהל מס' 8 קובע כי "כל מקרה של אירוע אבטחתי חריג - ייחקר – מטרת התחקיר הסקת מסקנות כדי למנוע אירוע כזה בעתיד".

6.5. נמצא לאחרונה כי קיים נוהל פנימי במועצה שמנחה מהו הטיפול הנדרש באירועי אבטחת מידע.

6.6. לא קיים תיעוד כלשהו באשר לאירועי אבטחת מידע שהתרחשו (אם התרחשו) במהלך השנים במועצה , אך נמסר לביקורת כי עד כה טרם התבצעה מתקפת סייבר נגד מערכות המידע של המועצה.

6.7. לא קיימים במועצה כלי ניטור על פעילות המשתמשים. לדוגמא, משתמשים אשר מתחברים שלא בשעות העבודה, משתמשים שטועים בסיסמא שלהם ולפיכך מתנתקים, משתמשים שמנקודת התקשורת שלהם מתחבר מחשב שאינו מחשב של המועצה וכיו"ב.
השימוש במערכות מידע הינו מחויב המציאות כיום, ולא ניתן לעלות על הדעת כיצד ניתן לתפעל ארגון כמו המועצה האזורית בלעדיהן. התפתחות המערך הטכנולוגי התומך בפעילות הארגונית ו/או העסקית, הכולל בתוכו את מערכות המידע, יוצר הזדמנויות עסקיות חדשות ומאפשר התייעלות בפעילות המועצה הכוללת.
במסגרת פעילותה השוטפת של המועצה האזורית נעשה שימוש רב במאגרי מידע הכוללים נתונים אישיים רבים על התושבים. בשנים אחרונות המועצה השקיעה משאבים רבים בפיתוח שירותים דיגיטליים הנגישים לתושבים באינטרנט ומיכון תהליכי עבודה פנימיים. שימוש במערכות מידע והגברת השימוש במאגרי מידע, מגביר את הסכנה כי מידע אישי ייחשף ברבים ויפגע בפרטיות התושבים.
כמו כן, שימוש זה חושף את המועצה האזורית לסיכוני סייבר אשר עלולים לפגוע בפעילותה מרחב הסייבר הינו המתחם הפיזי והלא פיזי, שנוצר או מורכב מחלק או מכל הגורמים הבאים: מערכות ממוכנות ממוחשבות, רשתות מחשבים ותקשורת, תוכנות, מידע ממוחשב, תוכן שמועבר באופן ממוחשב, נתוני תעבורה ובקרה והמשתמשים של

כל אלה. הסיכונים יכולים להיווצר החל מפגיעות אשר יש בהן כדי לשבש את הפעילות השוטפת, למנוע מהמועצה האזורית אספקת שירות לתושבים, לחשוף את המועצה האזורית לתביעות משפטיות ועיצומים רגולטוריים, או אף לסכן חיי אדם.

3 .אירוע אבטחת מידע הוא אירוע המעורר חשש לפגיעה מכוונת במרחב סייבר לוגי או מרחב פיזי בשלמות הנתונים במאגר המידע, פגיעה בזמינות הנתונים, המערכת, חומרה, ממשק או אירוע שבמסגרתו נעשה שימוש בנתוני מאגר המידע, במערכת, בחומרה, בממשק ללא הרשאה.

מתקפות הסייבר הופכות להיות יותר ויותר מתוחכמות וממוקדות מאשר בעבר.

בשנים האחרונות גדל היקף התקיפות באמצעות נוזקות)malware(או כופרות ransomware שונות, והפרות החוק ו"פשיעת המידע" הולכות ומתרבות. נוזקות הינן תוכנות שמטרתן לחדור למחשב או להזיק לו ללא ידיעתו של המשתמש בו. הגדרה זו חלה על וירוסים, תולעי מחשבים, תוכנות ריגול, סוסים טרויאניים ותוכנות פרסום. כופרות הינן נוזקות שמגבילות את הגישה לנתונים השמורים במערכת המחשב ומשמשת לסחוט מהמשתמש תשלום , דמי כופר, על מנת שתוסר מגבלת הגישה למערכת. חלק מהכופרות מבצעות הצפנה לקבצים על הכונן הקשיח, ובכך מקשות את תהליך הסרת ההצפנה בלי לשלם כופר עבור מפתח ההצפנה, ואילו תוכנות כופר אחרות נועלות את המערכת ומציגות הודעת שווא לפיה לא מתאפשרת גישה לקבצים על מנת לחייב את המשתמש לשלם את הכופר במרמה. תוכנת הכופר חודרת לרוב כסוס טרויאני המוסווה כקובץ תמים שמופיע בדרך כלל כקובץ המצורף להודעת דואר אלקטרוני או כתוכנה חופשית להורדה. בעת הפעלתו מקבל הוויורוס שולח אותה הלאה לחברים נוספים כך שבאופן מסווה התוכנה מתקינה את עצמה במחשב ועלולה לגרום נזק רב. בקרות ומנגנוני אבטחת מידע מטפלים במניעה, גילוי, תיעוד התרעה וחשיפה של אירועי אבטחת מידע. אבטחת המידע, מטפלת נושאי זמינות Availability , אמינות Integrity וחשאיות conidentiality המידע.

7. <u>פרק 7 – ניהול מאגרי המידע</u>

7.1. בסעיף 8 לחוק הגנת הפרטיות , תשמ"א – 1981 נקבע כי:

8 (א) לא ינהל אדם ולא יחזיק מאגר מידע החייב ברישום לפי סעיף זה, אלא אם כן התקיים אחד מאלה:

(1) המאגר נרשם בפנקס;

(2) הוגשה בקשה לרישום המאגר והתקיימו הוראות סעיף 10(ב);

(3) המאגר חייב ברישום לפי סעיף קטן (ה) והוראת הרשם כללה הרשאה לניהול והחזקה של המאגר עד רישומו.

7.2. הביקורת מציינת כי מטרת רישום המאגר היא להבטיח את ההגנה על הפרטיות במאגרי מידע, ולתת כלים, הן בידי רשם מאגרי המידע, והן בידי הציבור שמידע עליו מנוהל במאגרי המידע, לאכוף את הזכויות והחובות המוטלות בחוק הגנת הפרטיות על בעלי מאגרים.

7.3. מבדיקת הביקורת עולה כי כל מאגרי המידע הקיימים במועצה מנוהלים על ידי דובר המועצה וללא שנרשמו בפנקס אצל רשם מאגרי המידע, במשרד המשפטים.

8. <u>הגשת בקשה לרישום מאגר מידע לרשם</u>

8.1. בהתאם לסעיף 9 (א) – 9(ב) לחוק הגנת הפרטיות , תשמ"א – 1981 נקבע כי:

בקשה לרישום מאגר מידע תוגש לרשם.

(ב) בקשה לרישום מאגר מידע תפרט את –

(1) זהות בעל מאגר המידע, המחזיק במאגר ומנהל המאגר, ומעניהם בישראל;

(2) מטרות הקמת מאגר המידע והמטרות שלהן נועד המידע;

(3) סוגי המידע שייכללו במאגר;

(4) פרטים בדבר העברת מידע מחוץ לגבולות המדינה;

(5) פרטים בדבר קבלת מידע, דרך קבע, מגוף ציבורי כהגדרתו בסעיף 23, שם הגוף הציבורי מוסר המידע ומהות המידע הנמסר, למעט פרטים הנמסרים בהסכמת מי שהמידע על אודותיו.

8.2. כאמור בסעיף 7 לדוח ביקורת זה, המועצה לא רשמה את מאגרי המידע ברשם מאגרי המידע ולפיכך , גם לא הגישה בקשה לרישום המאגרים, לא הוקצו תקציבים למאגרי מידע כל זאת בהתאם להוראות סעיף 9 לחוק הגנת הפרטיות.

9. <u>פרק 9 בעלי הרשאה</u>

9.1. בהתאם לסעיף 1 לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017

"בעל הרשאה" - יחיד אשר יש לו גישה לאחד מאלה על פי הרשאתו של בעל המאגר או המחזיק:

(1) מידע מהמאגר;

(2) מערכות המאגר;

(3) מידע או רכיב הנדרש לצורך הפעלת המאגר או לצורך גישה אליו.

על אף האמור, מחזיק שאינו יחיד או יחיד שקיבל גישה על פי הרשאה של מחזיק, לא ייחשב כבעל הרשאה של בעל המאגר;

9.2. מועצה אזורית גלבוע מאפשרת למספר חברות העובדות עם המועצה ומאפשרת להם גישה למאגרי מידע הקיימות במועצה לצורך עבודתן.

9.3. נתקבל מידע על 9 שמות של חברות החיצוניות שעובדות עם המועצה וקיבלו הרשאות להחזיק במידע כמו כן התקבלה רשימת מאגרי מידע פנימיים. למעט שני חברות GIS ו-E.P.R לא ניתן היה לבדוק באם ההסכמים עם חברות אלו כוללות הסכם סודיות.
הביקורת מצא שמול שני החברות המוזכרות קודם קיימים חוזים הכוללים הסכמי סודיות

9.4. בהתאם לסעיף 2 (א) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017

(א) בעל מאגר מידע יגדיר במסמך הגדרות מאגר (להלן - מסמך הגדרות המאגר), את כל העניינים האלה לפחות:

(1) תיאור כללי של פעולות האיסוף והשימוש במידע;

(2) תיאור מטרות השימוש במידע;

(3) סוגי המידע השונים הכלולים במאגר המידע, בשים לב לרשימת סוגי המידע שבפרט 1(3) בתוספת הראשונה;

(4) פרטים על העברת מאגר המידע, או חלק מהותי ממנו אל מחוץ לגבולות המדינה או שימוש במידע מחוץ לגבולות המדינה, מטרת ההעברה, ארץ היעד, אופן ההעברה וזהות הנעבר;

(5) פעולות עיבוד מידע באמצעות מחזיק;

(6) הסיכונים העיקריים של פגיעה באבטחת המידע, ואופן ההתמודדות עמם;

(7) שמו של מנהל מאגר המידע, של מחזיק המאגר ושל הממונה על אבטחת מידע בו, אם מונה כזה.

9.5. נמצא כי המועצה לא הגדירה לבעלי ההרשאה מסמך הגדרות ובכך הגדילה את הסיכוי לפגיעה במאגרי המידע המוניציפליים .

10. <u>פרק 10 - מיקור חוץ</u>

10.1. בהתאם לסעיף 15 (א) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017:

"בעל מאגר המתקשר עם גורם חיצוני לצורך קבלת שירות, הכרוך במתן גישה למאגר המידע –

(1) יבחן, לפני ביצוע ההתקשרות עם הגורם החיצוני המסוים כאמור, את סיכוני אבטחת המידע הכרוכים בהתקשרות;

(2) יקבע במפורש בהסכם עם הגורם החיצוני (בתקנה זו – ההסכם) את כל אלה, בשים לב לסיכונים לפי פסקה (1):

(א) המידע שהגורם החיצוני רשאי לעבד ומטרות השימוש המותרות בו לצורכי התקשרות;

(ב) מערכות המאגר שהגורם החיצוני רשאי לגשת אליהן;

(ג) סוג העיבוד או הפעולה שהגורם החיצוני רשאי לעשות;

(ד) משך ההתקשרות, אופן השבת המידע לידי הבעלים בסיום ההתקשרות, השמדתו מרשותו של הגורם החיצוני ודיווח על כך לבעל מאגר המידע;

(ה) אופן יישום החובות בתחום אבטחת המידע שהמחזיק חייב בהן לפי תקנות אלה, וכן הנחיות נוספות לעניין אמצעי אבטחת מידע שקבע בעל מאגר המידע, אם קבע;

(ו) חובתו של הגורם החיצוני להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק לפי האמור בהסכם, וליישם את אמצעי האבטחה הקבועים בהסכם כאמור בפסקת משנה (ה);

(ז) התיר בעל מאגר מידע לגורם החיצוני לתת את השירות באמצעות גורם נוסף - חובתו של הגורם החיצוני לכלול בהסכם עם הגורם הנוסף את כל הנושאים המפורטים בתקנה זו;

(ח) חובתו של הגורם החיצוני לדווח, אחת לשנה לפחות, לבעל מאגר המידע על אודות אופן ביצוע חובותיו לפי תקנות אלה וההסכם ולהודיע לבעל המאגר במקרה של אירוע אבטחה;

(3) יפרט בנוהל האבטחה של המאגר גם את העניינים המנויים בפסקה (2(א)) עד (ה), וכן יפנה בו במפורש להסכם עם הגורם החיצוני ולנוהל האבטחה שלו;

(4) ינקוט אמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות תקנות אלה, בהיקף הנדרש בשים לב לסיכונים האמורים בפסקה (1)."

10.2. מבדיקת הביקורת עולה כי המועצה התקשרה עם מספר גורמים חיצוניים לצורך קבלת שרות ובהתאם לטבלה האמורה.

לביקורת הוצגו חלק מהחוזים ושמות החברות העובדות במיקור חוץ עם המועצה והמחוברות למערכות המחשוב של המועצה ולכן לא ניתן היה לבדוק באם בוצעה בטרם ההתקשרות סיכוני אבטחת המידע.

#	מחלקה	שם המאגר	האם בוצעה בטרם ההתקשרות בדיקת סיכוני אבטחת במידע
1	כלבייה ויחידה סביבתית	לולה-טרק, ורפיי	לא
2	שירותים חברתיים	EPR	כן
3	משא"ב	זמן אמת וסינריון	לא
4	ועדה מקומית	קומפלוט	לא
5	גזברות	אוטומציה	לא
6	רישוי עסקים	תוכנת רישוי עסקים	לא
7	קולחי הגלבוע	פריוריטי	לא
8	חכ"ל	חשבשבת	לא
9	מרכזים קהילתיים	דיאלוג-תוכנת רישום חוגים של החברה למתנס"ים	לא

11. <u>פרק 11 ההיבט האזרחי, הפלילי והעונשי</u>

11.1. במהלך הביקורת נשאלה הביקורת, מה קורה אם לא רושמים מאגר מידע שחלה עליו חובת רישום?

11.2. אין לנהל או להחזיק מאגר מידע מאגר מידע החייב ברישום מבלי שנרשם. ניהול, החזקה או שימוש במאגר מידע שחייב ברישום ולא נרשם מהווה עבירה פלילית שדינה מאסר שנה, לפי סעיף 31א(א)(1) לחוק הגנת הפרטיות.

11.3. בנוסף, ניהול, החזקה או שימוש במאגר מידע שחייב ברישום ולא נרשם מהווה עבירה בגינה רשאי רשם מאגרי מידע להטיל קנס מנהלי (ר' לעניין זה את תקנות העבירות המנהליות (קנס מנהלי - הגנת הפרטיות), התשס"ד-2004).

11.4. פגיעה בפרטיות של אדם היא עוולה כמו כל עוולה אחרת עפ"י דיני הנזיקין. כלומר, אדם שחושב שנגרם לו נזק עקב אי הקפדה על השימוש הנאות במידה אודותיו, רשאי לתבוע את המזיק את נזקיו בתביעה אזרחית לפיצויים אזרחיים.

12. <u>פרק 12 – שקיפות</u>

12.1. כפי שפורט בדוח הביקורת האמור לעיל, נמסרו 9 שמות של מאגרי המידע להכנת דו"ח ביקורת זה, אולם בהתאם בדו"ח לתושב ובאתר האינטרנט של המועצה לא פורטו שמות מאגרי המידע.

12.2. הביקורת מעירה כי על המועצה לפרסם באתר האינטרנט את שמות מאגרי המידע הקיימים ברשות.

13. <u>מעקב אחר דו"ח ביקורת מבקר המועצה בנושא אבטחת מידע שבוצע בשנת 2014, והתייחסות המבוקר לדו"ח זה.</u>

13.1. מדיניות אבטחת מידע

מס"ד	נושא ביקורת 2014	האם בוצע תיקון ליקויים כן / לא בשנים 2018 - 2022 ? – הערות
1	האם קיימת אסדרה בתחום ? ניהול סיכונים, קווי מדיניות, הנחיות, נהלים, כללי גישה, הרשאות וסיווג מידע.	חלקי, לא הושלם התהליך מול בזק. סקר סיכונים בוצע ע"י אגף הסייבר , במשרד הפנים. ממונה אבטחת המידע טרם הגיש תוצאות המבדק הפנימי בכתב. טרם בוצע מבדק חדירה חיצוני במועצה.
2	האם בוצע מינוי למנהל אבטחת מידע במועצה ?	בהסמכת מזכיר המועצה בע"פ , הייתה מנהלת ישירה. בוצע בהמשך ע"י מנכ"לית המועצה.
3	האם קיים תקציב למנהל אבטחת מידע ?	המועצה קיבלה לשימושה תוכנת הגנה בפני מתקפות סייבר כפיילוט שעודכן עד לסוף שנת 2022.
4	האם בוצעה ביקורת פנימית לבדיקת פרצות באבטחת מידע ?	חלקית ע"י בזק, מבחינת חיבור בין הסניפים של המועצה וכן הפרדת חיבורי WIFI מרשת המועצה. בוצע רק מבדק חדירה פנימי ע"י הממונה לאבטחת מידע שתוצאותיו לא נמסרו עדיין בדוח כתוב. לא בוצע עדיין מבדק חדירה חיצוני.
5	האם בוצעה ביקורת חיצונית לבדיקת פרצות באבטחת מידע ?	לא
6	באילו אמצעים השתמשת בכדי לבדוק חשיפה של מאגרי מידע פנימיים ?	לא בוצע על ידי המנמ"ר
7	בקרות כניסה פיזיות לחדרים קריטיים, האם הוספו כנדרש ?	הועברו שרתים למקלט ומצלמות אבטחה, קיים חדר נשק בסמיכות למשרדי מח' מחשוב. המקום מאובטח באמצעות מצלמות אבטחה ודלת פלדלת. מומלץ להתקין מערכת אזעקה.

8	בקרות כניסה לוגיות למחשבים המוגדרים כקריטיים , האם הוספו כנדרש ?	עדיין לא. במסגרת תוכנת ההגנה למתקפות סייבר, יש רישום חלקי לפעולות ברשת (לוגים).
9	ISO 17799 לא יושם במלואו. האם ייושם עד כה ?	התקן הינו מיושן ולא תואם במלואו את הרגולציה שנעשתה ב-2018. הסתיים התהליך מול בזק והותאמו הסעיפים המעודכנים.
10	פרוטוקול חירום, האם קיים ?	קיים
11	- בוצע אחסון פרוטוקול חרום בתחום מערכות מידע בכספת שמורה ? - בוצע מינוי בנוהל מחליף בנבצרות של מנהל מערכות מידע ?	עדיין לא. מינוי מחליף בע"פ, לא בכתב.
12	בוצעה בדיקת אבטחת מידע לשעון נוכחות של העובדים ?	בוצעה בדיקה מול חברת השעונים. המידע שנשמר בשעון מוגבל מאוד ומחייב גישה לתוכנת איסוף השעות.
13	האם מנהל מערכות המידע , משולב בדיונים של המועצה , בהן נדרשת חוות דעתו המקצועית.	כן. למיטב ידיעתי יש מודעות גבוהה בארגון לחשיבות הנושא , עקב העלייה בסיכונים הנשקפים לארגון.

המלצות

1. על מנת להבטיח את סודיות המידע החסוי ביותר של תושבי המועצה ולקוחותיה , המטופל ונאגר במערכות המידע ומתקני המועצה, יש לרשום בהקדם את כל מאגרי המידע הידועים, של מ.א הגלבוע , במשרד המשפטים.

2. נדרש זיהוי מאגרים קיימים וחדשים , ולכן יש לאתר כנוהל שבשגרה (כרגע ידועים 9 מאגרי מידע) , ושינוי ההתייחסות אליהם באמצעות הגדרתם , כמאגר מידע רשמי , הנדרש להיות כפוף תחת תקנות הגנת הפרטיות. לפיכך יש לערוך בקרה באמצעות ממונה אבטחת המידע והאחראי על המאגרים , לבדיקת השינויים במאגרי המידע (תוספת , גריעה).

3. יש לעמוד ברגולציות ונושאי אבטחת מידע מחייבים.

4. יש להמשיך ולהעלות את המודעות לאבטחת מידע , בקרב מנהלי ועובדי המועצה , כמו גם המשך העלאת הכשירות המקצועית של העוסקים בתחום אבטחת המידע במועצה.

5. יש לשפר את החוסן של מערכות המידע של המועצה , בפני פגיעה בהיבט סודיות , אמינות וזמינות, כתוצאה מפעילות זדונית ע"י גורם חיצוני או פנימי.

6. על ממונה אבטחת המידע , להעביר דוח כתוב בהקדם על מנת לדווח , את תוצאות המבדק הפנימי שערך , לתוכנת הגנת מתקפות הסייבר אשר פועלת במועצה , כאמור בפיילוט עד סוף שנת 2022.

7. בנוסף יש לערוך בהקדם לתוכנה מבדק חדירה חיצוני, המחייב את השלמת המסקנות , לבחינת עמידות מערכות המידע במועצה ובגופי הסמך.

8. בהתאם לתוצאות מבדקי החדירה (הפנימי והחיצוני) יש לבחור מבין החלופות הבאות : חלופה 1 - על רכישת והתקנת מערכת ה EDR הארגוני והפתרונות הנוספים שהומלצו על ידי הממונה על אבטחת המידע , או להשאיר בחלופה 2 - את התוכנה הקיימת ולרכוש את הפתרונות הנוספים שהומלצו על ידי ממונה אבטחת המידע במועצה.

9. ההחלטה על בחירה בין שתי החלופות שצוינו בהמלצה מספר 8 תלויה כאמור במבדקי החדירה שצוינו בהמלצות 7-6. על ממונה אבטחת המידע להודיע על מסקנותיו המקצועיות כאמור. יצוין כי קיים הבדל תקציבי של כ-200,000 ₪ +מע"מ בין שתי החלופות (חלופה 1 יקרה בכ-200000 ₪ חלופה 2).

במידה ויוחלט שמערכת התוכנה הקיימת , איננה מספקת הגנה מתאימה לאיומי הסייבר הנשקפים למועצה , יש לדאוג לשריון תקציבי מבעוד מועד לרכישת מערכת ה- EDR הארגונית (חלופה 1).