מועצה אזורית הגלבוע

דוח הביקורת לשנת 2019

1.ניהול מאגרי מידע

במועצה אזורית גלבוע

לשנים 2017-2019

2.אבטחת מערכות המידע

3.מעקב אחר תיקון הליקויים לדוח הביקורת לשנת 2014 – אבטחת מערכות מידע

1. נתונים כללים על מועצה אזורית גלבוע ליום 17/05/2020

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- 30000 תושבים*
- *קצב גידול שנתי של האוכלוסייה 1.8% (עפ"י הלמ"ס נכון לסוף 2017)*
- הדרוג הסוציואקונומי (חברתי כלכלי) 5.

ביקורת בנושא ניהול מאגרי מידע ואבטחת מערכות מידע

תקציר מנהלים

להלן עיקרי ממצאים, מסקנות והמלצות מדו"ח ביקורת שנערך במועצה אזורית הגלבוע בנושא: ניהול מאגרי מידע ואבטחת מידע.

- **לשם קבלות החלטות רצוי לעיין בדו"ח המלא**

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. 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".**

1.3. **במועצה אזורית גלבוע ישנם 10 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 והנגשתו רק למורשים וגיבוי המידע לצרכים המשפטיים ואחרים העתידיים של המועצה .**

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

1.6. **זיהוי מאגרים קיימים חדשים ושינוי התייחסות אליהם באמצעות הגדרתם כמאגר מידע רשמי הנדרש להיות כפוף תחת תקנות הגנת הפרטיות.**

2. - מנהל אבטחת מידע

נמצא כי המועצה מינתה עובד ייעודי העוסק בתחום אבטחת המידע, אולם הממונה על מאגרי המידע לא מונה כמפקח אחראי על תחום מאגרי המידע.

3. מבנה ארגוני וכתב מינוי

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. הליך בחירתו בוצע באופן תקין באמצעות מכרז , אולם לא התקבל כתב מינוי המתאר את כל תחומי האחריות וסמכויות התפקיד.

4. ועדת היגוי

במועצה מתקיימת וועדת היגוי לאבטחת מידע בראשות מנכ"לית, וחברים בה גם המנמ"ר, דובר המועצה והיועץ המשפטי של המועצה.
לא נמצאו פרוטוקולים של הוועדה באתר המועצה ובנוסף לא נכתב נוהל לפעילות וועדת ההיגוי לאבטחת מידע.

5. מדיניות אבטחת מידע ותכנית עבודה

5.1. בניגוד לנוהל המסגרת, לא קיים במחלקה מסמך מדיניות ונוהל אשר מפרט כיצד על המחלקה ועל המשתמשים במועצה 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,

5.2. הממונה על אבטחת מידע לא הכין תכנית לבקרה שוטפת וכן לא בוצע מיפוי וסקר סיכונים.

6. טיפול באירועי אבטחת מידע

6.1. לא קיים נוהל פנימי במחלקת מחשוב במועצה אשר מנחה מהו הטיפול הנדרש באירועי אבטחת מידע.

6.2. לא קיים תיעוד כלשהו באשר לאירועי אבטחת מידע שהתרחשו (אם התרחשו) במהלך השנים במועצה.

6.3. לא קיימים במחלקת מחשוב של המועצה 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.

7. ניהול מאגרי המידע

מבדיקת הביקורת עולה כי כל מאגרי המידע הקיימים במועצה והמנוהלים במועצה, לא נרשמו בפנקס אצל רשם מאגרי המידע, במשרד המשפטים.

8. הגשת בקשה לרישום מאגר מידע לרשם

המועצה לא רשמה את מאגרי המידע ברשם מאגרי המידע ולפיכך , גם לא הגישה בקשה לרישום המאגרים בהתאם להוראות סעיף 9 לחוק הגנת הפרטיות.

9. בעל הרשאה

9.1. לא התקבל מידע האם 9 החברות החיצוניות שעובדות עם המועצה ושקיבלו הרשאה להחזיק במידע , חתמו על הסכם סודיות.

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

10. 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.

11. ההיבט האזרחי, הפלילי ועונשי

11.1. אי רישום של מאגר מידע החייב ברישום מבלי שנרשם,

מהווה עבירה פלילית שדינה מאסר שנה, לפי סעיף 31א(א)(1) לחוק הגנת הפרטיות.

11.2. בנוסף, ניהול, החזקה או שימוש במאגר מידע שחייב ברישום ולא נרשם מהווה עבירה בגינה רשאי רשם מאגרי מידע להטיל קנס מנהלי.

12. 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.

13. 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. יחד עם זאת, הביקורת מוצאת כי יש להמשיך לפעול לתיקון הליקויים בשלמותם ובדגש על הקטנת הסיכונים על פי חומרתם ובדגש על מערכות הכספים והרווחה.

מבקר המדינה פרסם דוח שחובר בשנת 2017 על עיריית 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.**

להלן הדוח המלא

1 רקע כללי

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. 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.

1.2 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 לאספו. מאגרי מידע מסכנים בעצם קיומם את הפרטיות , ועל כן יש צורך בקביעת מנגנונים ייחודיים להגנה על המידע הנאגר בו.

1.3 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 מהעבר, 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 כי , "אמצעי המחשוב המודרניים והטכנולוגיה המתקדמת בתחום התקשורת מביאים עמם ברכה רבה בצד סכנות גוברות לפגיעה בזכותו של האדם לפרטיות".

1.4 בשנת 1981 נחקק חוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות), במטרה "לשריין את ההגנה של האדם לזכותו לפרטיות" .

1.5 בשל הפגיעה הפוטנציאלית הגלומה במאגרי מידע יוחד בחוק פרק לנושא זה, ונקבעה בו חובה לרשום מאגרי מידע , זאת כאמור 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.

1.6 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 .

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

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

2.2 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.

2.3 הביקורת מעירה כי למרות קיום מאגרי המידע האמורים, המועצה לא רשמה את מאגרי המידע במשרד המשפטים וכפי שיורחב בהמשך הדו"ח.

3. חוקים, הוראות ונהלים

3.1 צו המועצות המקומיות (מועצות אזוריות), תשי״ח-1958

3.2 חוק יסוד כבוד האדם וחירותו על פיו ״כל אדם זכאי לפרטיות ולצנעת חיו״.

3.3 חוק הגנת הפרטיות, תשמ״א- 1981 (להלן: ״חוק הגנת הפרטיות״)

3.4 תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבורים), תשמ״ו- 1986

3.5 חוק המחשבים, התשנ״ה- 1995.

3.6 חוק העונשין, תשל״ז-1977 הקובע את העונשים החלים על עובדי ציבור שמוסרים מידע שלא כחוק.

3.7 חוק להסדרת ביטחון בגופים ציבוריים, התשנ״ח- 1889, הקובע את דרכי הפעולה והניהול של הביטחון ובכלל זה אבטחת מידע ממוחשב ומידע פיזי רשומות בגופים ציבוריים.

3.8 תקנות הגנת הפרטיות (אבטחת מידע), התשע״ז – 2017.

3.9 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

4.1 איתור חריגות מחוקים, הוראות ונוהלי עבודה.

4.2 איתור חריגות מסמכויות.

4.3 איתור סיכונים עסקיים ותפעוליים.

4.4 איתור ליקויים מערכתיים (כגון: חסר או ליקוי בנהלים, ליקויי תוכנה).

4.5 איתור מקרים בהם קיים חשד לפגיעה בטוהר מידות מצד עובדי המועצה.

4.6 איתור מקרים בהם קיימת פגיעה בחיסכון, בשמירה על הרכוש וביעילות העבודה.

4.7 הביקורת בחנה את ההיבטים השונים הקשורים לנושא ניהול מאגרי מידע.

4.8 כמו כן, הביקורת בדקה האם פעילות המועצה בתחום מאגרי מידע מתבצעת תוך שמירה על חוקיות, סדירות, עקרון השוויון, חסכון, יעילות שקיפות ומניעת פגיעה בטוהר המידות.

5. היקף הביקורת ואופן הבדיקה

5.1 במהלך החודשים ינואר ועד יוני 2020 בוצעה ביקורת במועצה אזורית גלבוע.

5.2 הביקורת בוצעה בהתאם לתוכנית העבודה של מבקר המועצה לשנת 2019. הנושא נכלל בתכנית העבודה השנתית, בשל הסיכונים הכרוכים בו ובהתאם לסמכותו בחוק.

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

5.3 הביקורת בחנה את ההתנהלות המועצה ביחס לניהול מאגרי מידע במועצה האזורית גלבוע בין השנים 2017-2019 וכללה את ההיבטים הבאים: רישום מאגרי מידע, שקיפות המידע, הסכמים סודיות עם חברות הפועלות על מאגרי המידע ועוד.

5.4 לצורך ביצוע הביקורת נעזרה בין השאר בדוחות ביקורת שחוברו בארגונים נוספים וביניהם:

5.4.1 דוחות ביקורת בתחום "אבטחת מידע" שחוברו על ידי מבקרי רשויות .

5.4.2 דוח מבקר המדינה מספר 64ג', משנת 2014 בנושא רישום מאגרי מידע בישראל.

5.4.3 מבקר המועצה נפגש עם מומחים בתחום אבטחת מערכות המידע ומאגרי המידע וכן השתתף בשנים האחרונות באירועי שבוע הסייבר , באוניברסיטת תל אביב , אירוע הנערך אחת לשנה על ידי רשות הסייבר שבמשרד ראש הממשלה.

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 2- מנהל אבטחת מידע.

2.1. בסעיף 17 ב. (א) לחוק הגנת הפרטיות , תשמ"א – 1981 נקבע כי:

"הגופים המפורטים להלן חייבים במינוי אדם בעל הכשרה מתאימה שיהיה ממונה על אבטחת מידע (להלן - הממונה):"

2.2. הוראה זו חלה גם על רשויות מקומיות, שכן הן נכללות בהגדרה של רשויות ציבוריות, על פי הגדרות החוק.

משרד הפנים קבע הגדרת תפקיד לתפקיד מנהל אבטחת מידע (Chief Security Office),

במסגרתה נקבעו תחומי האחריות של הממונה, כפיפותו למנהל מערכות מידע ראשי

(מנמ"ר) וכן 4 דרישות סף לקבלה לתפקיד:

- בעל תעודת טכנאי או הנדסאי
- ידיעת השפות עברית ואנגלית ברמה גבוהה
- נסיון מקצועי - ברשות מקומית ברמה ב' וג' ניסיון מקצועי של שנה לפחות כמנהל או כסגן -מנהל מערכות מידע, או מנהל אבטחת מידע בחברה בעלת 25 עובדים ומעלה.
- היעדר עבר פלילי - היעדר הרשעה בעבירה שבנסיבות העניין יש עמה קלון.

2.3. **נמצא כי המועצה מינתה עובד ייעודי העוסק בתחום דוברות המועצה , אולם הוא לא מונה כמפקח האחראי על תחום מאגרי המידע. וללא רקע הסמכה, כתב מינוי וניסיון מקצועי בתחום אבטחת מידע.**

3. <u>פרק 3- מבנה ארגוני וכתב מינוי</u>

3.1. האגף לכוח 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.

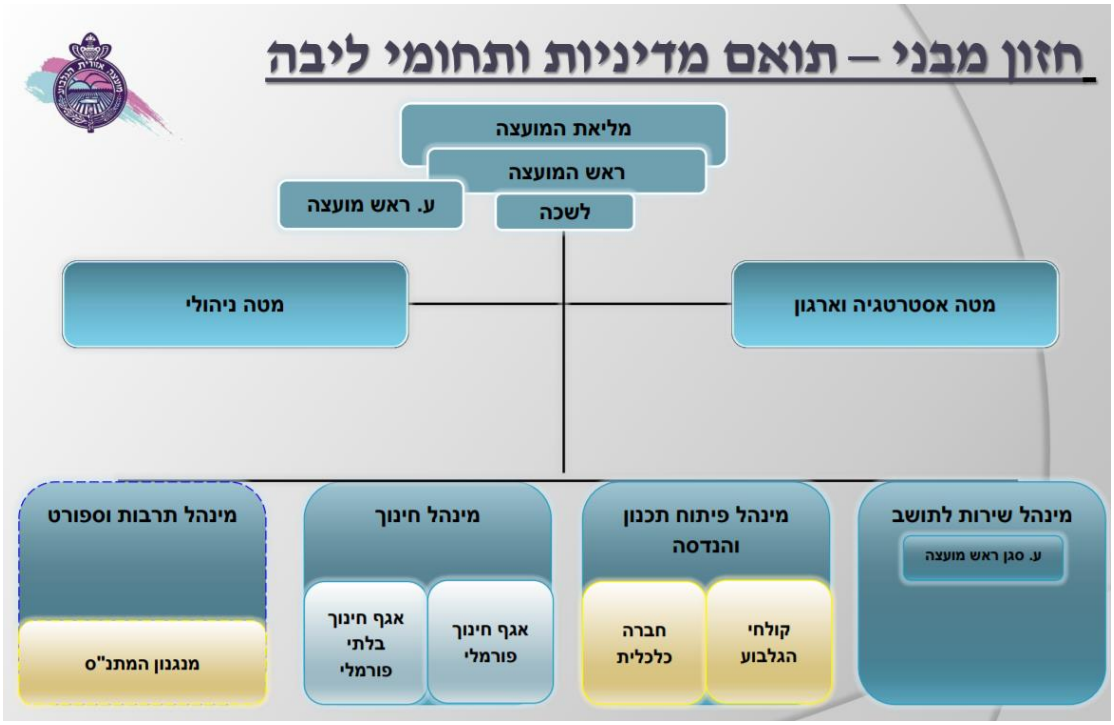
3.2. **נמצא כי בהתאם להנחיות אגף משאבי אנוש במשרד הפנים הקובעות כי המנמ"ר יהיה כפוף מנהלתית למנכ"ל המועצה, המנמ"ר כפוף למנכ"לית המועצה.**

3.3. **תפקיד מנהל הרשת במועצה ניתן לעובד המועצה ללא הליך מכרזי וללא כתב הסמכה וכתב מינוי ובו תיאור התפקיד עליו הוא אחראי.**

3.4. **הביקורת מעירה למועצה כי עליה לבצע מכרז לתפקיד מנהל הרשת וכן לכתוב כתב מינוי ולתאר בפועל על מה אחראי מנהל הרשת במועצה ואלו סמכויות יש לו.**

3.5. **כמו כן, לא נמצא במועצה עובד שהינו ממונה על אבטחת מידע עם כתב הסמכה מהמועצה.**

<u>להלן המבנה הארגוני של המועצה:</u>



4. <u>ועדת היגוי לאבטחת מידע</u>

4.1. 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).

4.2. **כנדרש בנוהל מסגרת מס׳ 5. קיים במועצה נוהל העוסק בפעילות וועדת היגוי לאבטחת מידע בראשות מנכ״לית, ובהשתתפות מנמ״ר, דובר והיועץ המשפטי של המועצה .**

4.3. **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 נמצא כי הממונה על אבטחת מידע לא הכין נוהל אבטחת מידע ולפיכך גם הנוהל לא אושר במועצה. 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 5)א(, 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"

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

5.7. 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."

5.8. **בביקורת נמצא כי לא בוצע מיפוי וסקר סיכונים.**

5.9. **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 בתפקידים , קודם להחלטה זאת , החתומים 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.**

5.10. **הממונה על אבטחת מידע לא הכין תכנית מלאה לבקרה שוטפת, לכן לא הוצגה בביקורת זו כמו כן לא בוצע מיפוי וסקר סיכונים.**

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. **לא 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.**

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.**

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 ולא נרשמו 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 רק 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.

מאגרים פנימיים				
#	**מחלקה**	**שם המאגר**	**שם הנאמן למידע**	**האם בוצעה בטרם ההתקשרות בדיקת סיכוני אבטחת במידע**
1	כלבייה ויחידה סביבתית	לולה-טרק, ורפיי	ד"ר שי רודריג	לא
2	שירותים חברתיים	EPR	סמדר אורג	כן
3	משא"ב	זמן אמת וסינריון	אביגיל קציר	לא
4	ועדה מקומית	קומפלוט	אורלי שטיינר	לא
5	גזברות	אוטומציה	ג'אוד זועבי	לא
6	רישוי עסקים	תוכנת רישוי עסקים	מיקי יוסף	לא
7	קולחי הגלבוע	פריוריטי	מוחמד אלבחירי	לא
8	חכ"ל	חשבשבת	שניר פרידמן	לא
9	מרכזים קהילתיים	דיאלוג- תוכנת רישום חוגים של החברה למתנס"ים	סיון גולדמן	לא

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

11.1. **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 נזיקין. 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 במהלך הכנת 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. מעקב אחר דו"ח ביקורת מבקר המועצה בנושא אבטחת מידע שבוצע בשנת 2014, והתייחסות המבוקר לדו"ח זה :

13.1. מדיניות אבטחת מידע

מס"ד	נושא ביקורת 2014	האם בוצע תיקון ליקויים כן / לא בשנים 2018 -2019 ? – הערות
1	האם קיימת אסדרה בתחום ? ניהול סיכונים, קווי מדיניות, הנחיות, נהלים, כללי גישה, הרשאות וסיווג מידע.	חלקי, לא הושלם התהליך מול בזק
2	האם בוצע מינוי למנהל אבטחת מידע במועצה ?	בהסמכת מזכיר המועצה בע"פ , הייתה מנהלת ישירה
3	האם קיים תקציב למנהל אבטחת מידע ?	קיים תקציב מחשוב אשר לא מאפשר כיסוי להוצאות אבטחת מידע
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
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
7	בקרות כניסה פיזיות לחדרים קריטיים, האם הוספו כנדרש ?	הועברו שרתים למקלט ומצלמות אבטחה, קיים חדר נשק בסמיכות למשרדי מח' מחשוב
8	בקרות כניסה לוגיות למחשבים המוגדרים כקריטיים , האם הוספו כנדרש ?	עדיין לא
9	ISO 17799 לא יושם במלואו. האם יושם עד כה ?	התקן הינו מיושן ולא תואם במלואו את הרגולציה שנעשתה ב-2018. לאחר סיום התהליך מול בזק יותאמו 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 ?	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 מידע משולב בדיונים של המועצה בהם נדרשת חוות דעתו המקצועית בתחום ?	לא בכולם

המלצות

המלצות

1. יש להנחות על מיפויים המידי ורישום כל מאגרי המידע המנוהלים במ.א הגלבוע , בפנקס הרשם במשרד המשפטים , כפי שהחוק מחייב.

2. יש להנחות כתיבת נוהל אבטחת מידע רשותי , הכולל בין השאר תכנית לביצוע בקרות שוטפות.

3. נוהל אבטחת המידע , ראוי שייכתב בהקדם ובמקביל להקמת מחלקת המחשוב במועצה, כפי שנמסר במסגרת ישיבת מליאת המועצה בחודש יוני 2020 , בה הוצג מבנה ארגוני חדש למ.א הגלבוע.

4. יש להנחות על ביצועי סקר סיכונים עד סוף שנת 2020, לאבטחת מידע עלפי דרישות האגף הייעודי במשרד הפנים , המשמש כרגולטור - ולכל אחד ממאגרי המידע הקיימים במועצה וכן ביצוע בקרות שוטפות באותם הסיכונים שאותרו.

5. יש למנות את בעלי התפקידים הבאים בהקדם וכן להנחות על קיום הדרכה באשר לאחריותם על פי תקנות הרגולטור :

א. ממונה אבטחת מידע.

ב. מנהל מאגרי מידע רשותי.

6. מומלץ להפריד בין בעלי התפקידים בסעיף הקודם , כך שלא ישמש אותו אדם בשני התפקידים במקביל במועצה, זאת על מנת שלא ייוצר חשש לניגוד עניינים. משמעות המלצה זו שמנהל תחום המחשוב לא יהיה אחראי בנוסף לתחומי אחריותו , במסגרת המבנה הארגוני החדש של המועצה, גם על מאגרי המידע במועצה.

7. יש לשלב את המנמ"ר, בכל הישיבות הנוגעות לתחום מערכות המידע, אבטחת מ. המידע ומאגרי המידע וכן כגורם מקצועי שייתן את דעתו המקצועית , במכרזים בתחומים אלו.

8. יש להנחות את היועץ המשפטי למועצה והמנמ"ר על כך שיש להביא לידי ביטוי במכרזים הקרובים בתחומים המוזכרים בדוח זה , את הערות הביקורת וכן את הערכת הסיכונים למאגרי

המידע השונים והבאתם ליידי ביטוי , בנספח מיוחד העוסק באבטחת המידע אשר יצורף להסכם ההתקשרות של המועצה , עם החברות הזוכות.

9. יש להנחות על כתיבת נהלי עבודה ברורים על מנת לשמור על סודיות המידע.

10. יש להורות על החתמת כלל בעלי התפקידים במועצה , החשופים למידע , על הצהרת שמירת הסודיות וכן לבצע הדרכות בתחום זה כחלק מתוכנית עבודה שנתית .

נספחים

לכבוד : מר רונן בגים – מנהל מערכות מידע מועצה אזורית גלבוע.

הנדון: שאלון בנושא מאגרי מידע ואבטחת מידע – מועצה אזורית גלבוע

שלום רב.

בהתאם להחלטתו של מבקר המועצה מר אייל פיגנבאום המעוניין לבדוק את נושא מאגרי מידע יופק שאלון איכותי ככלי עזר לביקורת.

בהתאם לפגישתנו שנערכה בתאריך 9.2.2020 בה נכחו מנמ"ר מ.א. גלבוע מר רונן בגים ומבקר המועצה מר אייל פיגנבאום להלן פירוט הנושאים שיבדקו במסגרת הביקורת שבנדון , אותם אנו מבקשים לרכז לצורך כך.

במסגרת הביקורת יבחנו הנושאים הבאים:

ניהול תקין ועמידה בחוקים ובנהלים הקיימים, סמכויות העוסקים: מנמ"ר, מנהל אבטחת מידע, מנהל מאגרי מידע, האם קיימים סיכונים עסקיים ותפעולים. ליקויי מערכתיים. טוהר המידות, חיסכון ויעילות עבודה. ניהול מאגרי מידע. כל זאת במסגרת ביצוע הפעולות תוך שמירה על חוקיות, סדירות, חיסכון, יעילות שקיפות ומניעת פגיעה בטוהר המידות.

מטרת השאלון:

השאלון הינו לשם איסוף מידע בדבר התנהלות אגף מערכות מידע בכפוף להוראות החוק, השאלון גם יתייחס להתנהלות נושא מאגרי מידע ואבטחת מידע במוסדות המועצה.

נבקשך למלא את השאלון הנ"ל ולצרף אסמכתאות במידת האפשר:

1. הבסיס החוקי

1.1 מהו הבסיס החוקי על פיו אתם עובדים בתחום מאגרי מידע?

1.2 מהו הבסיס החוקי על פיו אתם עובדים בתחום אבטחת מידע?

2. שקיפות – האם מאגרי מידע נמצאים באתר המועצה?

3. תקציב – האם קיים תקציב למאגרי מידע? האם קיימת חריגה מהתקציב?

4. האם מאגרי המידע נרשמו במשרד המשפטים ? אם כן פרט את שמות מאגרי המידע ?

5. האם בוצע תשלום אגרה למאגרי המידע ? אם כן ציין בנוסף את שמות מאגרי המידע שבוצע תשלום עבורם ? ציין האם קיים חוב עבור תשלום לאחד ממאגרי המידע המחויבים בתשלום.

6. שרטט את המבנה הארגוני ?

6. הסמכות ומקצועיות, האם העובדים הנושאים בתפקיד מוסמכים טכנית לעסוק בתפקידם תעודות / ניסיון ? (אגף מערכות מידע)

#	שם העובד	תפקיד	הסמכה	ניסיון בשנים

1.

2.

3.

8. מערכת רציפות תפקודית

האם קיימת מערכת רציפות תפקודית ؟ באחריות של מי לספק אותה ؟

תאריך עדכון אחרון של המערכת ؟ האם זה כלול בפרוטוקול החרום ؟

9. פרוטוקול חרום

האם קיים שיתוף פעולה של גורמים העוסקים באתר (האינטרנט) המועצה

ובחשבון הפייסבוק הרשמי במצבי חרום. הם הוסמכו לכך ؟

10. ועדת היגוי לאבטחת מידע . האם קיימת וועדת היגוי לאבטחת מידע ?

11. אבטחת מידע: הוגש דו"ח ביקורת לשנת 2014 בנושא אבטחת מידע. סיכום המלצות מדו"ח זה.

11.1 מדיניות אבטחת מידע

נושא ביקורת 2014 האם בוצע תיקון ליקויים כן / לא בשנים 2018 -2019 ? – הערות

11.1.1 האם קיימת אסדרה בתחום ?

ניהול סיכונים, קווי מדיניות, הנחיות, נהלים, כללי גישה, הרשאות וסיווג מידע.

11.1.2 האם בוצע מינוי למנהל אבטחת מידע במועצה ?

11.1.3 האם קיים תקציב למנהל אבטחת מידע ?

11.1.4 האם בוצעה ביקורת פנימית לבדיקת פרצות באבטחת מידע ?

11.1.5 האם בוצעה ביקורת חיצונית לבדיקת פרצות באבטחת מידע ?

11.1.6 באילו אמצעים השתמשת בכדי לבדוק חשיפה של מאגרי מידע פנימיים ?

11.1.7 בקרות כניסה פיזיות לחדרים קריטיים, האם הוספו כנדרש ?

11.1.8 בקרות כניסה לוגיות למחשבים המוגדרים כקריטיים , האם הוספו כנדרש ?

11.1.9 ISO 17799 לא יושם במלואו. האם ייושם עד כה ?

11.1.10 פרוטוקול חירום, האם קיים ?

11.1.11 -בוצע אחסון פרוטוקול חרום בתחום מערכות מידע בכספת שמורה ?

-בוצע מינוי בנוהל מחליף בנבצרות של מנהל מערכות מידע ?

11.1.12 בוצעה בדיקת אבטחת מידע לשעון נוכחות של העובדים ?

11.1.13 האם מנהל מערכות מידע משולב בדיונים של המועצה בהם נדרשת חוות דעתו המקצועית בתחום ?

12. מאגרי מידע פנימיים (כגון : ארנונה, גבייה, חינוך, וועדה מקומית , תכנון ובנייה) פרט את המאגרים, המחלקה המחזיקה בהם וציין אם קיים גיבוי וסוג הגיבוי , האם קיימים הסכמי סודיות עם מחזיקי המשרות .

מאגרים פנימיים

#	מחלקה	שם המאגר	סוג הגיבוי	שם הנאמן למידע
1				
2				
3				
4				
5				
6				

13. האם בוצע סקר סיכונים למאגרי מידע עם כל הגורמים הרלוונטיים ?

סקר סיכונים למאגרים פנימיים היכולים לשמש את התובע העירוני

#	מחלקה	שם המאגר	סוג הגיבוי	שם הנאמן למידע
1				
2				

3

4

5

6

14. מאגרי מידע חיצוניים בדיקת סיכונים טרם ההתקשרות, פרט את המאגרים.

מאגרים חיצוניים

#	שם הגורם החיצוני	מחלקה	מאגר	האם בוצע בדיקה לסיכוני אבטחת המידע טרם ההתקשרות ?
1				
2				
3				
4				
5				
6				
7				

8

9

10

15. האם נחתמו הסכמים עם קבלני חוץ למאגרי מידע ? אם כן מה תוקפם ?

מאגרים חיצוניים

#	שם הגורם החיצוני	מחלקה	מאגר	האם נחתם הסכם עם קבלני חוץ	טרם ההתקשרות ?
1					
2					
3					
4					
5					
6					
7					
8					

9

10

16. נהלים פנימיים. האם קיימים נהלים פנימיים בגיוס עובד חדש / סיום עבודה

, כגון הסכם סודיות. ריענון הוראות שנתי

17. כמחלקה המספקת שירותים למועצה ולא לתושב האם קיים שיתוף פעולה

עם מחלקות / גורמים שונים ? (דובר המועצה, מוקד 106, אתר המועצה, נאמן

חופש המידע)

18. בהתייחס לשאלה הקודמת האם מחלקת מערכות מידע האמונה על מאגרי מידע מקיימת ערוצי תקשורת פתוחים מול נושאי תפקיד מקבילים , פגישות, וועדות מועצה, האם קיים תיעוד (פרוטוקול לישיבות הנ"ל)

19. האם בוצעה ביקורת בעבר שתרמה לשינויים כלשהם בתפקוד מאגרי מידע ואבטחת מידע ?