מועצה אזורית הגלבוע

התייחסות הרשות לליקויים בדוח ביקורת בתחום מתקפות סייבר ואבטחת מידע

פירוט הליקוי	
3. מדיניות אבטחת מידע ותכנית עבודה עמוד 4	
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 מבאגר או במערכות המאגר ; אופן התמודדות עם אירועי אבטחת מידע לפי חומרת האירוע ומידת רגישות המידע ; הוראות לעניין ניהול של התקנים ניידים ושימוש בהם.	קיים מסמך מדיניות מעודכן בארגון מ13/06/2022 בהתייחס להתנהלות ארגונית בנושא אבטחת מידע ומוגנות בפני מתקפות סייבר. הנהלים וההנחיות קיימים בנוסף בכונן משותף ברשת למנהלים ודרכם מועבר לעובדים. כל ההוראות וההנחיות שנטען שלא קיימים פורסמו למשתמשים גם בהנחיות וגם במסגרת מיילים שיצאו לעובדים. ריכוז כל ההנחיות הועברו לעובדים במייל בתאריך 15/06/2022 (צורף צילום מסך והמסמך). ממונה מאגרי המידע מציין שכל מי שיש לו גישה למאגרי המידע מכיר את נהלי האבטחה של מאגרי המידע, ומאגרי המידע בשלבי סיום תהליך הרישום.(תיעוד מיילים על תהליך הרישום) סעיף 4.1 סותר את סעיף 3.1 בדוח המבקר, כאשר סעיף 3.1 מציין שלא קיים במחלקה מסמך מדיניות ונוהל בתחום המחשוב ואבטחת המידע וב-סעיף 4.1 **מודגש כי קיים נוהל פנימי וחיצוני במחלקת מחשוב המועצה משנת 2021 אשר מנחה מה הוא הטיפול הנדרש באירועי אבטחת מידע.** עזרא דיין ממונה אבטחת מידע במועצה ביצע הדרכת עם מנהלים בארגון והנחייתם לגבי אופן הפעילות השוטפת מול מאגרי המידע, בוצע בתאריך 21/06/21. בוצעו מספר פעולות אשר מצמצמות את האפשרות לגישה למאגרים ע״י אנשים לא מורשים כדוגמת נעילת המחשב לאחר מספר דקות, הקשחת סיסמאות לרמה גבוה. החלפת הסיסמאות בתדירות גבוה והפעלת מנגנון 2FA בגישה מבחוץ למחשבי המועצה. בנושא הוראות לעניין ניהול של התקנים ניידים ושימוש בהם הופץ במייל ע״י רונן - מנהל מערכות המידע בארגון והעובדים נתבקשו לחתום על טופס ההנחיות.
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.	ממונה אבטחת המידע ביצע באוגוסט 21 סקר סיכוני אבטחת מידע. מצ״ב סקר הסיכונים. סיכום מבדק חדירות - הסקר אמור להיות מושלם עד סוף יולי ויועבר למועצה.
טיפול באירועי אבטחת מידע עמוד 4	

פירוט הליקוי	
4.2. במחלקת מחשוב של המועצה קיימים כלי ניטור על פעילות המשתמשים בצורה חלקית , זאת מאחר והמלצות הממונה על אבטחת המידע לרכישת ציוד 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.	יש הטעיה באופן שבו מוצגים הדברים, הפתרון שהמועצה החליטה ללכת עליו מתקדם יותר ונותן מעטפת הגנה כפולה ומשמעותית יותר ולכן ההליכה על הפיתרון הנ"ל שהופעל כפיילוט הייתה הליכה על איכות ולא על מחיר. סיכום מבדק חדירות - הסקר אמור להיות מושלם עד סוף יולי ויועבר למועצה.
5 בעל הרשאה עמוד׳ 4 עד 5	
5.1 לא התקבל מידע מלא האם כל 9 חברות החיצוניות שעובדות עם המועצה ושקיבלו הרשאה להחזיק במידע , לא ניתן לבדוק באם ההסכמים עם חברות אלו כוללים וחתמו על הסכם סודיות.	ההנחיה הייתה להטמיע בכל המכרזים את מדיניות האבטחה. באחריות אתי מזרחי, מנהלת אגף בקרה ותאום- לבחון שזה מיושם. השבוע ניתנה תזכורת למחלקת הרכש, לוודא שבכל חידוש התקשרויות או התקשרויות חדשות עם ספקים - מחילים את מדיניות האבטחה וחתימת הספק על נספח התחייבות למדיניות האבטחה והסכם סודיות בהתאם.
5.2. נמצא כי המועצה לא הגדירה לבעלי ההרשאה מסמך הגדרות ובכך , הגדילה את הסיכוי לפגיעה במאגרי המידע המוניציפאליים.	כל מנהל מאגר החותם על טופס כתב מינוי כמנהל המאגר, מיודע שהינו אחראי לאבטחת המידע במאגר ולעניין זה חלות עליו גם החובות המפורטות בתקנות. קיים מסמך ובו מפורט כל הטיפול במאגר מידע. כמו כן נעשתה הדרכה בשנת 2021 למנהלי המאגרים. יש תיקצוב ותכנון להדרכה חוזרת לכלל המנהלים והגורמים הרלוונטים בקרוב.
6. מיקור חוץ עמוד 5	

פירוט הליקוי	
6.1 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.	ראה להלן תשובתנו בסעיף 5.1
10.2 עמ׳ 20 המועצה התקשרה עם מספר גורמים חיצוניים לצורך קבלת שרות - לביקורת הוצגו חלק מהחוזים ושמות החברות העובדות במיקור חוץ ומחוברות למערכות המחשוב של המועצה ולכן לא ניתן היה לבדוק באם בוצעו בטרם ההתקשרות סיכוני אבטחת המידע	ראה להלן תשובתנו בסעיף 5.1
7. שקיפות עמוד 5	
7.1 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.	מתוך הזהירות המחייבת, פנינו אל אגף הסייבר בעניין. הנחיה ראשונית של נציג מטה הסייבר, הייתה כי אין חובה לפרסם את מאגרי המידע באתר המועצה ולכלל התושבים. לבקשתנו הנושא נבדק שוב, וההנחיה תוקנה - לפרסם את המאגרים. לאור זאת, הם יפורסמו בהתאם לחוק בתום תהליך הרישום.
8.2 עמ׳ 18 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	המאגרים בתהליך סיום רישום מול רשם החברות, תהליך זה לוקח זמן וכן התחלפו מנהלים ולכן נדרשו החתמות חדשות. **הערה - מרבית המאגרים בשלב מתקדם - החומרים החתומים הוגשו לממונה אבטחת המידע להגשתם למשרד המשפטים עבור רישום. מס׳ מאגרים נמצאים בבדיקה והסדרת רישומם תיעשה בהתאם לנדרש.מצ״ב טבלה מרכזת של סטטוס רישום המאגרים.**
3. ועדת היגוי לאבטחת מידע עמוד 13 עד 14	
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. כנדרש בנוהל מסגרת מס׳ 5. **3.2 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.**	הוקמה ועדה על פי הנחיה של משרד הפנים והתכנסות מתבצעת בהתאם לצורך. עם השלמת הקמת התשתיות הארגוניות לאבטחת המידע תיכנס פעילות הועדה לשגרה שהוחלט עליה - פעמיים בשנה. כרגע הקשר והליווי של הועדה לבחינת העמידה ביעדים הוא בשוטף.

פירוט הליקוי	
1.8 עמ׳ 14 נהלים פנימיים: הביקורת כן מציינת כי דווח שכל עובד בכיר חדש במועצה חותם על הסכם סודיות, לא צוין אם בוצעה 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.	מנהלת משאבי אנוש החדשה פנתה למשרד הפנים שלא הכיר הנחיה כזאת. מאידך, המנמ״ר העביר אליה את ההנחיה וכן את הטופס לרבות מסמך החתימה וההנחיה מיושמת במידי.
1.8 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.	ממונה אבטחת המידע ביצע באוגוסט 21 סקר סיכוני אבטחת מידע. מצ״ב סקר הסיכונים. סיכום מבדק חדירות - הסקר אמור להיות מושלם עד סוף יולי ויועבר למועצה.
6.1 עמוד 15 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.	במהלך שנת 2021 זוהה ע״י מטה הסייבר ניסיון חדירה לשרת הדואר של המועצה. מכיוון שבדיוק באותו זמן בוצעו הקשחות במערכת לא נדרשנו לבצע שינוי ואף על פי כן הוחלט על הוצאת שרת הדואר מרשת המועצה לשרת מאובטח של מיקרוסופט ובכך להפחית משמעותית את הסיכון לחדירה לרשת המועצה. תהליך זה אמור להסתיים עד סוף שנת 2022. ובכל מקרה נוכחנו שאמצעי האבטחה שננקטו יעילים.

לסיכום: למעשה ההערה המשמעותית לאורך כל הדוח אשר חוזרת על עצמה כמה וכמה פעמים, היא אי קבלת סקר סיכונים ומבדק חדירות מעודכן. בכל שאר הפעולות שהובילה המועצה ביוזמתה בתחום יצירת תשתית ארגונית לניהול אבטחת מידע ומוגנות מפני מתקפת סייבר נמצאת המועצה במצב מצוין יחסית למועצות אזוריות ומקומיות אחרות. עם השלמת התהליך יפורסמו המאגרים באתר כנדרש ופעילות ועדת ההיגוי תשולב בשיגרת הניהול על פי הנדרש. קיימת תיקיית נהלים והנחיות נגישה לעובדים כולל רענון הנחיות ובקרת ביצוע.

	פירוט הליקוי

בברכה,
ענת מור
מנכ"לית המועצה
ויו"ר וועדת היגוי למחשוב ואבטחת מידע