מבקר המועצה

# דוח מבקר המועצה

לשנים 2022 - 2021

מועצה מקומית אפרת
ת.ד 1022 מיקוד 90435
טל: 02-9939306
mevaker@efrat.muni.il

ט' שבט תשפ"ג
31 בינואר 2023

לכבוד
מר עודד רביבי
ראש המועצה

שלום רב,

הנדון: **<u>דוח מבקר המועצה לשנים 2022 - 2021</u>**

הנני מתכבד להגיש את דוח מבקר המועצה לשנים 2022 - 2021 בהתאם לסעיף 66 ל' (א) לצו בדבר ניהול מועצות מקומיות (יהודה ושומרון) תשמ"א.

דוח הביקורת כולל ממצאים, מסקנות והמלצות בנושא אבטחת מידע במועצה, ואני מקווה כי תמצא בו כלי עזר מועיל לשיפור התפקוד והניהול בתחום זה.

אני מוצא לנכון לציין לחיוב את הסיוע ושיתוף הפעולה המלא מצד כל עובדי המועצה והנהלתה במהלך עבודת הביקורת.

בהתאם לאמור בצו, מועבר בזה עותק מהדוח לחברי ועדת הביקורת.

בצו נקבע כי בתוך 3 חודשים ממועד קבלת הדוח מהמבקר, עליך להגיש לוועדת הביקורת את הערותיך על הדוח, ולהעביר העתק ממנו בצירוף הערותיך למליאת המועצה.

בברכה,
תמיר פוגל
מבקר המועצה

העתק:
חברי ועדת ביקורת

דוח ביקורת בנושא:

# אבטחת מידע במועצה

# תוכן עניינים

עמוד

1. מבוא ..... 5
2. עיקרי הממצאים והמלצות ..... 7
3. רקע נורמטיבי ..... 14
4. נתונים כספיים ..... 15
5. כוח אדם ..... 17
6. התקשרות עם חברה לאספקת שירותי מיחשוב ..... 18
7. ממונה על אבטחת מידע ..... 21
8. מדיניות ונהלי עבודה ..... 24
9. רישום מאגרים ומינוי מנהלי מאגרים ..... 25
10. סקר סיכונים ..... 28
11. בדיקות חדירה ..... 29
12. אבטחה פיזית וסביבתית ..... 30
13. ניהול הרשאות הגישה ..... 31
14. הדרכות ותרגולים ..... 32
15. גיבוי ושחזור נתוני אבטחה ..... 36
16. התקנים ניידים ..... 38
17. אבטחת תקשורת ..... 39
18. קריאת כרטיסים תקן EMV ..... 40
19. היערכות לאסון בתחום מערכות המידע ..... 40
20. נספחים ..... 44

נספח א' - תרשים רשת ..... 44

נספח ב' - מינוי ממונה אבטחת מידע ..... 44

נספח ג' - מדגם יישומי המועצה ..... 45

נספח ד' - הנושאים הנדרשים לקיום מדיניות עפ"י מסמך הרשות להגנת הסייבר ..... 45

נספח ה' - דוגמא לתרחיש ייחוס – תכנית BCP ..... 46

הבסיס החוקי לעבודת המבקר ..... 47

## 1. מבוא

במועצה קיימים מאגרי מידע בתחומים שונים כגון: גביית מיסים, תשלומים לספקים, שכר, חינוך, שירות פסיכולוגי, שירותי רווחה, כוח אדם, רישוי עסקים, חנייה, ועוד. המועצה אמורה לוודא כי קיימים ברשותה אמצעים המאפשרים רמה נאותה של אבטחת מידע והגנה מפני סיכוני סייבר, הן בשגרה והן בחירום, על מנת להבטיח את המשך התפקוד והפעילות התקינה של הרשות, ושמירה על צנעת הפרט כנדרש עפ"י החוק.

יצוין כי במהלך השנים האחרונות גדל היקף התקיפות באמצעות תוכנות זדוניות המתפשטות באמצעות גלישה באינטרנט, שימוש בדוא"ל, או חיבור פיזי של התקני זיכרון למחשבים ברשת הארגון. כמו כן, מגפת הקורונה שהחלה בשנת 2020 גרמה לעובדים רבים לעבוד גם מהבית, מה שהפך את סביבת העבודה לפגיעה יותר לסיכוני סייבר מאשר בעבר.

אבטחת המידע נועדה להגן על שלמות וזמינות המידע הקיים בארגון, ולמנוע גישה, שימוש, חשיפה, שיבוש, העתקה או השמדה של מידע או מערכות מידע על ידי גורמים חיצוניים. מתקפת סייבר כתוצאה מניצול חולשות הקיימות במערכת עלולה לשבש את הפעילות השוטפת, למנוע אספקת שירותים לתושבים, ולחשוף את המועצה להוצאות כספיות ותביעות משפטיות.

מאגרי מידע מסכנים בעצם קיומם את פרטיות הגורמים שפרטיהם כלולים במאגר, ונדרש לקבוע מנגנונים ייחודיים להגנה על המידע המצוי בהם כדי להבטיח את סודיות, מהימנות ושרידות המידע. המחוקק נתן דעתו להיבטים שונים של אבטחת מידע, והדבר בא לידי ביטוי בין היתר בחוק הגנת הפרטיות, התשמ"א-1981. סעיף 8 (ג) לחוק מחייב את המועצה ברישום של מאגרי מידע בפנקס מאגרי המידע במשרד המשפטים. בחודש מאי 2017 נכנסו לתוקף תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017, בהן הוגדרו חובות מפורטות לבעל מאגר מידע, בנוגע לקיום פעולות פיקוח ובקרה הנדרשות לאבטחת המאגר (להלן: "תקנות הגנת הפרטיות").

המחלקה הבכירה לביקורת המדינה במשרד ראש הממשלה פרסמה בחודש ספטמבר 2005 "נוהל מסגרת לאבטחת מידע" הכולל 38 נהלים לאבטחת מידע במשרדי הממשלה העוסקים בקביעת מדיניות ומיפוי מידע; הגורם האנושי ואבטחת המידע; אבטחה לוגית; אבטחה פיזית; גיבוי, שחזור והתאוששות; אבטחת תקשורת ושימושי אינטרנט; אבטחת מידע במחשבים המנותקים מרשתות המשרד, ועוד. יצוין כי נוהל המסגרת האמור אינו מחייב את המועצה, אולם יש בו כדי ללמד על התשתית הדרושה לאבטחת המידע ולשמירה על הפרטיות בגופים ציבוריים.

במועד עריכת הביקורת המועצה ניהלה את תחום מערכות המידע באמצעות חברה שסיפקה למועצה עובד במשרה מלאה, ששימש בפועל כמנהל מערכות מידע ראשי. רשת המחשבים של המועצה כללה את כל המשתמשים הנמצאים במשרדים בבניין המועצה, מטה הנוער, מטה הצעירים והמוקד הביטחוני (ראה תרשים בנספח א'). לביקורת נמסר שכל מבני המועצה מחוברים ביניהם בסיב אופטי פנימי של המועצה.

הביקורת נועדה לבחון את נאותות הטיפול בנושא אבטחת מידע והגנה על מאגרי מידע במערכות המחשוב במועצה בהתאם להוראות החוק והתקנות, ולבדוק את אפקטיביות מנגנוני אבטחת המידע והמוכנות להתמודדות עם סיכוני סייבר.

במהלך הביקורת נערכו פגישות עם מנמ"ר המועצה, ועם עובדים נוספים שיש להם נגיעה לנושא, כולל עובדי גזברות, מחלקת הגביה, הנהלת חשבונות, ועוד. הביקורת סקרה דוחות, קבצים, ומסמכים רלוונטיים, כולל תקציב, כרטסת הנהלת חשבונות, נהלי עבודה, רשימות משתמשים במערכות המידע, רשימת מאגרי המידע, ועוד.

טיוטת הדוח נמסרה כמקובל לעיון המבוקרים, לצורך קבלת התייחסותם לממצאים ולהמלצות הביקורת.

## 2. עיקרי הממצאים והמלצות

1. בתקציב השנתי של המועצה לא קיים סעיף ייעודי עבור הוצאות בתחום המיחשוב, ואף לא בתחום אבטחת מידע. העדר רישום הוצאות אלו בסעיפים ייעודיים פוגע בשקיפות, מקשה על בקרה על הוצאות בפועל לעומת התקציב ועל תכנון שנתי של ההוצאות בתחום המחשוב בהתאם לצרכים.

**מומלץ לכלול בסעיף ייעודי בתקציב את כלל הוצאות המיחשוב של המועצה (רכש, תוכנות, תשלומים בגין פעילות המנמ"ר), ובסעיף נפרד הוצאות בתחום אבטחת מידע, כגון: רכישת כלי ניטור ייעודיים, הזמנת בדיקות חדירה, ועוד.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצה.

גזבר המועצה ציין בתגובתו כי בדעתו לאמץ במלואה את המלצת הביקורת, אך מאחר והתקציב כבר אושר הדבר יבוא לידי ביטוי בתקציב השנה הבאה.

2. נמצא כי ההסכם עם חברת המחשוב אינו מתייחס לאספקת עובד בתפקיד מנמ"ר, האמור להיות אחראי על מכלול שירותי מערכות המידע והיישומים הדיגיטאליים של המועצה ועל ניהול כלל המשאבים והתוויית האסטרטגיה של מערכות המידע, אלא לאספקת עובד בתפקיד מנהל רשת ואחראי תמיכה.

**מומלץ לקבוע בהסכם שהחברה תמנה מטעמה עובד בתפקיד מנמ"ר המועצה העומד בדרישות שנקבעו לתפקיד, ונושא באחריות למכלול שירותי מערכות המידע, גיבוש ויישום מדיניות מערכות המידע, ניהול תקציב והתקשרויות בתחום מערכות המידע, הכנת תכניות עבודה, ועוד.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצה.

3. נמצא כי ההסכם מתייחס בעיקר למתן שירותי תחזוקה ותיקון מחשבים, ואינו מבחין בין 3 סוגי שירותי הניתנים בפועל על ידי החברה: תחזוקת רשת, שירותי מערכות מידע, ושירותי אבטחת מידע.

**מומלץ לפרט בהסכם את מכלול השירותים הניתנים בפועל ע"י המנמ"ר ועובדי החברה, תוך אבחנה ברורה בין סוגי השירות.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי ההמלצה מקובלת ותבוצע בהקדם.

4. נמצא כי החברה אינה מיישמת בפועל את סעיף 10.5.2 להסכם, לפיו אמור להגיע למועצה מנהל רשת בכיר אחת לשבוע, בנוסף לעובד המשמש כמנמ"ר. לביקורת נמסר כי במקרה של היעדרות המנמ"ר, מגיע למועצה עובד המשמש כמנמ"ר חלופי, אולם לא מגיע מידי שבוע מנהל רשת בכיר.

**מומלץ לדרוש מהחברה לשלוח למשרדי המועצה מידי שבוע עובד נוסף, כמתחייב עפ"י ההסכם, ולשפר את הבקרה בנושא.**

המנמ"ר ציין בתגובתו לטיוטת הדוח כי בשלב זה מגיע פעם בחודש מנהל רשת או מנהל אבטחת מידע, והחברה תשתדל להגביר את תדירות הגעתם למועצה.

5. נמצא כי המנמ"ר כפוף בפועל למנכ"ל המועצה, אולם הדבר לא צוין במפורש בהסכם עם החברה.

**מומלץ לציין בהסכם מיהו הגורם במועצה האחראי על הפעילות של המנמ"ר ועל עריכת פיקוח ובקרה שוטפת על עבודתו.**

המנמ"ר ציין בתגובתו כי הוא מקבל את ההמלצה לפיה יצוין בהסכם עם החברה שפעילות המנמ"ר תהיה תחת פיקוח ראש המועצה או מנכ"ל המועצה.

6. נמצא כי ההסכם אינו מתייחס לחובת החברה לשלוח את עובדיה המעניקים שירות למועצה, לקורסים או השתלמויות כדי להתעדכן בטכנולוגיות חדישות, שינויים רגולטוריים, וכד'.

**מומלץ לכלול בהסכם את חובת החברה לשלוח את עובדיה לקורסים והשתלמויות, כדי להבטיח המשך קבלת שירותים ברמה נאותה לאורך זמן.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי חובת שליחת העובד לקורסים והשתלמויות אמורה לחול על החברה וגם על המועצה.

7. נמצא כי החברה אינה מגישה למועצה דוחות מפורטים לגבי כלל פעילויות המנמ"ר, כפי שנדרש עפ"י סעיפים 10.11, ו - 24 להסכם.

**מומלץ להקפיד על קבלת דוחות פעילות מהחברה בתדירות שנקבעה בהסכם, ולקבוע בהסכם ובנוהל העבודה את הגורם במועצה שאמור לקבל את הדוחות ולקיים ישיבות תקופתיות עם המנמ"ר לצורך מעקב ובקרה.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצה.

8. במועד הביקורת המנמ"ר שימש בפועל גם כממונה אבטחת מידע, לאחר שקיבל מינוי בכתב לתפקיד ע"י ראש המועצה. נמצא כי ההסכם עם החברה אינו מתייחס למתן שירותי אבטחת מידע, כפי הנדרש.

**מומלץ לכלול בהסכם את נושא אבטחת המידע, ולפרט בו את חובות החברה ומטלות המנמ"ר בתחום זה בהתאם להוראות החוק והתקנות המחייבות.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצה.

9. בכתב המינוי שניתן לממונה על אבטחת מידע, לא צוין שהוא כפוף למנכ"ל המועצה. נמצא כי גם בהסכם עם החברה וגם בנוהלי העבודה, אין התייחסות לנושא הכפיפות של העובד המשמש כממונה אבטחת מידע.

**מומלץ שכפיפות הממונה על אבטחת מידע למנכ"ל תעוגן בכתב המינוי, וכן בהסכם עם החברה ובנהלי העבודה במועצה.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח כי ההמלצה מקובלת, והוא יפעל להוצאת כתב מינוי מתוקן.

10. נוהל אבטחת מידע שהוצג לביקורת, טרם אושר על ידי מנכ"ל המועצה.

**מומלץ שמנהל אבטחת מידע יגיש בהקדם את הנוהל לאישור המנכ"ל.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצה.

11. לא נמצאה תכנית כתובה לבקרה שוטפת של ממונה אבטחת מידע על עמידה בדרישות שנקבעו בתקנות. כמו כן לא נמצא תיעוד לדיווחים שהועברו למנכ"ל על ממצאי בקרה שוטפת בנושא.

**מומלץ שמנהל אבטחת מידע יכין תכנית עבודה לביצוע בקרה שוטפת על יישום תקנות הגנת הפרטיות, יפעל לביצוע התכנית, ויעביר דיווחים תקופתיים למנכ"ל המועצה על הממצאים שעלו בבקרה.**

**מומלץ שהמנכ"ל ינהל מעקב אחר קבלת דיווח תקופתי על ממצאי הבקרה שנערכה בנושא.**

מנמ"ר המועצה ציין בתגובתו כי הוכנה על ידו תכנית לבקרה בנושא אבטחת מידע, והוא העביר דיווחים שוטפים בנוגע לאירועי אבטחת מידע למנכ"ל ולראש המועצה באמצעות הודעות מייל.

12. המנמ"ר המשמש גם כממונה אבטחת מידע, מטפל במקביל גם בעדכונים, הרשאות, ביצוע גיבויים, ועוד, פעולות שלגביהם הוא אמור לערוך פיקוח ובקרה כממונה על אבטחת מידע ולכן עלולות להעמידו בחשש לניגוד עניינים.

**מומלץ שעובד נוסף מטעם החברה שעפ"י ההסכם אמור להיות מידי שבוע במועצה, ימונה לתפקיד ממונה על אבטחת מידע במועצה, ולא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצה.

13. במועד עריכת הביקורת לא נמצאה תכנית עבודה מקושרת תקציב בנושא אבטחת מידע.

**מומלץ שהממונה על אבטחת מידע יכין מידי שנה תכנית עבודה מקושרת תקציב בנושא, על מנת להבטיח הקצאת משאבים נאותה בהתאם לצרכים.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצה.

14. בנהלים שהוצגו לביקורת לא צוין מועד עריכת הנוהל, תאריך עדכון אחרון, והם לא היו חתומים ע"י המנכ"ל כנדרש. בנוסף, נוהל אבטחת מידע תיאר ממשקי עבודה בין המנמ"ר לבין ממונה אבטחת מידע, כאשר בפועל מדובר באותו גורם. הנוהל גם לא פירט פעולות בסיסיות של ממונה אבטחת מידע, כגון: תדירות הדרכות משתמשים, תרגול תכנית התאוששות מאסון, ועוד.

**מומלץ שהמנמ"ר יעדכן את הנהלים הקיימים ויכלול בהם נושאים נוספים שצוינו בדוח.**

**מומלץ לצרף לנהלים גם נספחים, כגון: טופס דיווח על אירוע אבטחת מידע, התחייבות לשמירת סודיות של העובדים, וכד'.**

**מומלץ שהנהלים יועברו לאישור וחתימת מנכ"ל המועצה, כפי הנדרש.**

המנמ"ר ציין בתגובתו לטיוטת הדוח כי הוא מקבל את המלצות הביקורת, ונושא הנהלים יטופל בהקדם.

15. למעט 2 נהלי אבטחת המידע שהוצגו לביקורת, לא קיימת במועצה מדיניות סדורה בכתב המתייחסת לכלל היבטי אבטחת המידע, כפי שנדרש בהנחיות.

**מומלץ לקבל מהחברה המלצה על מסמך מדיניות אבטחת מידע עבור כלל מערכות המידע, אשר יידון מול המנמ"ר ויאושר על ידי הנהלת המועצה.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצה.

16. נמצא כי מספר מאגרי מידע של המועצה אינם רשומים במשרד המשפטים, כגון מאגר פניות למוקד העירוני, תיקי רישוי עסקים, רשימת מטופלי רווחה, ועוד. במועד הביקורת גם לא נמצא תיעוד מסודר של רשימת מנהלי מאגרי המידע במועצה, ולכלל הרישומים שבוצעו במשרד המשפטים.

**מומלץ למפות את כל מאגרי המידע במועצה ואת המידע הנאסף במסגרתם, ולבחון את החובה לרישומם בפנקס מאגרי המידע במשרד המשפטים, בשיתוף עם המנמ"ר והיועץ המשפטי.**

**מומלץ להשלים את רישום כל מאגרי המידע החייבים בכך עפ"י החוק, בהתאם לממצאי הבדיקה האמורה.**

**מומלץ להכין רשימה עדכנית של מנהלי מאגרי המידע הקיימים במועצה, ולהקפיד על תיעוד מסודר של מסמכי הרישום של כל מאגר.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח כי הוא מקבל את ההמלצות, והנושא אמור להיות מטופל על ידי ממונה אבטחת מידע.

17. במועד הביקורת לא נמצא תיעוד לעריכת סקרי סיכונים במועצה לבחינת נאותות אבטחת המידע, ואף לא לעריכת מבדקי חדירה למערכות המידע במהלך השנים שנבדקו. עוד נמצא, כי הנושאים האמורים לא נכללו במסגרת נוהל אבטחת המידע.

**מומלץ להקפיד על ביצוע סקר סיכונים ובדיקות חדירה למערכות המועצה אחת לשמונה עשר חודשים לפחות, כנדרש עפ"י התקנות.**

**מומלץ לעגן את עריכת סקרי הסיכונים ובדיקות החדירה בנוהל אבטחת מידע ולתקצב את עריכתם בסעיף הוצאות ייעודי בנושא אבטחת מידע.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי מבוצע סקר סיכונים או מבדקי חדירה על ידי החברה מידי חצי שנה, אך הוא מקבל את ההמלצה לעגן את הנושא בנוהל מסודר.

18. בבדיקת אמצעי אבטחת המידע הפיסיים הנדרשים בחדר השרתים במועצה לא נמצאו ליקויים, כמפורט בדוח. עם זאת, נוהל אבטחת המידע במועצה לא כלל התייחסות לכל אמצעי האבטחה הפיזיים הנדרשים עפ"י התקן והתקנות.

**מומלץ לכלול בנוהל אבטחת מידע התייחסות לכל אמצעי האבטחה הפיזיים הנדרשים בחדר השרתים.**

**מומלץ כי אחת לתקופה הנושא האמור ייבחן שוב ע"י ממונה אבטחת מידע.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצות.

19. בבדיקת הרשאות המשתמשים במערכות המועצה בהתאם להגדרות התפקיד של העובדים, לא נמצאו ליקויים. נמצא כי רק המנמ"ר מוגדר במערכת כמשתמש-על (Administrator), לא נמצאו משתמשים שאינם מזוהים באופן חד ערכי (גנריים), ואף לא משתמשים שכבר עזבו את עבודתם במועצה.

20. נמצא כי מלבד שליחת הודעות מייל רבות למשתמשים אשר כללו הנחיות ועדכונים בנושאים שונים, מנמ"ר במועצה כמעט ולא ביצע הדרכות לעובדים כנדרש עפ"י ההסכם עם חברת המחשוב, למעט מפגש בחודש מרץ 2018 ויוזמה להעברת הדרכות בחודש יולי 2018, כמפורט בדוח.

**מומלץ לפרט בהסכם עם החברה את תדירות ואופן ביצוע ההדרכות לעובדים, ולשפר את הבקרה על ביצוע ההדרכות הלכה למעשה.**

המנמ"ר ציין בתגובתו כי הוא מקבל את ההמלצה, והחל מחודש ינואר 2023 הוא מבצע מידי שבוע הדרכות ותרגולים לקבוצות שונות של עובדי המועצה.

21. במועד הביקורת לא נמצאה תכנית עבודה שנתית לביצוע הדרכות ע"י המנמ"ר בנושא מערכת המחשוב ואבטחת המידע. בנוסף, בנהלי אבטחת המידע לא נמצאה התייחסות לנושא ההדרכות, הן לגבי עובדים חדשים שנקלטו במועצה והן לגבי הדרכות לעובדים פעילים.

**מומלץ לכלול את נושא ההדרכות במדיניות אבטחת המידע במועצה ובמסגרת נהלי אבטחת המידע.**

**מומלץ שהמנמ"ר יכין תכנית עבודה שנתית לביצוע הדרכות בנושאים שונים, ויגיש אותה לאישור מנכ"ל המועצה.**

**מומלץ להפיץ לכל העובדים והמנהלים את תכנית ההדרכות השנתית לצורך רישום וקביעת מועדי השתתפות, ולערוך מעקב אחר השתתפותם בפועל.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצות.

22. במועד הביקורת המועצה נעזרה במערכת לניהול גיבויים של חברה חיצונית. בבדיקת הנושא לא נמצאו ליקויים. נמצא כי מבוצע גיבוי המתוזמן באופן יומי של כלל מאגרי המועצה, כי ניתן לשחזר בקלות את נתוני הגיבוי למערכות המועצה, וכי בנוסף לגיבוי הממוחשב בענן מבוצע גיבוי באמצעות דיסק נייד אשר נשמר בגזברות בכספת נעולה ומאובטחת.

23. בתקנות הגנת הפרטיות נקבע כי בעל מאגר מידע יגביל או ימנע אפשרות לחיבור התקנים ניידים למערכות המאגר במתכונת ההולמת את רמת אבטחת המידע שחלה על המאגר. נמצא כי הגישה להתקנים ניידים נחסמה על ידי מנמ"ר המועצה באמצעות מערכת אבטחת מידע, כפי הנדרש. בבדיקת הנושא הביקורת לא העלתה ממצאים חריגים.

24. נמצא כי המועצה נעזרת ברכיב אבטחת מידע חיצוני לשם חציצה בין רשתות האינטרנט והרשת הפנימית, כפי הנדרש. הרכיב מאפשר בין היתר חסימת גישה לתכנים בלתי מורשים ברשת, ומניעת גישה של גורמים שאינם מורשים למאגרי המידע של המועצה. עוד נמצא, כי המועצה נעזרת במערכת של חברת אנטי וירוס לצורך חסימת וירוסים, והמערכת האמורה מתעדכנת באופן שוטף.

25. בדיקה שנערכה במחלקת הגבייה העלתה, כי במועצה טרם מיושם תקן EMV שנועד לאבטחה מוגברת ולמניעת הונאות בסליקת עסקאות בכרטיסי אשראי. נמצא כי תשלום באשראי של תושב המגיע למחלקה מבוצע באמצעות הקלדה ידנית של פרטי כרטיס האשראי, בדומה לביצוע עסקה טלפונית. כתוצאה מכך, התשלומים במחלקה הם ברמת אבטחה נמוכה יותר ובניגוד לתקן EMV.

**מומלץ לפנות לחברה האחראית על מתן שירותי הסליקה במועצה לצורך שדרוג המערכת, ועמידתה בתקנים המקובלים בארץ.**

המנמ"ר ציין בתגובתו לטיוטת הדוח כי הנושא האמור לא נמצא בתחום אחריותו, אך הוא יפנה לחברת סליקת האשראי על מנת לבצע את ההמלצה.

26. נמצא כי בנוהל התאוששות מאסון של המועצה אין את כל המרכיבים שצוינו בהנחיות רשות הסייבר ותקן ISO 22301. הנוהל אינו מתייחס למספר היבטים, כגון רעידת אדמה הגורמת לקריסת המבנה כולל חדר השרתים, קריסת אחד מספקי שירותי הענן, מתקפת כופר, ועוד. בנוסף, אין בנוהל פירוט של הגורמים האחראים לכל תרחיש והפעולות הנדרשות, מיפוי תהליכי העבודה העלולים להיפגע בעת אסון, כגון: רישום לגני ילדים, תשלומים לספקים, גביית ארנונה, ועוד, ואופן ההתמודדות עם האירוע לצורך צמצום הנזקים וחזרה לשגרה.

**מומלץ לכלול בנוהל התאוששות מאסון את כל ההיבטים הנדרשים בהנחיות. מומלץ לתקצב הכנת תכנית BCP בהתאם להצעות מחיר ממספר ספקים המתמחים בהכנת התכנית, עפ"י תכולה שתוכן ע"י ממונה אבטחת המידע.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצות.

## 3. רקע נורמטיבי

### 3.1 הנחיות מערך הסייבר הלאומי

מערך הסייבר הלאומי, הינו הגוף הממלכתי המופקד על "הגנת מרחב הסייבר הלאומי של מדינת ישראל מפני איומי סייבר, ועל קידום וביסוס עוצמתה בתחום" (להלן: "מערך הסייבר").

מערך הסייבר פרסם מסמך שדן ב"תפיסה לאומית בסייבר להיערכות ולניהול מצבי משבר נכסי סייבר", אשר נועד לסייע בהעלאת העמידות והחוסן של ישראל בסייבר. מסמך זה מגדיר כאירוע סייבר כמצב שיש בו איום ממשי לפגיעה בנכס סייבר חיוני, או פגיעה בו בפועל, אשר עלול לגרום נזק קריטי לשגרת הפעילות ולתדמית, נזק כלכלי ופגיעה בחיי אדם. משבר סייבר נע במדרג רמות חומרה, ובמצב קיצון נגרם נזק ניכר לתהליכי ליבה ולרציפות התפקוד הארגונית/המשקית, והוא עלול להסלים עד כדי מצב חירום לאומי.

מערך הסייבר הלאומי פרסם 2 מסמכים עיקריים המתייחסים לנושא תכנית BCP (תכנית המשכיות עסקית). מסמכים אלו כוללים רשימה של בקרות הנדרשות ליישום בארגון:

- "תורת ההגנה בסייבר לארגון" (להלן: "**תורת ההגנה 2018**")

פורסם בחודש אפריל 2018 מסמך המסמך כולל בין פירוט הבקרות הנדרשות מן הארגון לטובת הגנה בתחום הסייבר, בקרות אלו כוללות תהליכים, נהלים, מערכות הגנה וטכנולוגיות, אשר על הארגון ליישם במטרה להפחית את הסיכון להתממשות אירוע במרחב הסייבר.

- "המדריך היישומי (השלם) להגנת הסייבר של הארגון" (להלן: "**תורת ההגנה 2021**")

פורסם בחודש יוני 2021 . המסמך מעדכן ומרחיב את תורת ההגנה 2018, מטרת המסמך הינה לסייע בהשגת הכרה טובה יותר של הארגון את הסיכונים הרלוונטיים, גיבוש מענה הגנתי ולסייע במימוש תכנית להפחתת הסיכונים בהתאם.

3.2 <u>תקנות הגנת הפרטיות</u>

בחודש מאי 2017 נכנסו לתוקף תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017, בהן הוגדרו חובות מפורטות לבעל מאגר מידע, בנוגע לקיום פעולות פיקוח ובקרה הנדרשות לאבטחת המאגר (להלן: "תקנות הגנת הפרטיות"). תקנות אלו מבקשות להגן על האנשים שמידע אודותיהם קיים במאגר המידע (להלן: "תקנות הגנת הפרטיות").

התקנות האמורות כוללות מספר הגדרות בסיסיות, ביניהם:

- <u>אבטחת מידע</u> - אבטחת מידע פירושה הגנה על שלמות המידע והגנה עליו מפני חשיפה, שימוש או העתקה, על ידי גורמים שאינם מורשים.
- <u>מהי הרמה הנדרשת לכל מאגר</u> - התקנות קובעות שלוש רמות של מאגרי מידע, עליהן חלות רמות אבטחה שונות, בהתאם לסיכוני האבטחה שהם מייצרים.

## 4. נתונים כספיים

משרד הפנים פרסם "הנחיות להנהלת חשבונות ודווח כספי ברשויות המקומיות" (להלן: "ההנחיות") הנחיות אלו קובעות בין היתר כי מטרת ניהול החשבונות הינה הצגת הנתונים בשקיפות מלאה כפי שמתואר בסעיף 6.1.2 להנחיות:

**6.1.2 מיון ושיוך הכנסות והוצאות לסעיפי התקציב.**

כלל חשוב ומנחה בניהול החשבונות התקציביים הוא הקפדה על מיון ושיוך נכון של ההכנסות וההוצאות לפרקים ולסעיפים המתאימים של התקציב המאושר (התקציב הרגיל או תקציב הפיתוח) המהווה את תוכנית העבודה של הרשות. המטרה העיקרית של הרישום החשבונאי והדיווח הכספי הוא להציג בפני קורא הדוח הכספי את הביצוע הנכון של התקציב המאושר בשקיפות ובגילוי נאות, בפני מועצת הרשות המקומית, מוסדות השלטון המרכזי וציבור משלמי המיסים.

בכדי להשיג את מטרת הגילוי הנאות יש להקפיד הקפדה מלאה, כי כל הוצאה או הכנסה תרשם במלואה (ברוטו) **ללא קיזוז** כל שהוא בין ההוצאות להכנסות או להיפך, על מנת לתת ביטוי מלא לשלמות ההכנסה ושלמות ההוצאה.

יש לשייך את התקבולים לסעיף ההכנסה המתאים סמוך למועד קבלתם. אין להותיר את מיון ההכנסות לסוף התקופה המדווחת.

תקציב המועצה כולל סעיף 1613000750 בשם "מזכירות-עבודות קבלניות". נמצא כי הסעיף משמש לרכישות וקבלת שירותים עבור הנהלת המועצה, וכן לרכישות ציוד בתחום המיחשוב ותשלומים שוטפים לחברה חיצונית בגין אספקת שירותי מיחשוב.

להלן היקף ההוצאות שנרשמו בסעיף האמור בשנים האחרונות (באלפי ₪):

| מס' סעיף תקציבי | שם הסעיף | 2019 | 2020 | 2021 | 2022 * |
|---|---|---|---|---|---|
| 1613000750 | מזכירות עבודות קבלניות | 1,249 | 1,229 | 990 | 946 |

* נכון ליום 25.12.22

בדיקה בכרטסת הנהלת החשבונות העלתה, כי בסעיף "מזכירות-עבודות קבלניות" נרשמות הוצאות בגין שירותים שונים, כולל טלפון וחשמל, תשלומים לחברת בזק בינלאומי ולחברת האנטי וירוס, וכן עבור תוכנות מיחשוב לכלל מחלקות המועצה. בנוסף, נרשמים תשלומים חודשיים בסך של כ- 32 אלפי ₪ לחברה חיצונית בגין אספקת שירותי מיחשוב, המסתכמים בכ- 384 אלפי ₪ לשנה.

נמצא כי בתקציב המועצה לא קיים סעיף ייעודי עבור הוצאות בתחום המיחשוב, ואף לא בתחום אבטחת מידע. לדעת הביקורת, העדר רישום הוצאות אלו בסעיפים ייעודיים פוגע בשקיפות מול מועצת הרשות ומוסדות השלטון, ומקשה על עריכת בקרה על ההוצאות בפועל לעומת התקציב. כמו כן, הדבר מקשה על תכנון שנתי מקושר תקציב של הוצאות בתחום המחשוב, בהתאם לצרכים שהועלו ע"י המנמ"ר והגורמים המקצועיים.

**מומלץ לכלול בסעיף ייעודי בתקציב את הוצאות המיחשוב הכוללות של המועצה (רכש, תוכנות, תשלומים בגין פעילות המנמ"ר), ובסעיף נפרד את ההוצאות בתחום אבטחת המידע, כגון: רכישת כלי ניטור ייעודיים, הזמנת בדיקות חדירה למערכת, ועוד.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצה.

גזבר המועצה ציין בתגובתו כי בדעתו לאמץ במלואה את המלצת המבקר, אך מאחר והתקציב השנתי כבר אושר הדבר יבוא לידי ביטוי בתקציב השנה הבאה.

## 5. כוח אדם

רשות מקומית אמורה להעסיק מנהל מערכות מידע ראשי (מנמ"ר) ולהגדיר את תחומי אחריותו בהתאם לצרכים והגדרות התפקיד הנדרשות. עפ"י הנחיות משרד הפנים המנמ"ר אחראי על תכנון וניהול מערכות המידע של הרשות כמנגנון ניהולי ובסיסי בארגון. עוד נקבע, כי המנמ"ר נושא באחריות למכלול שירותי מערכות המידע וליישומים הדיגיטאליים של הרשות ועל ניהול כלל המשאבים, וכן על התוויית האסטרטגיה של מערכות המידע והיישומים התומכים בפעילויות ובתהליכי העבודה.

להלן תחומי האחריות של המנמ"ר כפי שנקבעו על ידי משרד הפנים:

משרד הפנים
מינהל השלטון המקומי
אגף בכיר בקרת הון אנושי ברשויות המקומיות

**מנהל מערכות מידע ראשי (מנמ"ר)- Chief (CIO) Information Officer**

| |
|---|
| **נתוני המשרה** |
| **סוג תפקיד:** |
| התפקיד אינו מוגדר בחקיקה. |
| **תאריך עדכון:** |
| 20/6/2019 |
| **תיאור התפקיד** |
| **ייעוד:** |
| תכנון וניהול מערכות המידע של הרשות המקומית כמנגנון ניהולי ותפעולי בסיסי בארגון.<br>נושא/ת באחריות למכלול שירותי מערכות המידע והיישומים הדיגיטליים של הרשות ועל ניהול כלל המשאבים. אחריות על התוויית האסטרטגיה של מערכות המידע והיישומים הדיגיטליים כך שיתמכו באסטרטגיה, בתהליכים העסקיים ובפעילויות של הרשות המקומית. |
| **תחומי אחריות:** |
| 1. אספקת מערכות ושירותי מחשוב לרשות.<br>2. גיבוש ויישום של מדיניות מערכות מידע ברשות, בהלימה לאסטרטגיה ולתהליכי העבודה של הרשות.<br>3. תכנון תכניות עבודה וניהול התקציב בתחום מערכות המידע.<br>4. ניהול עובדי וספקי מערכות המידע.<br>5. ניהול התקשרויות ורכש בתחום מערכות המידע. |

בנוסף למנמ"ר, נדרש למנות ברשות מקומית ממונה על אבטחת מידע. סעיף 17ב' לחוק הגנת הפרטיות קובע כי המועצה מחויבת למנות אדם בעל הכשרה מתאימה לתפקיד הממונה על אבטחת מידע.

בהנחיות משרד הפנים נקבע כי ניהול אבטחת מידע ברשות יהיה בהתאם להוראות הדין הקיים ולנהלי הרשות, כפי שמוצג להלן:

משרד הפנים
מינהל השלטון המקומי
האגף לכוח אדם ושכר ברשויות המקומיות

**Chief Security officer – מנהל אבטחת מידע**

| |
|---|
| **נתוני המשרה**<br>**(סעיף תקציבי *****)** |
| **סוג תפקיד:** תפקיד מוגדר בחקיקה. |
| כל גוף ציבורי (לרבות רשויות מקומיות) ימנה ממונה על אבטחת המידע (סעיף 17 ב' לחוק הגנת הפרטיות).[1] |
| **תיאור התפקיד** |
| **ייעוד:** |
| ניהול אבטחת המידע ברשות המקומית בהתאם להוראות הדין הקיים ולנהלי הרשות המקומית ומדיניותה. |
| **תחומי אחריות:** |
| 1. תכנון מדיניות אבטחת המידע ובקרה על יישומה.<br>2. תכנון וביצוע סקרי אבטחת מידע.<br>3. ניהול ההרשאות, ודרכי הגישה למשתמשים.<br>4. תכנון ויישום תוכנית התאוששות - DRP.<br>5. ניהול ההגנה על מערכות המידע והתקשורת. |

## 6. התקשרות עם חברה לאספקת שירותי מיחשוב

במועד הביקורת הטיפול בתחום המיחשוב במועצה נוהל ע"י חברה שנבחרה באמצעות מכרז פומבי (11/2020) לקבלת "שירותי תחזוקה ותיקון מחשבים במשרדי המועצה ומוסדותיה". ההסכם עם החברה הזכיינית נחתם ביום 2.11.20. תקופת ההתקשרות נקבעה ל - 36 חודשים, עם אופציה להארכה בשנתיים נוספות.

שירותי החברה ניתנו באמצעות העסקת נציג קבוע במועצה בהיקף של משרה מלאה, ששימש בפועל כמנמ"ר המועצה (מנהל מערכות מידע ראשי).

בבחינת תנאי ההסכם עם החברה ומידת יישומם בפועל, עלו הממצאים הבאים:

6.1 נמצא כי ההסכם אינו מתייחס לאספקת עובד בתפקיד מנמ"ר המועצה, האמור להיות אחראי על מכלול שירותי מערכות המידע והיישומים הדיגיטאליים של הרשות, ועל ניהול כלל המשאבים והתוויית האסטרטגיה של מערכות המידע, אלא לאספקת עובד בתפקיד מנהל רשת ואחראי תמיכה, כמתואר בסעיף 10.5 להסכם:

10.5. הספק ימנה עובדים מטעמו (בהתאם לכשירויות כמפורט בתנאי המכרז) אשר יבצעו את השירותים. מנהל הרשת ישמש כאיש קשר בין המועצה לספק לשם טיפול בנושאים הקשורים לקיום מחויבות הספק ע"פ הסכם זה.

10.5.1 שרות במשרדי המועצה - יבוצע ע"י **מנהל רשת** ואחראי תמיכה העומד בדרישות הסף בהיקף של משרה מלאה במשרדי המועצה (5 ימים בשבוע).

**10.5.2 שירות מנהל רשת בכיר יבוצע על ידי מנהל בכיר בחברה – בהגעה אחת לשבוע למשרדי המועצה.**

10.5.3. זהות מבצעי השירותים מטעם הספק תהיה כמפורט לעיל. והשירותים יבוצעו על-ידי כל אחד מהם באופן אישי, בהתאם

**מומלץ לקבוע בהסכם שהחברה תמנה מטעמה עובד בתפקיד מנמ"ר המועצה העומד בדרישות שנקבעו לתפקיד, ונושא באחריות למכלול שירותי מערכות המידע, גיבוש ויישום מדיניות מערכות המידע בהלימה לאסטרטגיה ולתכניות העבודה של הרשות, הכנת תכניות עבודה, ניהול תקציב, ניהול התקשרויות בתחום מערכות המידע, ועוד.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצה.

6.2 נמצא כי ההסכם אינו מבחין בין 3 סוגי שירותי הניתנים כיום בפועל על ידי החברה: שירותי תחזוקת רשת, שירותי מערכות מידע, ושירותי אבטחת מידע. לחילופין, ההסכם מתייחס בעיקרו למתן שירותי תחזוקה ותיקון מחשבים, כמפורט להלן:

> שירותי התחזוקה ותיקון המחשבים כוללים, בין היתר, תחזוקת רשתות המחשבים, מחשבים, תיקון תשתיות רשת בסיביות ואספקת ציוד נלווה, ביצוע תיקונים, אחזקה שוטפת, התקנת ציוד ותוכנות, מתן פתרון מידי לבעיות דחופות, מתן הדרכות, אחזקה, תמיכה ופתרון בעיות המתעוררות מעת לעת, וכן כל השירותים וההתחייבויות שעל הספק לבצע על פי המפורט בהסכם זה.

**מומלץ לפרט בהסכם את מכלול השירותים הניתנים בפועל ע"י החברה באמצעות המנמ"ר, תוך אבחנה ברורה בין סוגי השירות.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי ההמלצה מקובלת ותבוצע בהקדם.

6.3 נמצא, כי החברה אינה מיישמת בפועל את האמור בסעיף 10.5.2 להסכם, לפיו מנהל רשת בכיר יגיע למשרדי המועצה אחת לשבוע, וזאת בנוסף על מנהל הרשת המשמש כמנמ"ר המועצה. לביקורת נמסר כי במקרה של היעדרות מהעבודה של המנמ"ר, החברה שולחת למועצה נציג אחר המשמש כמנמ"ר חלופי, אולם לא מגיע מידי שבוע למועצה מנהל רשת בכיר.

**מומלץ לדרוש מהחברה לשלוח למשרדי המועצה מידי שבוע עובד נוסף, כמתחייב עפ"י ההסכם, ולשפר את הבקרה השוטפת בנושא.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי בשלב זה מגיע פעם בחודש מנהל רשת או מנהל אבטחת מידע מטעם החברה, והיא תשתדל להגביר את תדירות הגעתם למועצה.

6.4 האחראי מטעם המועצה על מתן הוראות ועריכת פיקוח על השירותים הניתנים על ידי החברה מוגדר בהסכם "מנהל". נמצא כי בפועל המנמ"ר כפוף למנכ"ל המועצה, אולם הדבר אינו מצוין במפורש בהסכם.

**מומלץ לציין בהסכם מיהו הגורם במועצה האחראי על הפעילות של המנמ"ר ועל עריכת פיקוח ובקרה שוטפת על עבודתו.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצה לפיה יצוין בהסכם כי פעילות המנמ"ר תהיה תחת פיקוח ראש המועצה או מנכ"ל המועצה.

6.5 נמצא כי ההסכם אינו מתייחס לחובת החברה לשלוח את עובדיה המעניקים שירות למועצה, לקורסים או השתלמויות מקצועיות כדי להתעדכן בטכנולוגיות חדישות, שינויים רגולטוריים, וכד'.

**מומלץ לכלול בהסכם את חובת החברה לשלוח את עובדיה לקורסים והשתלמויות על מנת להבטיח המשך קבלת שירותים ברמה נאותה לאורך זמן.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי חובת שליחת העובד לקורסים והשתלמויות אמורה לחול על החברה וגם על המועצה.

6.6 נמצא כי החברה אינה מגישה למועצה דוחות מפורטים לגבי כלל פעילויות המנמ"ר כפי שנדרש עפ"י סעיפים 10.11, ו - 24 להסכם:

10.11. הספק יגיש למועצה דו"חות בהתאם לדרישת המועצה - בהם יפרט את חתך הפעולות שבוצעו עבור המועצה, מגוון התקלות, כולל דו"חות מפורטים לגבי מופעי התקלות, אופן הטיפול בהן ולוח זמנים לסיום הטיפול - וזאת בתוך 7 ימים מיום דרישתה של המועצה.

**דו"חות**

24. הספק יגיש למועצה אחת לחודש, ולא יאוחר מהראשון לכל חודש קלנדרי, דו"ח מפורט בגין שירותי התחזוקה והתיקון שניתנו על ידו בפועל למשרדי המועצה בחודש החולף. לדו"ח האמור יצרף הספק חשבון אשר יכלול את הסעיפים כדלקמן:

24.5. הסכום החודשי אשר על המועצה לשלם על פי המפורט בפרק 3 נספח ב' למסמכי המכרז.

24.6. פרוט כל החלקים, האביזרים והתוכנות והמחיר הנדרש בגינם, אשר סופקו על ידו במהלך החודש החולף בצרוף האישורים אשר ניתנו על ידי המנהל לרכישתם ולמחירם (להלן ולהלן: "**החשבוו**").

**מומלץ להקפיד על קבלת דוחות פעילות מהחברה בתדירות שנקבעה בהסכם, ולקבוע בהסכם ובנוהל העבודה את הגורם במועצה שאמור לקבל את הדוחות ולקיים ישיבות תקופתיות עם המנמ"ר לצורך בקרה שוטפת.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצה.

## 7. ממונה על אבטחת מידע

סעיף 17ב' לחוק הגנת הפרטיות קובע כי המועצה מחויבת למנות אדם בעל הכשרה מתאימה לתפקיד הממונה על אבטחת מידע.

בהתאם לכך צוין בהנחיות משרד הפנים, כי "כל גוף ציבורי (לרבות רשויות מקומיות) ימנה ממונה על אבטחת מידע שתפקידו יהיה "ניהול אבטחת המידע ברשות המקומית בהתאם להוראות הדין הקיים ולנהלי הרשות המקומית ומדיניותה".

נמצא כי מנמ"ר המועצה משמש בפועל גם כממונה אבטחת מידע, לאחר שקיבל מינוי רשמי בכתב לתפקיד ע"י ראש המועצה (ראה כתב מינוי **בנספח ב'**).

נמצא כי ההסכם עם החברה אינו מתייחס למתן שירותי אבטחת מידע, כפי הנדרש.

**מומלץ לכלול את נושא אבטחת המידע במסגרת ההסכם, תוך פירוט חובות החברה ומטלות המנמ"ר בתחום חשוב זה, בהתאם להוראות החוק והתקנות המחייבות.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצה.

על פי הגדרת התפקיד במשרד הפנים, ממונה אבטחת מידע אמון על הנושאים הבאים:

- תכנון מדיניות אבטחת המידע ובקרה על יישומה;
- תכנון וביצוע סקרי אבטחת מידע;
- ניהול ההרשאות ודרכי הגישה למשתמשים;
- תכנון ויישום תכנית התאוששות- DRP;
- ניהול ההגנה על מערכות המידע והתקשורת.

במהלך הביקורת נבדק אופן העסקתו של הממונה על אבטחת מידע, בהתאם לתקנות הגנת הפרטיות (אבטחת מידע) שפרסמה הרשות להגנת הפרטיות במשרד המשפטים. להלן ממצאי הבדיקה וההמלצות לתיקון הליקויים:

| הסעיף בתקנות | ההנחיות המחייבות | ממצאי הבדיקה (תקין/לא תקין) והמלצות |
|---|---|---|
| 3(1) | ממונה אבטחה יהיה כפוף למנהל מאגר המידע או למנהל פעיל. | בכתב המינוי שניתן לממונה אבטחת מידע לא צוין שהוא כפוף למנכ"ל המועצה. כמו כן אין התייחסות לנושא הכפיפות בהסכם ההתקשרות שנחתם עם החברה, ואף לא בנהלי העבודה במועצה.<br>**מומלץ שכפיפות הממונה על אבטחת מידע למנכ"ל המועצה תעוגן בכתב המינוי, וכן בהסכם עם החברה ובנהלי העבודה.**<br>מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את המלצת הביקורת, והוא יפעל להוצאת כתב מינוי מתוקן. |
| 3(2) | הכנת נוהל אבטחת מידע והבאתו לאישור בעל המאגר. | נוהל אבטחת מידע טרם אושר על ידי מנכ"ל המועצה.<br>**מומלץ שמנהל אבטחת מידע יגיש בהקדם את נוהל אבטחת המידע לאישור מנכ"ל המועצה.**<br>מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצה. |

| הסעיף בתקנות | ההנחיות המחייבות | ממצאי הבדיקה (תקין/לא תקין) והמלצות |
|---|---|---|
| 3(3) | הכנת תכנית לבקרה שוטפת על העמידה בדרישות תקנות אלה, ביצוע התכנית והודעה לבעל מאגר המידע ולמנהל המאגר על ממצאיו. | לא נמצאה תכנית כתובה לבקרה שוטפת של ממונה אבטחת מידע על עמידה בדרישות שנקבעו בתקנות. כמו כן לא נמצא תיעוד לדיווחים שהועברו למנכ"ל המועצה על ממצאי הבקרה השוטפת בנושא.<br>**מומלץ שמנהל אבטחת מידע יכין תכנית עבודה לביצוע בקרה שוטפת על יישום תקנות הגנת הפרטיות, יפעל לביצוע התכנית, ויעביר דיווחים תקופתיים למנכ"ל על הממצאים שעלו בבקרה.**<br>**מומלץ שהמנכ"ל ינהל מעקב אחר קבלת דיווחים תקופתיים לגבי ממצאי הבקרה שנערכה בנושא.**<br>מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוכנה על ידו תכנית לבקרה בנושא אבטחת מידע, וכי הועברו דיווחים שוטפים בנוגע לאירועי אבטחת מידע למנכ"ל ולראש המועצה באמצעות הודעות מייל. |
| 3(4) | הממונה על אבטחת מידע לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים במילוי תפקידו לפי תקנות הגנת הפרטיות. | מנמ"ר המועצה משמש במקביל גם כממונה על אבטחת מידע. המנמ"ר מטפל בין היתר בעדכונים, הרשאות, ביצוע גיבויים, ועוד - פעולות שלגביהם הוא אמור לערוך פיקוח ובקרה כממונה על אבטחת מידע ולכן עלולות להעמידו בחשש לניגוד עניינים.<br>**מומלץ שעובד נוסף מטעם החברה שעפ"י ההסכם אמור להיות מידי שבוע במועצה, ימונה לתפקיד ממונה על אבטחת מידע במועצה, ולא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים.**<br>מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצה. |
| 3(5) | הטיל בעל מאגר על הממונה על אבטחה המידע משימות נוספות לשם ביצוע תקנות אלה, יגדירן בצורה ברורה. | בהסכם ההתקשרות לא קיימת הגדרה ברורה לעניין אבטחת מידע.<br>**מומלץ להגדיר בהסכם את המשימות של הממונה על אבטחת מידע, כפי הנדרש.**<br>מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצה. |
| 3(6) | בעל מאגר המידע יקצה לממונה את המשאבים הדרושים לו לשם מילוי תפקידו. | בתקציב המועצה לא מוגדרים סעיפים ספציפיים לנושא אבטחת מידע. כמו כן, לא נמצאה תכנית עבודה מקושרת תקציב בנושא.<br>**מומלץ לתקצב את תחום אבטחת המידע בסעיף תקציבי נפרד על מנת להבטיח הקצאת משאבים בהתאם לצרכים, ולאפשר לממונה על אבטחת מידע להכין תכנית עבודה מקושרת תקציב.**<br>מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצה. |

## 8. מדיניות ונהלי עבודה

נוהל הוא מסמך שאושר על ידי בעל תפקיד האחראי לפעילות הנדונה בו, המגדיר עקרונות ותפקידים לביצוע פעילות ומתאר תהליך עבודה, שיטה או מבנה ארגוני. נהלי עבודה הינם כלי חשוב שנועד להבטיח התנהלות מיטבית תוך מתן אפשרות לפיקוח ובקרה להנהלת הרשות המקומית.

נוהל כולל בדרך כלל מבנה אחיד, מספר נוהל, תאריך עדכון ומספר מהדורה על מנת שניתן יהיה לעקוב אחר שינויים המבוצעים בו ומועדם. נוהל תקין אמור לכלול חמישה או שישה פרקים הכוללים בדרך כלל את הנושאים הבאים:

1. מטרה - בפרק זה תוגדר המטרה לשמה נכתב הנוהל.
2. מסמכים ישימים - פירוט מסמכים עליהם נשען הנוהל, כגון תקנים או נהלים.
3. הגדרות - הגדרת מונחים שיש להם משמעות מיוחדת בנוהל.
4. שיטה - פירוט שיטת או תהליך העבודה, כולל האחראים לביצוע הפעילויות, לוחות זמנים, גורמים לדיווח.
5. אחריות - פירוט בעלי התפקידים האחראים לביצוע הוראות הנוהל.
6. נספחים - טפסים המשמשים לקיום הוראות הנוהל.

הביקורת קיבלה 2 נהלי אבטחת מידע שהוכנו על ידי מנמ"ר המועצה:

- נוהל אבטחת מידע - הנוהל כולל בין היתר את הנושאים הבאים: מדיניות הרשאות המשתמשים, ניהול סיסמאות הרשת, ניהול מערך הגיבויים, אופן ניהול סיכוני אבטחת המידע, ועוד.
- נוהל התאוששות מאסון - הנוהל מגדיר את הפעולות הנדרשות לביצוע במקרה של אירוע אבטחת מידע.

נמצא כי הנהלים אינם ערוכים בפורמט של נהלי עבודה כפי שתואר לעיל, לדוגמא: לא צוין בהם מועד עריכת הנוהל, תאריך עדכון אחרון, והם אינם חתומים על ידי המנכ"ל כפי הנדרש. בנוסף, נוהל אבטחת מידע מתאר ממשקי עבודה בין המנמ"ר לבין ממונה אבטחת המידע, כאשר בפועל המדובר באותו גורם. הביקורת גם מציינת כי הנוהל אינו מפרט יישום פעולות בסיסיות של הממונה על אבטחת מידע, כגון: תדירות הדרכות משתמשים, תרגול תכנית התאוששות מאסון, ועוד.

**מומלץ שהמנמ"ר יעדכן את הנהלים הקיימים ויכלול בהם נושאים נוספים כגון אלו שצוינו לעיל.**

**מומלץ לצרף לנהלים נספחים, כגון: טופס דיווח על אירוע אבטחת מידע, התחייבות לשמירת סודיות של העובדים, וכד'.**

**מומלץ שהנהלים יועברו לאישור וחתימת מנכ"ל המועצה, כפי הנדרש.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את המלצות הביקורת, ונושא הנהלים יטופל בהקדם.

הנחיות הרשות הלאומית להגנת הסייבר הן לשנת 2018 והן לשנת 2021 קובעות כי אחת הבקרות הבסיסיות של הארגון בתחום אבטחת המידע הינה קיום "מדיניות ארגונית ואסטרטגיה סדורה בהיבטי הגנת מידע וסייבר". נמצא כי למעט 2 נהלי אבטחת המידע לא קיימת במועצה מדיניות סדורה בכתב המתייחסת לכלל היבטי אבטחת המידע כפי שנדרש בהנחיות. (ראה פירוט רשימת הנושאים **בנספח ד'**).

**מומלץ לקבל מהחברה המלצה על מסמך מדיניות אבטחת מידע עבור כלל מערכות המידע במועצה, אשר יידון מול המנמ"ר ויאושר על ידי הנהלת המועצה.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצה.

### 9. רישום מאגרים ומינוי מנהלי מאגרים

ברשות מקומית קיימים מאגרי מידע רבים בתחומים שונים כגון: גבייה, שכר, תשלומים לספקים, חינוך, שירות פסיכולוגי, גני ילדים, שירותי רווחה, כוח אדם, רישוי עסקים, תחבורה וחנייה, תברואה, ועוד.

עפ"י הוראות חוק הגנת הפרטיות, חובה לרשום את מאגרי המידע בפנקס מאגרי המידע במשרד המשפטים. על הרישום לכלול את זהות בעל מאגר המידע, המחזיק במאגר ומנהל המאגר, ומעניהם בישראל, מטרות הקמת מאגר המידע והמטרות שלהן נועד המידע, וכן את סוגי המידע שייכללו במאגר.

חוק הגנת הפרטיות קובע את ההגדרות הבאות:

- "**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 אפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף;

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

סעיף 8(ג) לחוק הגנת הפרטיות קובע כי "בעל מאגר מידע חייב ברישום בפנקס ועל בעל המאגר לרשמו אם נתקיים בו אחד מאלה:

1. מספר האנשים שמידע עליהם נמצא במאגר עולה על 10,000;
2. יש במאגר מידע רגיש;
3. המאגר כולל מידע על אנשים והמידע לא נמסר על ידיהם, מטעמם או בהסכמתם למאגר זה;
4. המאגר הוא של גוף ציבורי כהגדרתו בסעיף 23;
5. המאגר משמש לשירותי דיוור ישיר כאמור בסעיף 17ג."

הגדרת "**גוף ציבורי**" עפ"י סעיף 23 לחוק הגנת הפרטיות: "משרדי ממשלה ומוסדות מדינה אחרים, רשות מקומית, וגוף אחר הממלא תפקידים ציבוריים על פי דין".

על הרישום לכלול את זהות בעל מאגר המידע, המחזיק במאגר ומנהל המאגר, ומעניהם בישראל, מטרות הקמת מאגר המידע והמטרות שלהן נועד המידע וכן את סוגי המידע שייכללו במאגר.

סעיף 31א(א)(1) לחוק הגנת הפרטיות קובע בין היתר כי ניהול, החזקה או שימוש במאגר מידע החייב ברישום ולא נרשם מהווה עבירה פלילית שדינה מאסר שנה. בנוסף על כך, בגין עבירה זו רשאי רשם מאגרי מידע להטיל קנס מינהלי .

תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו- 1986, מוסיפות את החובה למנות מנהל לכל מאגר.

יחידת ממשל זמין ברשות התקשוב / מערך הדיגיטל הלאומי, הקימה את אתר data.gov.il בכדי להציג מידע ממשלתי אמין ומוסמך לשימוש הציבור הרחב, זאת כחלק ממדיניות ממשל פתוח המקדמת שקיפות מצד משרדי הממשלה.

להלן מאגרי המידע השייכים למועצה שהוצגו באתר האמור במועד הביקורת:

| id | מספר מאגר | מזהה בעל המאגר | שם מלא | שם המאגר | ישוב |
|---|---|---|---|---|---|
| 19739 | 980005175 | 500236500 | מ. מ. אפרתה | בטחון | אפרתה |
| 19740 | 980005182 | 500236500 | מ. מ. אפרתה | הנהלת חשבונות | אפרתה |
| 20987 | 990029520 | 500236500 | מ. מ. אפרתה | מרשם תושבים | אפרתה |
| 20995 | 990029605 | 500236500 | מ. מ. אפרתה | חינוך | אפרתה |
| 21003 | 990029689 | 500236500 | מ. מ. אפרתה | מקרקעין | אפרתה |

נמצא כי מאגרי מידע נוספים של המועצה אינם רשומים במשרד המשפטים, כגון מאגר הפניות למוקד העירוני, תיקי רישוי עסקים, רשימת מטופלי רווחה, ועוד. במועד הביקורת גם לא נמצא תיעוד מסודר לרשימת מנהלי מאגרי המידע במועצה, ולכלל הרישומים שבוצעו במשרד המשפטים.

**מומלץ למפות את כל מאגרי המידע במועצה ואת המידע הנאסף במסגרתם, ולבחון את החובה לרישומם בפנקס מאגרי המידע, בשיתוף עם המנמ"ר והיועץ המשפטי.**

**מומלץ להשלים את רישום כל מאגרי המידע החייבים בכך עפ"י החוק, בהתאם לממצאי הבדיקה האמורה.**

**מומלץ להכין רשימה עדכנית של מנהלי מאגרי המידע במועצה, ולהקפיד על תיעוד מסודר של מסמכי הרישום של כל מאגר.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצה, והנושא אמור להיות מטופל על ידי ממונה אבטחת מידע.

## 10. סקר סיכונים

בסעיף 5 לתקנות הגנת הפרטיות נקבע כלהלן:

"...(ג) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר אחראי לכך שייערך סקר לאיתור סיכוני אבטחת מידע (להלן - סקר סיכונים); בעל מאגר המידע ידון בתוצאות סקר הסיכונים שיועברו לו, יבחן את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ויפעל לתיקון הליקויים שהתגלו במסגרת הסקר, ככל שהתגלו; סקר סיכונים כאמור ייערך <u>אחת לשמונה עשר חודשים לפחות</u>...

(ה) ארגון שהוא בעל כמה מאגרי מידע, רשאי לקבוע את רשימת המצאי כאמור בתקנת משנה (א), במסמך אחד לעניין כל מאגרי המידע שברשותו, המצויים באותה רמת אבטחה וכן רשאי לקיים את החובות הקבועות בתקנות משנה (ג) ו-(ד) בסקר סיכונים או במבדק חדירות, לפי העניין, אחד לעניין כל מאגרי המידע שברשותו, המצויים באותה רמת האבטחה."

בנוהל מספר 3 לנוהלי המסגרת שצוינו לעיל בנושא "סקרי סיכונים - ניהול והערכה" נקבע, כי "במסגרת ניהול הסיכונים מתבצע סקר סיכונים, שמטרתו לאתר את הסיכונים לארגון ולהעריך את חומרתם, זאת על מנת לאפשר קבלת החלטה מבוססת באיזה סיכונים לטפל, ובאיזה סדר עדיפות, עלות ולוח זמנים."

הנוהל ממליץ להעריך סיכונים כשלב מקדים בתהליך עיצוב מדיניות אבטחת מידע, כאשר תוצאות ההערכה יסייעו לקבוע מהן פעולות האבטחה שראוי לנקוט וישמשו כאמצעי לקביעת קדימויות להקצאת המשאבים.

במועד הביקורת לא נמצא תיעוד לעריכת סקרי סיכונים במועצה לבחינת נאותות אבטחת המידע. עוד נמצא, כי נושא סקר הסיכונים אינו נכלל בנוהל אבטחת המידע של המועצה.

**מומלץ להקפיד על עריכת סקר סיכונים אחת לשמונה עשר חודשים לפחות, כנדרש עפ"י התקנות.**

**מומלץ לעגן את סקרי הסיכונים בנוהל אבטחת מידע, ולתקצב את עריכתם בסעיף ייעודי של הוצאות בנושא אבטחת מידע.**

## 11. בדיקות חדירה

מבדקי חדירה (Penetration Test) נועדו לבחון את פוטנציאל הנזק העלול להיגרם לאתרי האינטרנט ולמערכות המידע ברשת הפנימית כתוצאה ממתקפות סייבר. המבדקים מתבצעים דרך "עיניו של הפורץ" לצורך איתור פרצות אבטחה, ובדיקה של מצב אבטחת המידע הקיים בפועל.

סעיף 5(ד) לתקנות הגנת הפרטיות קובע כי "במאגר מידע שחלה עליו רמת האבטחה **הגבוהה**, בעל המאגר אחראי לכך שייערכו מבדקי חדירות למערכות המאגר לבחינת עמידותן בפני סיכונים פנימיים וחיצוניים, **אחת לשמונה עשר חודשים לפחות**; בעל המאגר ידון בתוצאות מבדקי החדירות ויפעל לתיקון הליקויים שהתגלו, ככל שהתגלו."

במועד הביקורת, לא נמצא תיעוד לעריכת מבדקי חדירה למערכות המועצה במהלך השנים 2021 - 2020, בניגוד לתקנות הקובעות כי יש לבצע מבחני חדירה אחת ל - 18 חודשים לפחות. עוד נמצא, כי נושא מבדקי החדירה אינו נכלל בנוהל אבטחת המידע של המועצה.

**מומלץ להקפיד על ביצוע בדיקות חדירה אחת לשמונה עשר חודשים לפחות, כנדרש עפ"י התקנות.**

**מומלץ לעגן את בדיקות החדירה בנוהל אבטחת מידע, ולתקצב את עריכתם בסעיף ייעודי של הוצאות בנושא אבטחת מידע.**

**מומלץ כי הזמנת בדיקות החדירה וסקרי הסיכונים והפיקוח המקצועי על עריכתן יבוצעו על ידי מנמ"ר המועצה, ויתועדו באופן מסודר לצורך מעקב ובקרה.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי מבוצע סקר סיכונים או מבדקי חדירה על ידי החברה מידי חצי שנה, אך הוא מקבל את ההמלצה לעגן את הנושא בנוהל מסודר.

## 12. אבטחה פיזית וסביבתית

בסעיף 6 לתקנות הגנת הפרטיות נקבע כלהלן:

"(א) בעל מאגר מידע יבטיח כי המערכות המפורטות בתקנה 5(א)(1) יישמרו במקום מוגן, המונע חדירה וכניסה אליו בלא הרשאה, והתואם את אופי פעילות המאגר ורגישות המידע בו.

(ב) בעל מאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, ינקוט אמצעים לבקרה ולתיעוד של הכניסה והיציאה מאתרים שבהם מצויות המערכות המפורטות בתקנה 5(א)(1) ושל הכנסה והוצאה של ציוד אל מערכות המאגר ומהן."

כאמור, תקנות הגנת הפרטיות קובעות חובה לאבטחת המקום בו שמורים מאגרי המידע במועצה. בנוסף, בנהלי המסגרת שצוינו לעיל נקבע בין היתר כיצד יש לאבטח את חדרי השרתים. בנוהל מס' 27 לנהלי המסגרת בנושא "סיכוני אש, חשמל ומים בחדר המחשב" נקבע, כי "בחדר המחשב המרכזי יוצבו לפחות 5 מטפי גז הלון, בנקודות שיקבעו על ידי האחראי על הבטיחות...". עוד נקבע בנוהל, כי "מחשבים הניצבים על הרצפה יוצבו על משטח מוגבה יציב בגובה של 10 ס"מ לפחות, וזאת כדי למנוע פגיעת רטיבות ונוזלים".

בתקן ישראלי 1243 של מכון התקנים הישראלי בנושא "בטיחות אש של מחשבים וציוד היקפי" נקבע, כי רצפת חדר המחשב תנוקז גם כשהציוד מוצב במישרין על הרצפה. עוד נקבע בתקן, כי בכניסה לחדר המחשבים תוצב דלת אש תקנית בעלת עמידות אש של 30 דקות לפחות, וכי בחדר לא יאוחסנו חומרים דליקים כגון קרטון.

נמצא כי מערכת מס"ב המשמשת את הגזברות לביצוע העברות כספיות לספקים ולעובדים, ומערכת קומפלוט של אגף הנדסה, ממוקמות בשרת ייעודי שנמצא בחדר המנמ"ר שבבניין המועצה. הביקורת ביקשה לבחון מהן הבקרות הפיסיות הקיימות באותו חדר, שנועדו להבטיח את שרידות מערכות המידע המאחסנות יישומים אלו.

**נמצא תקין** ✓. הביקורת העלתה כי הכניסה לחדר מתאפשרת אך ורק למנמ"ר באמצעות כרטיס מגנטי, ובעת הכניסה לחדר נשלחת אליו הודעת מייל כי בוצעה כניסה לחדר.

להלן טבלה המציגה את אמצעי אבטחת המידע הפיסיים הנדרשים בחדר המחשבים, לעומת אמצעי האבטחה שנמצאו במועד הביקורת:

| תיאור הבקרה הנדרשת | תיאור הסיכון | קיום הבקרה בפועל |
|---|---|---|
| מטפים/ גלאי עשן/ גלאי טמפרטורה | שריפה | ✓ |
| גנרטור | חשמל | ✓ |
| אל – פסק (UPS) | חשמל | ✓ |
| רצפה צפה (*) | הצפה | ✓ |
| קודן כניסה/מנעול (**) | גניבה | ✓ |
| מערכות מיזוג אויר | חום/ שריפה | ✓ |

(*) קיים גלאי למקרה של הצפה.

(**) קיימת בקרה השולחת הודעת מייל עם פתיחת דלת חדר השרתים.

נמצא כי בנוהל אבטחת המידע במועצה אין התייחסות לכל אמצעי האבטחה הפיזיים הנדרשים עפ"י התקן והתקנות.

**מומלץ לעדכן את נוהל אבטחת המידע, ולכלול בו את כל אמצעי האבטחה הפיזיים הנדרשים.**

**מומלץ כי אחת לתקופה הנושא האמור ייבחן שוב ע"י הממונה על אבטחת המידע.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצות.

## 13. ניהול הרשאות הגישה

בסעיף 7 לתקנות הגנת הפרטיות נקבע כלהלן:

"(א) לא ייתן בעל מאגר מידע גישה למידע המצוי במאגר, ולא ישנה היקף הרשאה שניתנה, אלא אם כן נקט אמצעים סבירים, המקובלים בהליכי מיון עובדים ושיבוצם, כדי לברר שאין חשש כי בעל ההרשאה אינו מתאים לקבלת גישה למידע המצוי במאגר; אמצעים כאמור יינקטו בשים לב לרגישות המידע שבמאגר ולהיקף הרשאות הגישה לתפקיד שמיועד לו הנוגע בדבר, כאמור בתקנה 8.

בסעיף 8 לתקנות הגנת הפרטיות נקבע:

"(א) בעל מאגר מידע יקבע הרשאות גישה של בעלי הרשאות למאגר המידע ולמערכות המאגר, בהתאם להגדרות תפקיד; הרשאת הגישה לכל תפקיד תהיה במידה הנדרשת לביצוע התפקיד בלבד.

(ב) בעל מאגר מידע ינהל רישום מעודכן של תפקידים, הרשאות הגישה שניתנו להם, ושל בעלי ההרשאות הממלאים תפקידים אלה (להלן - רשימת ההרשאות התקפות)".

בהתאם לאמור לעיל, על המועצה לקבוע הרשאות גישה למערכות המידע שברשותה בהתאם לבעלי התפקידים, ולנהל רישום מעודכן בנושא. על מנת להשתמש בנתוני המאגר יש לייצור מנגנון אימות משתמשים, המאפשר גישה למערכות הממוחשבות.

הביקורת בחנה את הרשאות המשתמשים המנוהלות במועצה במערכת ניהול הרשת Active Directory , וזאת בהתאם להגדרות התפקיד של העובדים הלכה למעשה.

נמצא כי אך ורק מנמ"ר המועצה מוגדר כמשתמש-על (Administrator) – ✓ **תקין**.

לא נמצאו משתמשים אשר אינם מזוהים באופן חד ערכי (גנריים) – ✓ **תקין**.

לא נמצאו משתמשים שכבר עזבו את המועצה, וזאת עפ"י רשימת העובדים שעזבו את המועצה כפי שנמסרה לביקורת על ידי משאבי אנוש) – ✓ **תקין.**

## 14. הדרכות ותרגולים

נוהל מס' 8 בקובץ נהלי המסגרת לאבטחת מידע שצוין לעיל, קובע מספר כללים בנוגע למודעות, הדרכה, הטמעה והסברה, ובכלל זה:

- המשתמשים יקבלו הדרכה בנושא נהלי אבטחה והשימוש הנכון באפשרות לעיבוד מידע, כדי למזער סיכוני אבטחה אפשריים.
- פעילות ההדרכה תקבל תקציב הולם.
- ההדרכה תכלול דרישות אבטחה, מחויבויות על פי החוק ובקרות, וכן הדרכה לשימוש נכון באפשרות לעיבוד מידע, כגון נהלי כניסה למערכת, שימוש בחבילות תוכנה, ועוד.

- פעם בשנה תתבצענה פעילויות הדרכה בנושא אבטחת מידע לקבוצות עובדים, משתמשי מחשב ו/או לקבוצות להן נגיעה למידע. הפעילות תתבצע באופן קבוצתי בחלוקה לבעלי תפקידים שונים: מנהלים בכירים, עובדי האגפים השונים, מתאמי מחשוב, מנהלי מאגרים וקבוצות עובדים אחרות.
- ההדרכה תאורגן ע"י ממונה על אבטחת המידע, בתיאום עם הממונה על ההדרכה. ימי עיון ייעודיים לעובדים חדשים או שטרם הודרכו, יתואמו עם מחלקת הדרכה.
- אחת לשנה תתבצע פעילות של ריענון להגברת המודעות האבטחתית.

נמצא כי המנמ"ר נוהג לשלוח הודעות מייל למשתמשים, הכוללים עדכונים והנחיות בנושאים שונים. להלן דוגמאות להודעות שנשלחו ע"י המנמ"ר בשנים 2018-2022:

| תאריך | נושא ההודעה |
|---|---|
| 5.3.18 | הזמנה לביקור במטה הנוער לקבלת הסבר על הנעשה בתחום המחשוב במועצה ושיתופי פעולה וממשקים בין המחלקות (כולל הקרנת סרט). |
| 15.5.18 | הזמנת העובדים להירשם ל - 3 השתלמויות שיועברו ע"י המנמ"ר בחודש יולי. (בנושא תוכנת אקסל, POWERPOINT, הכרת המחשב, אינטרנט, טפסים, וטיפים. |
| 22.10.19 | תזכורת - הנחיות לגבי התנהלות ברשת המחשבים במועצה. |
| 8.12.20 | פירוט תוצאות תרגול בנושא אבטחת המידע שבוצע במועצה. |
| 5.4.21 | עדכון לגבי מתקפות סייבר המתרחשות בישראל. |
| 15.3.22 | עדכון על שינויים בתכנת הדואר עקב שדרוג תכנת האופיס. |

יודגש כי בנוסף לדוגמאות שצוינו בטבלה לעיל, נשלחו על ידי המנמ"ר הודעות מייל רבות נוספות במהלך השנים שנבדקו, שהתייחסו לנושאים שונים, כגון אזהרות ממייל חשוד, עוקץ טלפוני, וירוס חדש שמסתובב ברשת, הנחיות כיצד לנהוג ביציאת העובד לחופשה, עדכונים שוטפים בנושאים טכניים, עדכוני תוכנה, ועוד.

בסעיף 10.1 להסכם עם החברה נקבע כי השירות שיסופק למועצה יכלול גם הדרכות:

**שירותי אספקת תחזוקת ותיקון מחשבים**

10.

10.1. הספק מתחייב לספק שירותי התחזוקה ותיקון המחשבים הכוללים, בין היתר, תחזוקת רשתות המחשבים, מחשבים, תיקון תשתיות רשת בסיביות ואספקת ציוד נלווה, ביצוע תיקונים, אחזקה שוטפת, התקנת ציוד ותוכנות, מתן פתרון מידי לבעיות דחופות, מתן הדרכות, אחזקה, תמיכה ופתרון בעיות המתעוררות מעת לעת.

נמצא, כי מלבד שליחת הודעות מייל למשתמשים שכללו הנחיות ועדכונים כאמור, המנמ"ר כמעט ולא ביצע הדרכות לעובדי המועצה כנדרש עפ"י ההסכם, למעט מפגש בחודש מרץ 2018 ויוזמה להעברת הדרכות בחודש יולי 2018, שצוינו בטבלה לעיל.

**מומלץ לפרט בהסכם עם החברה את תדירות ואופן ביצוע ההדרכות לעובדים, ולשפר את הבקרה על ביצוע ההדרכות הלכה למעשה.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצה. עוד ציין המנמ"ר, כי החל מחודש ינואר 2023 הוא מבצע מידי שבוע הדרכות ותרגולים לקבוצות שונות של עובדי המועצה.

נמצא כי בתאריך 7.12.20 ביצע המנמ"ר תרגול לעובדי במועצה בנושא אבטחת מידע, שבמהלכו הוא שלח אליהם מייל מזויף עם לוגו של חברת מיקרוסופט. בהודעה נטען ששולח המייל מכיר את המנמ"ר ומציע להתקין תוסף למייל הכולל בתוכו קישור לטופס. בסיום מילוי הטופס, לחיצה על כפתור "שלח" הפנתה הודעה למשתמש שנכנס וירוס למחשב.

למחרת, בתאריך 8.12.20 שלח המנמ"ר הודעה לעובדים, ועדכן שיום קודם לכן הוא ערך את התרגיל. המנמ"ר ציין כי לצערו הוא מסכם את התרגיל ככישלון, מאחר וכ - 20% בלבד מהעובדים פנו אליו כדי לשאול אם לפתוח את ההודעה, כ - 77% מהעובדים אפילו לא דווחו לו שהם קיבלו מייל בעייתי, וכ - 3% פתחו את המייל לחצו על הקישור ונפלו בפח, וחצי מהם לא הודיעו לו עד עכשיו שהם נפלו קורבן לתוכנת כופר. המנמ"ר חזר והדגיש כי חייבים להבין שמספיק עובד אחד שלא עומד ברמת אבטחת המידע כדי להפיל את כל מערכות המועצה, והביע תקווה שהלקח נלמד ושמקרים כאלו, בתרגיל או חס ושלום במציאות, לא יקרו שוב.

נמצא כי בהודעת המייל שצוינה לעיל, המנמ"ר כלל הנחיות מפורטות כיצד יש לנהוג במקרה של קבלת מייל חשוד, כלהלן: אין לסמוך על מייל עם לוגו, על טענת השולח שהוא מכיר את המנמ"ר, ושהוא מציג עצמו כמנכ"ל חברה גדולה כמו מיקרוסופט. יש לוודא את כתובת המייל של השולח, ולזכור שחברות גדולות לעולם אינן פונות ישירות לעובדים. אין לסמוך על טענה שהמייל נשלח ל"כולם", אין ללחוץ בשום פנים על קישור המופיע במייל, במיוחד במייל שלא מכירים אישית את השולח. בטופס שנפתח אין לתת את המייל של העובד, ויש ליידע מיד את המנמ"ר על כל דבר חשוד.

**לדעת הביקורת, הכללים החשובים שצוינו בהודעת המייל האמורה, אמורים להיות מועברים לעובדים גם במסגרת הדרכות שיועברו מעת לעת ע"י המנמ"ר, על מנת למנוע מצב שבו עובד לא יקרא בתשומת לב ראויה את ההודעה עקב עומס העבודה.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצה.

במועד עריכת הביקורת, לא נמצאה תכנית עבודה שנתית לביצוע הדרכות על ידי המנמ"ר בנושא מערכת המחשוב ואבטחת מידע.

עוד נמצא, כי בנהלי אבטחת המידע במועצה לא קיימת התייחסות לנושא ההדרכות, הן לגבי עובדים חדשים שנקלטו במועצה, והן לגבי הדרכות לעובדים פעילים.

**מומלץ לכלול את נושא ההדרכות במדיניות אבטחת המידע של המועצה, ובמסגרת נהלי אבטחת המידע.**

**מומלץ שהמנמ"ר יכין תכנית עבודה שנתית לביצוע הדרכות בנושא אבטחת מידע על היבטיה השונים, ויגיש אותה לאישור מנכ"ל המועצה.**

**מומלץ להפיץ לכל העובדים והמנהלים את תכנית ההדרכות השנתית לצורך רישום וקביעת מועדי השתתפות, ולערוך מעקב אחר השתתפותם בפועל.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצות.

## 15. גיבוי ושחזור נתוני אבטחה

בסעיף 17 לתקנות הגנת הפרטיות נקבע כלהלן:

"(א) בעל המאגר מידע ישמור את הנתונים הנצברים במסגרת יישום הוראות תקנה 6(ב), 8 עד 11, 14, 15(א)(4) ו-16, ככל שתקנות אלה חלות עליו, באופן מאובטח למשך 24 חודשים.

(ב) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, בעל המאגר יגבה את הנתונים שנשמרו כאמור בתקנת משנה (א), באופן שיבטיח שיהיה ניתן, בכל עת, לשחזר את הנתונים האמורים למצבם המקורי."

בנוסף, בסעיף 18 לתקנות הגנת הפרטיות נקבע כלהלן:

"(א) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יקבע בעל המאגר במסמך -

(1) נהלים לביצוע גיבוי כאמור בתקנה 17(ב), באופן תקופתי שגרתי;

(2) נהלים, להבטחת שחזור הנתונים כאמור בתקנה 17(ב), ובלבד שביצוע השחזור יהיה באישור מנהל המאגר;

(3) כי במסגרת תיעוד אירועי אבטחה כאמור בתקנה 11, יתועדו גם הליכי שחזור המידע, ובכלל זה זהותו של מי שביצע את הליכי השחזור ופרטי המידע ששוחזר.

(ב) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל מאגר אחראי לכך שיישמר עותק הגיבוי של הנתונים האמורים בתקנה (א)(1) ושל הנהלים כאמור בתקנת משנה (א)(2), באופן שיבטיח את שלמות המידע ואת אפשרות השחזור של המידע במקרה של אבדן או הרס."

הביקורת ביקשה לבחון האם המועצה כללה במסגרת התקשרויותיה עם ספקים התייחסות לנושא הגיבויים.

נמצא כי במסגרת ההתקשרות עם החברה המספקת את המערכת לניהול ועדה לתכנון ובנייה, ניתנה התייחסות נרחבת לנושא הגיבויים, והחברה התחייבה לבצע שחזורים על פי רמת שירות מוגדרת (SLA- Service level Agreement), כמוצג להלן:

מועצה מקומית אפרת
**מכרז זוטא מערכת ניהול מידע ועדה לתכנון ובנייה**

| | | | |
|---|---|---|---|
| .13 | שחזור המערכת מגבוי לאחר אסון | התקבלה הודעת שגיאה מידית או מצב בו השחזור לא הסתיים תוך 8 שעות | 12 שעות |
| .14 | הקמת הרשאות למערכות באתר חליפי | התקבלה תודעת שגיאה מידית או השחזור לא הסתיים תוך 8 שעות | 12 שעות |
| .15 | שחזור המערכות באתר חליפי | התקבלה הודעת שגיאה מידית או השחזור לא הסתיים תוך 8 שעות | 12 שעות |
| .16 | כל מערכת | כל השבתה שלא נזכרת לעיל הגורמת לנזק תפקודי ו/או כלכלי ו/או פגיעה במוניטין המועצה | 4 שעות מרגע דיווח על השבתת הרכיב / שרות |

במועד הביקורת המועצה נעזרה במערכת לניהול גיבויים של חברה חיצונית. בבדיקת הנושא עלו הממצאים הבאים:

<u>ביצוע גיבויים בתדירות יומית</u> – נמצא כי מבוצע גיבוי המתוזמן באופן יומי של כלל מאגרי המועצה – ✓ **תקין.**

<u>בחינת תקינות שחזורי המידע</u> – נמצא כי ניתן בקלות לשחזר את נתוני הגיבוי למערכות המועצה – ✓ **תקין**.

<u>שימוש בדיסקים מעבר לגיבוי בענן של החברה החיצונית</u> – נמצא כי בנוסף לגיבוי הממוחשב בענן מבוצע גיבוי באמצעות דיסק נייד אשר נשמר בגזברות בכספת נעולה ומאובטחת. – ✓ **תקין.**

## 16. התקנים ניידים

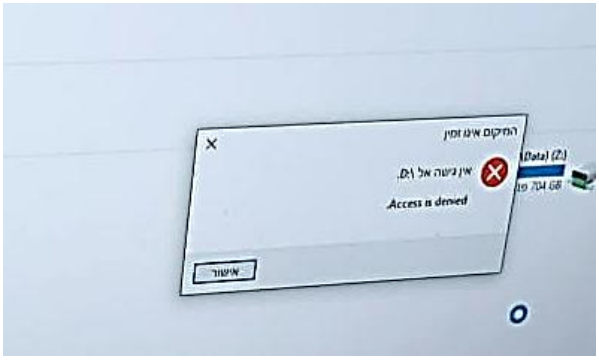
התקן נייד הוא מחשב או התקן אחסון המיועד לשימוש נייד, כמו למשל מחשב נייד, התקן זיכרון נייד, כונן חיצוני וטלפון נייד חכם. מאחר ומדובר בהתקנים ניידים הניתנים להעברה ממקום למקום, השימוש בהם כרוך בסיכון לדליפת מידע.

בסעיף 12 לתקנות הגנת הפרטיות נקבע כלהלן:

"בעל המאגר יגביל או ימנע אפשרות לחיבור התקנים ניידים למערכות המאגר במתכונת ההולמת את רמת אבטחת המידע שחלה על המאגר, את רגישות המידע, את הסיכונים המיוחדים למערכות המאגר או למידע הנובעים מחיבור ההתקן הנייד ואת קיומם של אמצעי הגנה מתאימים מפני סיכונים אלה; בעל מאגר מידע המאפשר שימוש במידע מהמאגר בהתקן נייד או העתקה שלו להתקן נייד ינקוט אמצעי הגנה בשים לב לסיכונים המיוחדים הקשורים לשימוש בהתקן נייד באותו מאגר מידע; לעניין זה יראו שימוש בשיטות הצפנה מקובלות כנקיטת אמצעים סבירים להגנה על מידע שהועתק להתקן הנייד."

נוהל 31 לנהלי המסגרת שצוינו לעיל: "אבטחת מידע במחשבים ניידים, palm pilot, ו-דיסקים נתיקים" מנחה לגבי האופן שבו יש להגן על מידע הנאגר או המעובד במחשבים ניידים, במגמה לצמצם את הסיכון שבגניבת הציוד ו/או חשיפת המידע השמור בו ו/או נגישות לרשת המשרד באמצעות המחשב הנייד.

הביקורת ביצעה בדיקה אקראית במחשב של עובדת גזברות המועצה, שבמהלכה נעשה ניסיון להשתמש בהתקן USB שחובר לתחנת העבודה. הבדיקה העלתה כי אפשרות זו חסומה, כמוצג בצילום המסך להלן:




נמצא כי הגישה להתקנים ניידים נחסמה על ידי מנמ"ר המועצה באמצעות מערכת אבטחת מידע.

בבדיקת הנושא הביקורת לא העלתה ממצאים חריגים – ✓ **תקין**.

## 17. אבטחת תקשורת

בזמן שמערכות המידע מחוברות לרשת האינטרנט, נוצר סיכון של גישה חיצונית ולא מורשית אליהן, כך גם בעת עבודה מרחוק תוך שימוש בהתקנים ניידים.

בסעיף 14 לתקנות הגנת הפרטיות נקבע כלהלן:

"(א) בעל מאגר מידע לא יחבר את מערכות המאגר לרשת האינטרנט או לרשת ציבורית אחרת, בלא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב.

(ב) העברת מידע ממאגר המידע, ברשת ציבורית או באינטרנט, תיעשה תוך שימוש בשיטות הצפנה מקובלות.

(ג) במאגר מידע שניתן לגשת אליו מרחוק באמצעות רשת אינטרנט או רשת ציבורית אחרת, ייעשה שימוש נוסף על אמצעי אבטחה כאמור בתקנות משנה (א) ו-(ב), באמצעים שמטרתם לזהות את המתקשר, והמאמתים את הרשאתו לביצוע הפעילות מרחוק ואת היקפה; לעניין גישה של בעל הרשאה למאגר מידע ברמת האבטחה הבינונית והגבוהה, ייעשה שימוש באמצעי פיזי הנתון לשיטתו הבלעדית של בעל ההרשאה."

בדיקה אקראית שערכה הביקורת באחת מנקודות הרשת במשרדי המועצה העלתה, כי עם חיבור מחשב נייד / אמצעי נתיק לרשת המשתמשים אשר אינו מוגדר על ידי המנמ"ר, נקודת החיבור מתנתקת באמצעות רכיב NAC (Network Access Control) המונע כניסת משתמשים בעלי כוונות זדוניות לרשת – ✓ **נמצא תקין**.

הביקורת בחנה את תוכנת האנטי וירוס אשר בשימוש המועצה של חברת אנטי וירוס והעלתה כי התכנה עדכנית כפי הנדרש.

לסיכום, נמצא כי המועצה נעזרת ברכיב אבטחת מידע חיצוני לשם חציצה בין רשתות האינטרנט והרשת הפנימית. הרכיב מאפשר בין היתר חסימת גישה לתכנים לא מורשים ברשת, ומניעת גישה של גורמים שאינם מורשים למאגרי מידע של המועצה – ✓ **נמצא תקין**.

בנוסף המועצה נעזרת במערכת של חברת אנטי וירוס לחסימת וירוסים. הביקורת העלתה כי המערכת האמורה מתעדכנת באופן שוטף – ✓ **נמצא תקין**.

### 18. קריאת כרטיסי אשראי - תקן EMV

תקן EMV (Europay, MasterCard, Visa) נועד לאבטחה מוגברת ומניעת הונאות בסליקת עסקאות בכרטיסי אשראי. התקן קובע כי עסקאות בנוכחות כרטיס חכם (סליקה בבית העסק) יסלקו רק באמצעות טכנולוגיית EMV, כלומר תוך הכנסת כרטיס האשראי למסופון ייעודי והקשת קוד סודי בן 4 ספרות בעת ביצוע העסקה, או בעסקאות ללא מגע עד 300 ש"ח (נכון למועד הביקורת) - ללא הקלדת הקוד הסודי.

בהתאם להוראות בנק ישראל התקן האמור, המיושם כבר מספר שנים בחו"ל, נכנס לשימוש הדרגתי בישראל.

בבדיקה שנערכה עם עובדת מחלקת הגבייה במועצה, נמצא שתקן זה טרם מיושם. לביקורת נמסר שכאשר תושב מגיע למחלקת הגביה ומעוניין לשלם באשראי, התשלום מתבצע באמצעות הקלדה ידנית של פרטי כרטיס האשראי למערכת, בדומה לביצוע עסקה טלפונית. כתוצאה מכך, התשלומים במחלקה הם ברמת אבטחה נמוכה יותר ובניגוד לתקן EMV.

**מומלץ לפנות לחברה האחראית על מתן שירותי הסליקה במועצה לצורך שדרוג המערכת, ועמידתה בתקנים המקובלים בארץ.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח כי הנושא האמור לא נמצא בתחום אחריותו, אך הוא יפנה לחברת סליקת האשראי על מנת לבצע את ההמלצה.

### 19. היערכות לאסון בתחום מערכות המידע

תכנית המשכיות עסקית (BCP - Business Continuity Plan) הינה תכנית פנימית אשר נועדה להבטיח רציפות תפעולית של התהליכים העסקיים הקריטיים של הארגון בשעת חירום, בפרק זמן מוגדר וברמת שירות מוגדרת. התכנית האמורה מתייחסת לאירועי חירום שונים ומגדירה תכניות פעולה לפונקציות הקריטיות בארגון, לצורך התאוששות באופן מלא או חלקי בהתאם למדיניות הארגון.

אחד מאירועי החירום המרכזיים מפניהם מסייעת תכנית ה-BCP להתגונן, הוא **אירוע סייבר משמעותי**. מרחב הסייבר מוגדר באופן שונה בין מדינה למדינה, אך ניתן לומר באופן כללי כי הוא מורכב משלושה רבדים: חומרה, תוכנה, והגורם האנושי (מפתחים ומשתמשים).

תקן ISO 22301 עוסק בתכנית לניהול המשכיות עסקית. התקן נועד לספק לארגון כלים ודרכי פעולה לשם המשך פעילותו העסקית בזמן אירוע בתחום אבטחת מידע, ומדגיש את מרכיבי תכנית ה - BCP הנדרשים.

התקן מציין כי תכנית התאוששות מאסון צריכה לתמוך במספר היבטים מרכזיים, ובכלל זה:

- תמיכה ביעדים האסטרטגיים שלה;
- צמצום החשיפה המשפטית והפיננסית;
- שיפור יכולתה להישאר אפקטיבית במהלך שיבושים;
- טיפול בפרצות תפעוליות.

כאשר מתייחסים לאירוע סייבר, מתכוונים בדרך כלל לאירוע של השבתת מערכות המידע של הארגון, או לאירוע שבו נגרמה פגיעה לאבטחת המידע של הארגון. הארגון נדרש לפתח בקרות בתחום ההמשכיות העסקית לשם הקטנת הנזק, וכן לצורך יכולת שחזור מהירה של תשתיות הסייבר לרמה נאותה. על הארגון להיערך מבחינת תשתיות חלופיות, כולל זמינות ויתירות, ולבחון מעת לעת את תכנית ההמשכיות העסקית ואף לתרגל אותה. הנושא של גיבויים אפקטיביים, אמינים וזמינים הוא קריטי לתהליך המשכיות עסקית יעיל, ונדרש לתרגל אותו באופן שוטף.

תכנית BCP אמורה להיות מנוהלת על ידי מנהל מערכות המידע, והגורם המקצועי האחראי על הנושא הוא הממונה על אבטחת מידע.

תכנית המשכיות עסקית (BCP) כוללת מספר תכניות, כמתואר בתרשים הבא:

מן התרשים עולה כי חלק מתכנית BCP היא התכנית להתאוששות מאסון (DRP), העוסקת בשרידות מערכות המידע של הארגון בעת אירוע סייבר. בנוסף לתכנית DRP קיימים היבטים נוספים שנדרשים להיכלל בתכנית ה - BCP, כגון: תכנית ניהולית לניהול המשבר, רשימות העובדים הנדרשים לטיפול בכל תרחיש, רשימת ספקים ופרטי הקשר שלהם, מיפוי תהליכי העבודה, כתיבת נהלי משבר (כל האמור במסגרת תכנית CMP).

היבט נוסף מתייחס לכל הגורמים אליהם אמורים לפנות בעת חירום, באילו משאבים נשתמש כדי להקל על מצב החירום, פירוט פעולות נדרשות להפחתת הסכנה, חובות ואחריות כל אחד מהעובדים, ועוד (כל האמור במסגרת תכנית ERP).

לביקורת הועבר נוהל בנושא "התאוששות מאסון" המשמש כתכנית DRP במועצה. בנוהל צוין בין היתר כי "האסטרטגיה שנבחרה היא לאתר התאוששות מלאה במשרדי המועצה". כלומר, במקרה של אירוע אסון העבודה תמשיך להתבצע מהמשרדים בבניין המועצה, ולא יהיה מעבר או שימוש באתר חלופי.

הנוהל האמור מפרט את אופן ההתמודדות של המועצה עם אירועי אסון שונים. להלן פירוט האירועים המתוארים בנוהל ואופן ההתמודדות עימם:

| אסון פוטנציאלי | דירוג השפעה | דירוג הסתברות | תיאור קצר של תוצאות אפשריות ופעולות מתקנות |
|---|---|---|---|
| מבול | 1 | 1 | כל הציוד הקריטי נמצא בקומה שניה במשרדי המועצה |
| אש | 4 | 3 | קיימת מערכת גילוי אש בחדר המחשבים |
| מלחמה | 5 | 2 | קיים מיגון ברמת דלת פלדלת וחדר מוגן ללא חלונות |
| מעשה טרור קיברנטי | 3 | 2 | עדכוני FW שלוש פעמים ביום באופן אוטומטי |
| מעשה חבלה | 3 | 4 | עדכוני FW שלוש פעמים ביום באופן אוטומטי |
| הפסקת חשמל ארוכה | 4 | 3 | כל חדר התקשורת מחובר לגנרטור שמופעל אוטומטית בעת הפסקת חשמל. בנוסף, קיים בחדר אל-פסק שנותן גיבוי חשמלי ל - 3 שעות לפחות. |

הביקורת ערכה בדיקת השוואה בין נוהל המועצה שצוין לעיל, לבין הנחיות רשות הסייבר ונוהל ISO 22301. הבדיקה העלתה שנוהל המועצה אינו מתייחס למספר היבטים בסיסיים, כמפורט להלן:

- הנוהל אינו כולל התייחסות לאסון רעידת אדמה הגורם לקריסת מבנה המועצה כולל חדר השרתים. כמו כן אין התייחסות למקרה של קריסת אחד מספקי שירותי הענן, כגון EPR, קומפלוט, וכד'.
- הנוהל מתייחס למעשה טרור קיברנטי באופן כללי, ואינו מפרט מקרים נוספים כגון מתקפת כופר, או אירוע סייבר הגורם לפגיעה באתר האינטרנט של המועצה.
- הנוהל לא כולל תרחישים מפורטים הכוללים את הגורמים האחראים לכל תרחיש, סדר הפעולות הנדרשות, וכו'. **(ראה נספח ה')**.
- בנוהל לא נמצאה התייחסות למיפוי מלא של תהליכי העבודה במועצה העלולים להיפגע בעת אירוע אסון, כגון: רישום לגני ילדים, תשלומים לספקים, גביית ארנונה, ועוד, ולגבי אופן ההתמודדות עם האירוע לצורך צמצום הנזקים וחזרה לשגרה.
- בנוהל לא צוינו פרטים של עובדי המועצה החיוניים במקרה של אירוע סייבר.

יצוין, כי חלק מהרכיבים שאמורים להיכלל בתכנית ה - BCP עפ"י ההנחיות, כגון מערכות גיבוי ונהלי עבודה, קיימים בנוהל התאוששות מאסון אשר הוצג לביקורת, אולם הנוהל האמור אינו ערוך כתכנית המכילה את כלל המרכיבים כפי שמצוינים בהנחיות רשות הסייבר ותקן ISO 22301.

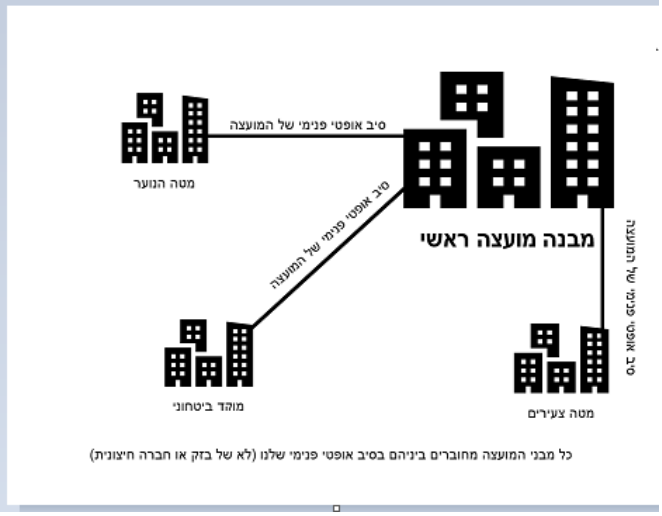
**מומלץ לעדכן את נוהל התאוששות מאסון של המועצה, ולכלול בו את כל ההיבטים שצוינו לעיל.**

**מומלץ שהמועצה תתקצב הכנת תכנית BCP בהתאם לקבלת הצעות מחיר ממספר ספקים המתמחים בהכנת התכנית, עפ"י תכולה שתוכן ע"י ממונה אבטחת המידע.**

מנמ"ר המועצה ציין בתגובתו לטיוטת הדוח, כי הוא מקבל את ההמלצות.

## 20. נספחים

### נספח א' - תרשים רשת




### נספח ב' - מינוי ממונה אבטחת מידע


אפרת
מועצה מקומית
משאבי אנוש ושכר

כי תמוז תשי"ף
12/07/2020

לכבוד
מר

שלום רב,

הנדון: כתב מינוי ממונה אבטחת מידע

בהסגרת חוק הגנת הפרטיות, התשמ"א, ומתוקף תפקידי כראש מועצה מקומית אפרת, הנני ממנה אותך כממונה אבטחת מידע.

תוקף המינוי מידי.

אני מאחל לך הצלחה רבה בתפקיד חשוב זה.

בברכה,
עודד רביבו
ראש המועצה

מועצה מקומית אפרת
ת.ד 1022 מיקוד 9043932
טל: 02-9939312
פקס: 1532-9939382

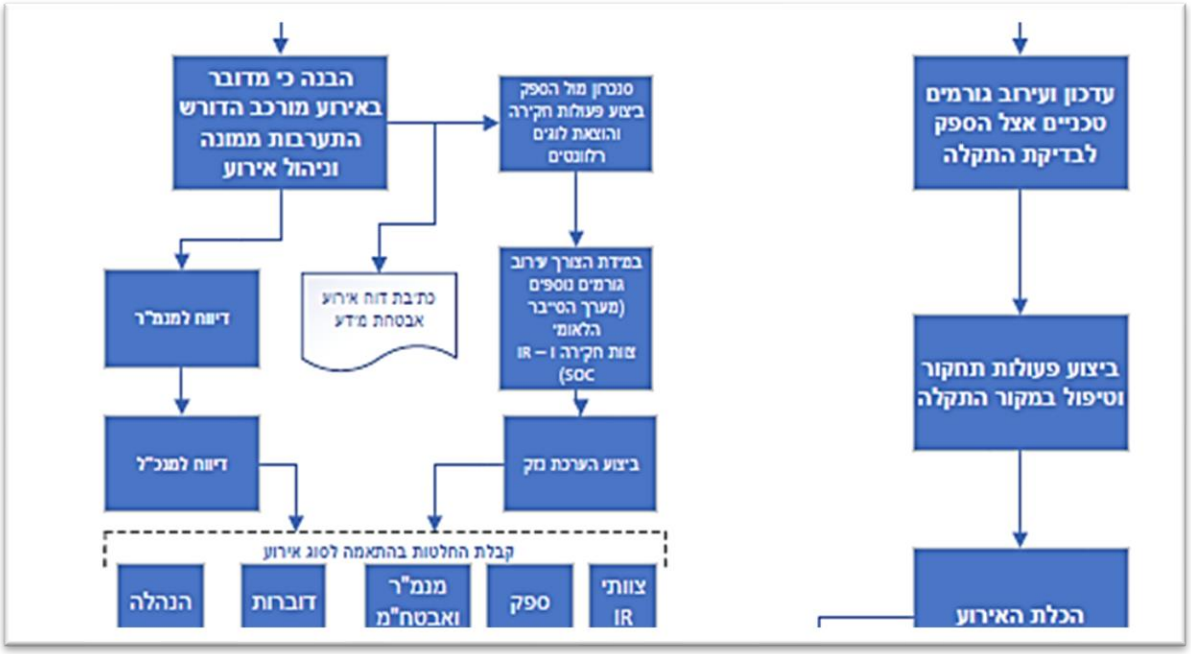
## נספח ג' - מדגם יישומי המועצה

| שם המערכת | מחלקה | מיקום מערכת ענן / מקומי |
|---|---|---|
| 365 | כולם | ענן |
| Ctconnect | כולם | ענן |
| EPR גביה | גביה | ענן |
| EPR גזברות | גזברות ונציג כל מחלקה | ענן |
| EPR חינוך | חינוך | ענן |
| EPR רווחה | רווחה | ענן |
| כל נתון | גביה גזברות | ענן |
| שירת הים | מועצה דתית | ענן |
| תאורה | שפע | ענן |
| משפח"ה | שפ"ח | ענן |
| מס"ב | גזברות | מקומי |
| קומפלוט | הנדסה | מקומי |

## נספח ד' - רשימת נושאים נדרשים לקיום מדיניות עפ"י הנחיות הרשות הלאומית להגנת הסייבר לשנת 2021

| מס' | נושא |
|---|---|
| 1 | אחריות ההנהלה והדירקטוריון |
| 2 | ניהול סיכונים והערכת סיכונים |
| 3 | בקרת גישה |
| 5 | הגנה על המידע |
| 6 | מחשוב ענן ציבורי |
| 7 | הגנה על יעדי ההגנה |
| 8 | ניהול שינויים (Change Management) והעברה לייצור |
| 9 | הגנה על תחנות עבודה ושרתים |
| 10 | פיתוח מאובטח |
| 11 | הגנה פיזית וסביבתית |
| 12 | הגורם האנושי |
| 13 | הגנה על סביבות OT |
| 14 | אבטחת רשת |
| 15 | אבטחת ערוצים |
| 16 | קריפטוגרפיה |
| 17 | הגנת סייבר פרואקטיבית |
| 19 | מערך ניטור מרכזי |
| 20 | ניהול אירועים ודיווח |
| 21 | המשכיות עסקית |

## נספח ה' - דוגמא לתרחיש ייחוס - תכנית BCP



# הבסיס החוקי לעבודת המבקר

בצו מס' 892 בדבר ניהול מועצות מקומיות (יהודה ושומרון) נקבע כלהלן:

**פרק ד'4: מינוי מבקר וסמכויותיו[33]**

**מינוי מבקר המועצה (תוקן בתיקון מס' 178 [34])**

**66כה.** (א) המועצה, בהחלטת רוב חבריה, תמנה מבקר פנימי במשרה מלאה, למועצה (להלן – המבקר), על פי הוראות צו שירות העובדים, כהגדרתו בסעיף 60.

(ב) היה מספר התושבים בתחום המועצה המקומית 10,000 או יותר, רשאי הממונה לאשר שהמבקר יכהן במשרה תלקית שלא תפחת מחצי משרה בתנאי שהשלמת משרתו לא תהיה אלא בעבודת בקורת ברשות מקומית אחרת, בישראל או באזור, ובאישור הממונה.

(ג) היה מספר התושבים בתחום המועצה המקומית פחות מ-10,000 רשאי הממונה לאשר שהמבקר יכהן במשרה תלקית שלא תפחת מרבע משרה ובתנאים האמורים בסעיף-קטן (ב).

**(תיקון מס' 178)**

(ד) השלמת משרה של מבקר יכול שתהיה באחד מאלה:

(1) במועצה שבה הוא מכהן כמבקר – בתפקיד הממונה על תלונות הציבור או הממונה על תלונות העובדים, אם המועצה, לפי המלצת ועדת הבקורת, אישרה זאת, לאחר שמצאה כי אין בתפקיד נוסף זה כדי לפגוע במילוי תפקידו כמבקר;

(2) בעיסוק או בעבודה נוספים מחוץ למועצה – אם אישרו זאת המועצה והממונה, לאחר שמצאו כי התקיימו כל אלה:

(א) אין בעיסוק או בעבודה כדי לפגוע במילוי תפקידו או במעמדו כמבקר;

(ב) אין ולא עלול להיווצר ניגוד עניינים בין העיסוק או העבודה לבין תפקידו כמבקר;

(ג) אין בעיסוק או בעבודה משום התחרות בלתי הוגנת עם מי שאינו עובד המועצה;

(ד) המבקר הצהיר על התמורה שיקבל בעבור העיסוק או העבודה.

**(תיקון מס' 178)**

(ה) בוטל.

**מינוי מבקר (הוסף בתיקון מס' 107)**

**66כו.** (א) לא ימונה אדם למבקר מועצה ולא יכהן כמבקר מועצה אלא אם כן נתקיימו בו כל אלה:

(1) הוא יחיד;

(2) הוא תושב ישראל או האזור;

(3) הוא לא הורשע בעבירה שיש עמה קלון;

(4) הוא בעל תואר אקדמי מאת מוסד להשכלה גבוהה בישראל או באזור או מוסד להשכלה גבוהה בחוץ לארץ שהכיר בו, לעניין זה, מוסד להשכלה גבוהה בישראל או שהוא עורך דין או רואה חשבון;

(5) הוא רכש נסיון במשך שנתיים בעבודת בקורת.

**(הוסף בתיקון מס' 178[35])**

(6) הוא אינו חבר בהנהלה פעילה של מפלגה או בהנהלה פעילה או בגוף דומה אחר של רשימת מועמדים שהתמודדה בבחירות למועצה.

**(הוחלף בתיקון מס' 178[35])**

(ב) לא ימונה ולא יכהן כמבקר מי שכיהן כחבר מועצה, אלא אם כן עברו עשר שנים מתום כהונתו כחבר מועצה באותה מועצה, או שנתיים מתום כהונתו כחבר מועצה במועצה גובלת; לענין סעיף קטן זה, "מועצה" – לרבות מועצה כהגדרתה בסעיף 1 לתקנון המועצות האזוריות (יהודה והשומרון), התשל"ט-1979.

**(הוסף בתיקון מס' 107)**

(ג) מי שיהיה מועמד בבחירות למועצה לא יכהן כמבקר אותה מועצה, למשך כל תקופת כהונתה של המועצה שהיה מועמד לה.

**(הוסף בתיקון מס' 107)**

(ד) על אף האמור בסעיף קטן (א), רשאי הממונה לאשר מינוי למבקר המועצה של אדם אשר לא נתמלא בו –

(1) אחד התנאים המנויים בסעיף קטן (א)(4), אם רכש נסיון במשך עשר שנים בעבודת בקורת בגוף ציבורי כמשמעו בחוק הבקורת הפנימית, התשנ"ב – 1992, כפי תוקפו בישראל;

(2) התנאי שבסעיף קטן (א)(5), אם עבר השתלמות מקצועית שאישר הממונה.

**מועצה שלא מינתה מבקר (תוקן בתיקון מס 178 [36])**

**66כז** (א) ראה הממונה כי המועצה אינה ממנה מבקר, רשאי הוא לדרוש ממנה בהודעה כי תמנה מבקר כאמור בסעיף 66כה תוך הזמן הנקוב בהודעה.

(ב) לא מילאה המועצה אחר ההודעה תוך הזמן האמור, רשאי הממונה למנות מבקר למועצה ולקבוע את שכרו.

**תפקידי המבקר (תוקן בתיקון מס' 178 [49], תיקון מס' 190)**

**66כח.** (א) ואלה תפקידי המבקר:

(1) לבדוק אם פעולות המועצה, לרבות פעולות של ועדת תכנון מיוחדת ורשות רישוי מקומית הפועלת בתחום המועצה המקומית לפי צו בדבר תכנון ערים, כפרים ובנינים (יהודה והשומרון) (מס' 418), התשל"א-1971, ולפי חוק תכנון ערים, כפרים ובנינים, מס' 79 לשנת 1966, או לפי צו בדבר מתן היתרים בשטחים תפוסים לצרכים צבאיים (יהודה והשומרון) (מס' 997), התשמ"ב-1982, או תקיקת משנה מכוחם, לפי הענין, נעשו כדין בידי המוסמך לעשותם תוך שמירה על טוהר המידות ועקרונות היעילות והחסכון;

(2) לבדוק את פעולות עובדי המועצה;

(3) לבדוק אם הוראות הנוהל של המועצה מבטיחות קיום הוראות כל דין ותחיקת בטחון, טוהר המידות ועקרונות היעילות והחסכון;

(4) לבקר את הנהלת החשבונות של המועצה ולבדוק אם דרכי החזקת כספי המועצה והחזקת רכושה ושמירתו מניחות את הדעת;

(5) לבדוק אם תוקנו הליקויים בהנהלת ענייני המועצה שעליהם הצביע המבקר או מי שמכהן כמבקר המדינה בישראל.

(ב) הביקורת לפי סעיף קטן (א) תעשה גם לגבי המועצה הדתית שבתחום המועצה וכן לגבי כל תאגיד, מפעל, מוסד, קרן או גוף אשר המועצה משתתפת בתקציבם השנתי כדי יותר מעשירית לגבי אותה שנת תקציב, או משתתפת במינוי הנהלתם (כל אחד מאלה, להלן - גוף מבוקר).

**(תיקון מס' 190)** (ב1) ממצאי הביקורת לגבי מועצה דתית יועברו גם לרשות המוסמכת כהגדרתה בנספח מספר 12.

(ג) בכפוף להוראות סעיף קטן (א), יקבע המבקר את תכנית עבודתו השנתית, את נושאי הבקורת בתקופה פלונית ואת היקף הבקורת לפי -

(1) שיקול דעתו;

(2) דרישת ראש המועצה לבקר עניין פלוני;

**(תיקון מס' 178)** (3) על פי דרישת ועדת הבקורת, ובלבד שמספר הנושאים לביקורת לא יעלה על שני נושאים לשנת עבודה.

**(הוסף בתיקון מס' 107)** (ד) המבקר יקבע, לפי שיקול דעתו, את הדרכים לביצוע בקורתו.

**(הוסף בתיקון מס' 107)** (ה) המבקר יכין ויגיש לראש המועצה מדי שנה הצעת תקציב שנתית ללשכתו, לרבות הצעת תקן עובדים; המועצה תדון במסגרת דיוניה בהצעת התקציב השנתי, בהצעת התקציב והתקן של לשכת המבקר, כפי שהגיש המבקר.

**המצאת מידע למבקר (הוסף בתיקון מס' 107, תוקן בתיקון מס' 178 [51])**

**66כט.** (א) ראש המועצה וסגניו, חברי המועצה, עובדי המועצה, ראש המועצה הדתית וסגניו, חברי המועצה הדתית, עובדי המועצה הדתית, וחברים ועובדים של כל גוף מבוקר, ימציאו למבקר, על פי דרישתו, כל מסמך שברשותם אשר לדעת המבקר דרוש לצרכי הבקורת ויתנו למבקר כל מידע או הסבר שיבקש בתוך התקופה הקבועה בדרישה ובאופן הקבוע בה.

(ב) למבקר או לעובד שהוא הסמיך לכך תהיה גישה, לצורך ביצוע תפקידו, לכל מאגר מידע רגיל או ממוחשב, לכל בסיס נתונים ולכל תוכנת עיבוד נתונים אוטומטי של המועצה או של גוף מבוקר.

(ג) לגבי מידע החסוי על פי דין או תקיקת בטחון או דין במדינת ישראל, יחולו על המבקר ועל העובדים מטעמו המגבלות הקבועות בדין או בתקיקת הבטחון או בדין במדינת ישראל, לפי הענין, או לפיהם לגבי המורשים לטפל במידע כאמור.

(ד) עובד של המבקר שאינו עובד המועצה יחולו עליו לעניין עבודתו האמורה, כל איסור והגבלה החלים על עובד הציבור שהוא עובד המבקר.

(ה) לצורך ביצוע תפקידו, יוזמן המבקר ויהיה רשאי להיות נוכח בכל ישיבה של מליאת המועצה או של כל ועדה מועדותיה או כל ועדה מועדותיו של גוף מבוקר; בישיבה שאינה סגורה רשאי להיות נוכח גם עובד מעובדיו של המבקר.

**דו"ח על ממצאי הבקורת (הוסף בתיקון מס' 107, תוקן בתיקון מס' 178 [52])**

**66ל.** (א) המבקר יגיש לראש המועצה דו"ח על ממצאי הבקורת שערך; הדו"ח יוגש אחת לשנה, לא יאוחר מ-1 באפריל של השנה שלאחר השנה שלגביה הוגש הדו"ח; בדו"ח יסכם המבקר את פעולותיו, יפרט את הליקויים שמצא וימליץ על תיקון הליקויים ומניעת הישנותם בעתיד; בעת הגשת הדו"ח לפי סעיף קטן זה, ימציא המבקר העתק ממנו לוועדת הבקורת.

(ב) בנוסף לאמור בסעיף קטן (א) רשאי המבקר להגיש לראש המועצה ולוועדת הבקורת דו"ח על ממצאי בקורת שערך בכל עת שייראה לו או כאשר ראש המועצה או ועדת הבקורת דרשו ממנו לעשות כן.

**(תיקון מס' 178)** (ג) בתוך שלושה חודשים מיום קבלת דו"ח המבקר יגיש ראש המועצה לוועדת הבקורת את הערותיו על הדו"ח וימציא לכל חברי המועצה העתק מהדו"ח בצירוף הערותיו.

| | | |
|---|---|---|
| (תיקון מס' 178) | | (ד) ועדת הביקורת תדון בדו"ח המבקר ובהערות ראש המועצה עליו ותגיש למועצה לאישור את סיכומיה והצעותיה תוך חודשיים מיום שנמסרו לה הערות ראש המועצה כאמור בסעיף קטן (ג); לא הגיש ראש המועצה את הערותיו על הדו"ח עד תום התקופה האמורה, תדון הוועדה בדו"ח המבקר ותגיש למועצה לאישור את סיכומיה והצעותיה עד תום תמישה חודשים ממועד המצאתו על ידי המבקר לוועדה; בטרם תשלים הועדה את סיכומיה והצעותיה רשאית היא, אם ראתה צורך בכך, לזמן לדיוניה נושאי משרה של המועצה או של גוף מבוקר כדי לאפשר להם להגיב על הדו"ח. |
| (תקן בתיקון מס' 178) | | (ה) (1) תוך חודשיים מן היום שבו הגישה ועדת הביקורת את סיכומיה והצעותיה תקיים המועצה דיון מיוחד בהם ובדו"ח המבקר ותחליט בדבר אישור הסיכומים או ההצעות כאמור. |
| | | (2) לא הגישה הוועדה את סיכומיה והצעותיה לחברי המועצה עד תום התקופה כאמור בסעיף קטן (ד), או לא המציא ראש המועצה לכל חברי המועצה העתק מהדו"ח בצירוף הערותיו, ימציא המבקר עותק הדו"ח לכל חברי המועצה, והמועצה תדון בדו"ח ובהמלצותיו לא יאוחר משבעה חודשים ממועד הגשתו לראש המועצה. |
| | | (ו) לא יפרסם אדם דו"ח מן האמורים בסעיף זה או את תוכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ואולם רשאים המבקר או ראש המועצה באישור הוועדה, להתיר |
| | | פרסום כאמור; לעניין סעיף קטן זה, "דו"ח" – לרבות חלק מדו"ח ולרבות ממצא בקורת. |
| | | (ז) הוגש דו"ח בקורת למועצה יעביר ראש המועצה העתק ממנו לממונה; אין בהוראות סעיף זה כדי לגרוע מסמכות הממונה לפי סעיף 147. |
| (הוסף בתיקון מס' 178) | | (ח) היה למבקר המועצה יסוד להניח שראש המועצה או היועץ המשפטי של המועצה, הוא צד לעשיית עבירה לפי הוראות סימן ב' לפרק ה' לחוק העונשין, התשל"ז-1977, כפי תוקפו בישראל מעת לעת, יעביר המבקר את הענין במישרין לידיעת מבקר המדינה בישראל. |
| (הוסף בתיקון מס' 178) | | (ט) דו"חות המבקר, חוות דעת או כל מסמך אחר שהוציא או שהכין מבקר המועצה במילוי תפקידו, לא ישמשו ראיה בכל הליך משפטי, אך לא יהיו פסולים בשל כך לשמש ראיה בהליך משמעתי. |
| (הוסף בתיקון מס' 178) | | (י) המפרסם דו"ח כהגדרתו בסעיף קטן (ו), ומפר בכך את סעיף קטן (ו) או תנאי בהיתר שניתן לו לפי הסעיף הקטן האמור, דינו – מאסר שנה. |
| מינוי עובדים ללשכת המבקר (הוסף בתיקון מס' 107) | 66לא. | (א) ראש המועצה ימנה בהסכמת המבקר עובדים ללשכת המבקר בהתאם לתקנים שקבע השר ובכפוף להוראות סעיף 61 לתקנון. |
| | | (ב) דין עובדי לשכת המבקר כדין שאר עובדי המועצה, ואולם הם יקבלו הוראות מקצועיות מהמבקר בלבד. |
| | | (ג) לא יופסק שירותו של עובד לשכת המבקר שלא בהסכמתו של המבקר אלא בכפוף להוראות סעיף 65א(1). |
| תיקון ליקויים (הוסף בתיקון מס' 178 [א]) | 66לב. | (א) ראש המועצה ימנה צוות לתיקון ליקויים, שבראשו יעמוד מזכיר המועצה (להלן בסעיף זה – "הצוות"). |
| | | (ב) העלתה הביקורת של מבקר המדינה בישראל ליקויים בפעולתה של המועצה, ידון הצוות בדרכים לתיקון הליקויים, יקבל החלטות בדבר תיקונם, וידווח על דיוניו ועל החלטותיו לראש המועצה סמוך לאחר קבלת ההחלטות. |
| | | (ג) הצוות רשאי, באישור ראש המועצה, לדחות את תיקונו של ליקוי מסוים. |
| | | (ד) ראש המועצה ידווח למבקר המדינה בישראל על ההחלטות שהתקבלו לפי סעיפים קטנים (ב) ו-(ג), סמוך לאחר קבלתן; ראש המועצה ידווח, בין השאר, על הדרכים לתיקון הליקויים והמועד לתיקונם, וכן על הליקויים שהוחלט לדחות את תיקונם והנימוקים לכך. |
| | | (ה) מבקר המדינה בישראל רשאי, בכל עת, לדרוש דיווחים נוספים, על אלה המנויים בסעיף זה. |
| | | (ו) הצוות ידון בדרכים ובמועדים לתיקון ליקויים שנמצאו בדו"ח שהגיש המבקר ושנדון על ידי המועצה לפי סעיף 66ח(ה)(1) או (2), לפי הענין, ובדרכים למניעת הישנותם של ליקויים בעתיד. |
| | | (ז) הצוות יגיש את המלצותיו לראש המועצה בתוך שלושה חודשים מיום שדו"ח המבקר נדון על ידי המועצה, וידווח לוועדת הביקורת על יישום המלצותיו אחת לשלושה חודשים. |
| | | (ח) ראש המועצה רשאי לדחות את תיקונו של ליקוי מסוים, ובלבד שינמק דחייה זו לפני ועדת הביקורת והמבקר, בכתב, לא יאוחר משלושה חודשים לאחר שהוגשו לו המלצות הצוות. |