

## אבטחת מידע

מחשוב ומערכות מידע



## ביקורת אבטחת מערכות מידע

### 1. כללי

1.1. על-פי תכנית העבודה של מבקרת העירייה נערכה בין חודש אוקטובר 2020 לחודש מרץ 2021 ביקורת באגף מערכות מידע ומחשוב, הכפוף לחטיבת השירות, בנושא "אבטחת מידע".

1.2. נושא אבטחת המידע תפס תאוצה בשנים האחרונות, ובעיקר בשנת 2020 עם פרוץ מגפת הקורונה, וזאת לאור הגידול הרב בהיקף השימושים בכלים טכנולוגיים.

1.3. במסגרת עבודתם השוטפת, משתמשים עובדי האגפים השונים בעיריית בת-ים במידע אישי רב על תושבים, בעלי עסקים, ספקים ועוד, ועל כן חלה על העירייה החובה לעמוד בדרישות חוק הגנת הפרטיות והתקנות שהותקנו מכוחו.

1.4. ברור לכל, כי על-ידי אימוץ טכנולוגיות חדשות וקישוריות מרובה ניתן לעשות שימוש אופטימלי במשאבים, לחסוך בעלויות, ולהעניק שירותים טובים וזמינים יותר לתושבי העיר, עובדי העירייה, והקהל הרחב הזקוק לכך. אך יש לזכור, כי שימוש בטכנולוגיות אלו חושף את העירייה לסיכונים חדשים אשר על הנהלת העיר לתת את דעתה עליהם.

1.5. על-פי "מערך הסייבר הלאומי", בשנה האחרונה זוהו עשרות אלפי תקיפות בישראל ובעולם כולו בתשתיות וגופים ציבוריים ופרטיים.

1.6. ביום 23/05/2021 פרסמה הרשות להגנת הפרטיות כי עיריית הוד-השרון הפרה את חוק הגנת הפרטיות, וזאת בעקבות דליפת מידע אישי של עובדי העירייה ותושבים. הרשות להגנת הפרטיות קבעה קנס מנהלי על העירייה בגין אי-רישום מאגרי מידע.

1.7. בחודש יוני 2021 פרסם "מערך הסייבר הלאומי" את המדריך היישומי להגנת הסייבר בארגונים (הכולל רשויות מקומיות).

### 2. תוכנית הביקורת

2.1. הביקורת בדקה את אופן עמידתה של העירייה בהוראות חוק הגנת הפרטיות (בנוגע לאבטחת המידע) ותקנות "אבטחת מידע" - אשר נכנסו לתוקף בחודש מאי 2018, כולל חובות מנהליות המוטלות על העירייה מתוקף החוק.

2.2. הביקורת התמקדה בבדיקת הנושאים הבאים:

2.2.1. עמידה בהוראות חוק הגנת הפרטיות.

2.2.2. עמידה בתקנות הגנת הפרטיות- אבטחת מידע, לרבות:

- מינוי בעלי תפקידים סטטוטוריים.
- רישום מאגרי מידע.
- בחינת מדיניות, נהלים והוראות עבודה.

- קיום סקר סיכונים בתחום אבטחת מידע.
- ניהול מערכות ממוחשבות : ביצוע גיבויים, הדרכות, מתן הרשאות וכו'.
- ניהול אתרי תקשורת.
- 2.2.3. המבנה הארגוני של האגף ובעלי התפקידים.
- 2.2.4. ניהול התקציב.
- 2.3. במטרה ללמוד על תהליכי העבודה הקיימים מההיבטים התפעוליים והכספיים נפגשה הביקורת עם בעלי התפקידים הבאים :
  - 2.3.1. סגן מנהל האגף מערכות מידע ומחשוב
  - 2.3.2. מנהלת תפעול מחשוב
  - 2.3.3. הממונה על אבטחת המידע
- 2.4. בנוסף, ערכה הביקורת סיור בחדר השרתים ואתרי תקשורת שונים ברחבי העיר.

### 3. סיכום הביקורת

- 3.1. בתום הביקורת, נדונו ממצאיה עם מנכ"לית העירייה, סמנכ"לית שירות, סגן מנהל אגף מערכות מידע ומחשוב, ממונת אבטחת מידע והיועץ החיצוני בתחום אבטחת המידע, לצורך קבלת התייחסותם לממצאי הביקורת.
- 3.2. הביקורת מציינת בחיוב, כי לאורך כול שלבי העבודה זכתה לשיתוף פעולה מלא מכל הגורמים האחראים בתחום זה.
- 3.3. מנכ"לית העירייה מכירה בחשיבות נושא אבטחת המידע, ותפעל ככל שניתן למנוע אירועים חריגים בנושא זה.
- 3.4. עם זאת, יש לקחת בחשבון שהמשאבים הכספיים הנדרשים לשמירה ולאבטחת המידע רבים, ותקציב העירייה מוגבל לאור תוכנית ההבראה בה מצוייה העירייה.
- 3.5. מנכ"לית העירייה הנחתה את סמנכ"לית שירות וסגן מנהל אגף מערכות מידע ומחשוב, להכין תוכנית לשיפור יכולות אבטחת המידע של העירייה בהתאם לממצאי סקר הסיכונים.
- 3.6. מדיניות אבטחת המידע העירונית, כפי שהוגשה על ידי סגן מנהל אגף מערכות מידע ומחשוב למנכ"לית העירייה מאושרת על ידה.
- 3.7. סגן מנהל האגף מערכות מידע ומחשוב, מברך על עריכת דוח ביקורת בנושאים שבאחריות האגף, זו הפעם הראשונה במשך שנים רבות מאד בהן הוא מנהל את האגף, ומקווה שהדבר יוביל להבנת הצרכים בתחום זה.
- 3.8. לדבריו, הנושא מקצועי ומורכב ביותר. רוב עובדי העירייה אינם מודעים למשמעויות הרבות של נושא אבטחת המידע, ולא מכירים אותו ברמה המקצועית. אי לכך, אנו נתקלים לא אחת בבעיות מולם.
- 3.9. סגן מנהל האגף סבור, כי נושא אבטחת המידע, אינו יכול להוות עיסוק צדדי או נוסף על המטלות השוטפות, אלא יש למנות אחראי מקצועי בעל התמחות מיוחדת, שיהיה זמין גם בשעות שלאחר שעות העבודה המוגדרות. קיים קושי אובייקטיבי ליישם את ההנחיות במצבת כוח האדם הקיימת.

- 3.10. היקף התקציב לנושא זה מוגבל ביותר, והעירייה אשר מתמודדת עם תכנית הבראה וחשב מלווה, מתקשה להגדילו באופן משמעותי ותואם לצרכים.
- 3.11. למרות כל זאת, מסכם סגן מנהל האגף, אנו מנסים לפעול ככל יכולתנו ולפי הבנתנו. בנוסף, משבר הקורונה גרם לכך שחלק מהתהליכים המתוכננים בתחום ההדרכות נעצרו.

#### 4. היבט חוקי

- 4.1. להלן החוקים והתקנות המרכזיים המהווים את המסגרת המשפטית אשר על בסיסה מושתת נושא אבטחת מידע, עליהם התבססה הביקורת:
- 4.2. פקודת העיריות [נוסח חדש].
- 4.3. חוק הגנת הפרטיות, התשמ"א-1981.
- 4.4. תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017.
- 4.5. תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), תשמ"ו-1986.

#### ממצאי הביקורת העיקריים:

#### 5. כללי

- 5.1. באופן כללי התרשמה הביקורת, כי באגף מערכות מידע ומחשוב מועסקים בעלי תפקידים מקצועיים ומסורים אשר מטפלים מערכות ממוחשבות רבות ומורכבות ומשמרים אותן.
- 5.2. עבודת צוות העובדים באגף המחשוב מתבצעת ברובם המוחלט של הנושאים שנבדקו באופן תקין.
- 5.3. עם זאת, במהלך עבודת הביקורת נמצאו מספר ליקויים הנוגעים בעיקר להיעדר כוח אדם מקצועי בנושא אבטחת מידע, וכתוצאה מכך גם היעדרן של בקורות מספקות. דוגמאות לכך, בהמשך הדוח.
- 5.4. עניין זה מהותי ביותר, משום שמשמעותם של הליקויים בנושאים שנבדקו, עלולים לגרום לנזקים כספיים כבדים לעירייה, לחשיפה לתביעות של תושבים ואחרים, לנזקים תפעוליים, כגון: פגיעה ברציפות תפקודית ושיבוש מידע וכן נזקים תדמיתיים.
- 5.5. הביקורת ממליצה ככל שניתן, על אימוץ תורת ההגנה של "מערך הסייבר הלאומי" אשר פורסם ביוני 2021.
- 5.6. הביקורת מציינת לחיוב, כי במהלך הביקורת תוקנו מספר ליקויים. פירוט בהמשך הדוח.

## 6. תקציב

6.1. סקירת תקציבי האגף (ללא תשלומי שכר) לשנת 2018 ואילך מעלה את הנתונים הבאים:

סוג תקציב	מספר סעיפי תקציב	סכום כולל (אש"ח)
רגיל	9	5,359
תב"ר	9	8,317
סה"כ	18	13,676

6.2. בחינת סעיפי התקציב מעלה, כי בכל שנה קיימת עלייה בסך תקציב אגף מערכות מידע ומחשוב.

6.3. ניצול התקציב הרגיל בשנת 2018 ו-2020 עמד על 103% ו-99.9% בהתאמה.

6.4. ניצול התקציב הרגיל בשנת 2019 עמד על 87% בלבד.

6.5. ניצול תב"ר מספר 4173 בשנת 2018 הסתכם ב- 8% בלבד. התקציב יועד לפיתוח האתר העירוני (להרחבה ראה פרק א' סעיף 4). לדברי סגן מנהל אגף מערכות מידע ומיחשוב, מדובר בתב"ר שיועד לביצוע קול קורא "אמצעים דיגיטליים" לשנים 2018-2020 שביצעו הסתיים. סגן מנהל האגף יפעל מול החברה המועסקת ע"י העירייה להשלים את הדיווח למשרד הממשלתי הרלוונטי, על מנת לעדכן את ההוצאה בתב"ר, ולקבל את התקציב.

## 7. מבנה ארגוני

7.1. אגף מערכות מידע ומחשוב כפוף לחטיבת השירות המנוהלת על-ידי סמנכ"לית שירות.

7.2. בעלי התפקידים באגף הינם: סגן מנהל האגף מערכות מידע ומחשוב (תפקיד מנהל האגף אינו מאוייש) (להלן: "סגן מנהל האגף"), סגנית מנהל מחלקת מערכות מידע ומחשוב (בתחום מערכת הגבייה והחינוך), סגנית מנהל מחלקת מערכות מידע ומחשוב (בתחום המערכת הפיננסית), תומך בתהליכי תפעול שוטף, ממונת אבטחת מידע ואחראית על תפעול פרויקטים, ממונה מחשוב מוסדות חינוך, סגנית מנהל מחלקת בתחום התפעול מחשוב (להלן: "מנהלת תפעול מחשוב"), טכנאי תמיכה ושירות ומזכירת האגף וכן סטודנט המועסק במשימות שונות.

7.3. בעלי תפקידים נוספים באגף מערכות מידע ומחשוב:

7.3.1. העירייה התקשרה עם ספקים אשר מספקים שירותים במיקור חוץ לעירייה כגון טכנאי מחשבים, ושירותים שונים לתוכנות המשמשות את העירייה.

7.3.2. העירייה התקשרה עם יועץ אבטחת מידע חיצוני (להלן: "היועץ"). (להרחבה ראה פרק א' סעיף 2).

## **8. תוכנית עבודה שנתית**

8.1. סקירת תוכנית העבודה השנתית של אגף המחשוב ומערכות המידע לשנת 2021 מעלה, כי קיימות משימות בתחום אבטחת המידע לרבות רכישת מערכות ממוחשבות וביצוע הדרכות לעובדי העירייה (להרחבה ראה פרק א' סעיף 5).

## **9. מדיניות**

9.1. לעירייה קיימת מדיניות אבטחת המידע המתועדת כנדרש (להרחבה ראה פרק א' סעיף 6).

## **10. נהלים והוראות עבודה**

10.1. בדיקה בפורטל העירוני העלתה, כי ישנם נהלים אשר לא עודכנו זמן רב. לביקורת הועברו 9 הוראות עבודה חדשות אשר נכתבו בהתאם לתקנות אבטחת המידע (להרחבה ראה פרק א' סעיף 7).

## **11. מסמך הגדרות המאגר**

11.1. הביקורת מצאה, כי מסמכי הגדרות המאגר מתועדים בהתאם לתקנות.  
11.2. עם-זאת נמצא, כי זהות מנהלי מאגרי המידע אינה מעודכנת. לדברי סגן מנהל אגף מערכות מידע ומיחשוב, בחודשים האחרונים היו חילופי תפקידים רבים של מנהלים האמורים לשמש כמנהלי מאגרי מידע. הוגשה בקשה לרשם המאגר לעדכון הפרטים, אולם טרם התקבלה התייחסות כלשהי.

## **12. מינוי ממונה אבטחת מידע**

12.1. העירייה מינתה ממונת אבטחת מידע אשר מינוי זה הינו נוסף על תפקידה בתפעול פרויקטים, והיא כפופה לסגן מנהל אגף מערכות מידע ומחשוב.  
12.2. כפיפותה של ממונת אבטחת המידע למנהל זה יוצרת מצב של ניגוד עניינים לכאורה בשל התלות שלה במנהל והיעדר עצמאותה. שכן, ממונת אבטחת מידע אמורה לערוך בקרה אחר פעילות סגן מנהל האגף ותפקודו בנושא אבטחת המידע. זהו מצב שרצוי להימנע ממנו.  
12.3. ממונת אבטחת מידע זו אינה בעלת ההכשרה והניסיון הטכני הנדרשים על-פי דרישות החוק (להרחבה ראה פרק ג' סעיף 2).  
12.4. על-כן סבורה הביקורת, כי הממונה אינה יכולה לבצע את המטלות הנדרשות בתפקיד זה.  
12.5. לאור הנאמר לעיל, הביקורת ממליצה:  
12.5.1. יש להכפיף את ממונת אבטחת המידע למנהל בכיר אחר.  
12.5.2. יש לפעול להכשרת ממונת אבטחת מידע.  
12.5.3. לחילופין, יש למנות ממונה אבטחת מידע אחר, כולל בדרך של מיקור חוץ.  
12.6. מנכ"לית העירייה הורתה, כי הכפיפות הארגונית של הממונה לאבטחת מידע, בנושא זה תהיה לסמנכ"לית שירות. כמו כן, ממונת אבטחת מידע תעבור הכשרה מקצועית בתחום זה.

### **13. ביצוע סקר סיכונים ומיפוי המאגר**

- 13.1. סקר סיכונים בוצע בעירייה בשנת 2020 על-ידי יועץ חיצוני. הביקורת העלתה, כי ישנם ליקויים אשר טרם תוקנו.
- 13.2. התקיימו מבחני חדירות כנדרש בתקנות.
- 13.3. לעירייה "תיק אתר" אשר ממפה את שרתי העירייה.
- 13.4. לא קיים תרשים רשת עירונית בה פועלים מאגרי המידע (להרחבה ראה פרק ג' סעיף 3).

### **14. אבטחה פיזית וסביבתית**

- 14.1. בחינת הוראות העבודה מעלה, כי קיימת התייחסות בהוראות העבודה לאבטחת מערכות המחשב בנושאי בטיחות חשמל, אש ומים, מניעת כניסת אדם ללא הרשאה, וקיום אמצעים לבקרה ותיעוד גישה לאתרי המחשב.
- 14.2. נמצא, כי לרע"ן מקלטים וכיבוי אש קיימת תוכנית לבדיקות שגרתיות למערכות ההגנה הפיזית.
- 14.3. לא קיימת מערכת לתיעוד כניסת אנשים לחדרי השרתים (להרחבה ראה פרק ג' סעיף 4).

### **15. אבטחת מידע - ניהול כח-אדם**

#### **גיוס עובדים**

- 15.1. הביקורת העלתה, כי על-פי שיטות העבודה הנהוגות בחטיבת הון-אנושי:
  - 15.1.1. מועמדים לגיוס מתבקשים למלא טופס שאלון אישי אשר בו קיימת הצהרת היעדר הרשאה פלילית.
  - 15.1.2. בנוסף, על עובד חדש למלא טופס "הצהרה והתחייבות להימנע ממסירת מידע ממאגר מידע" (להלן: "הצהרת שמירת סודיות").
  - 15.1.3. לעובד ניתן דף הנחיות "אבטחת מידע והגנת הפרטיות- דף הנחיות לעובד".
- 15.2. מבדיקה מול חטיבת הון אנושי עולה, כי טפסי השאלון האישי וכן הצהרת שמירת סודיות נשמרים בתיק האישי של העובד וכן באגף מערכות מידע.

#### **סיום העסקת עובד**

- 15.3. הביקורת מצאה, כי ברשת העירייה קיימים חשבונות משתמשים פעילים לעובדים/אחרים אשר סיימו את תפקידם בעירייה. לדברי סגן מנהל אגף מערכות מידע ומחשוב, המידע על משתמשים ברשת העירונית שיש להסירם אינו מגיע מחטיבת הון אנושי לאגף באופן מסודר.
- 15.4. יש לציין, כי בעקבות הערת הביקורת הוסרו חשבונות משתמשים אשר סיימו את תפקידם בעירייה. יש לוודא קבלת המידע באופן שוטף ורציף על מנת למנוע מצבים כגון אלו בעתיד.



### **שינוי תפקיד**

15.5. הביקורת מצאה, כי לעירייה אין אפשרות להפיק דוח המרכז את כלל העובדים אשר שינו את תפקידם. כך שלא מתקיימת בקרה שוטפת על-ידי הממונה לאבטחת מידע. עם זאת בבדיקה מדגמית של עובד באגף הפיקוח אשר שינה תפקיד לאגף אחר בעירייה בשנת 2020 עולה, כי הפרופיל הישן נסגר, וכי לא ניתן לעשות בו שימוש.

15.6. לדברי סגן מנהל אגף מערכות מידע ומחשוב, הנושא מצוי באחריות המנהל הישיר וחטיבת הון-אנושי, אשר אמורים לבצע את המעקב מול אחראית תפעול מיחשוב, בידיעת הממונה על אבטחת המידע. אגף מערכות מידע ומחשוב מטפלים בסוגיה זו במסגרת ניהול הרשאות משתמשים.

15.7. לדברי ממונת אבטחת מידע, קיים תכנון עתידי להעברת דוח משתמשים למנהלי המחלקות אשר ידרשו לבדוק אותן, ולאשרו. בהתאם לכך, יבוצע עדכון משתמשים במערכת העירונית.

### **הדרכות בעלי הרשאות**

15.8. הביקורת מצאה, כי עד כה לא התקיימו הדרכות ייעודיות לבעלי התפקידים במאגרי המידע, לרבות מנהלים ומשתמשים. מגיפת הקורונה בעטייה, נעדרו עובדים רבים מעבודתם לתקופות ארוכות, והעירייה נדרשה למשימות מורכבות ודחופות השונות מהמשימות בשגרה, עיכבו את יישום ההדרכות.

15.9. יש לציין, כי במועד מיפוי מאגרי המידע בעירייה בשנת 2019 הועברו הנחיות למנהלי המאגרים.

15.10. סקירת תוכנית העבודה לשנת 2021 העלתה, כי עתידה להתקיים הדרכה למנהלי מאגרי המידע, וכן לבעלי הרשאות ביחידות המשתמשות במידע אישי רגיש.

### **העלאת מודעות עובדים**

15.11. לצורך העלאת מודעות עובדים והדרכתם, משתמש סגן מנהל אגף מערכות מידע ומחשוב בתפוצה לכלל המשתמשים, בהודעות דוא"ל בעלות מידע על סיכוני אבטחה, והדרך שבה על העובד לנהוג באם נתקל במצב דומה.

15.12. בנוסף, העביר סגן מנהל האגף הודעות דוא"ל אשר מכילה קישור ללומדה מקוונת בנושא אבטחת מידע שפותחה על-ידי מערך הסייבר הלאומי.

15.13. על פי תוכנית העבודה השנתית לשנת 2021, יחל שימוש בלומדה חיצונית אשר תועבר לכלל העובדים בנושאי אבטחת מידע.

15.14. ואכן, לאחרונה, הועברה לומדה באמצעות חטיבת הון אנושי לכלל עובדי העירייה, בה נכלל גם נושא הדרכה בתחום אבטחת המידע. העובדים נבחנו על תוכן המידע. הדבר נותן אינדקציה מסויימת לגבי העברת המידע וקבלתו על ידי העובד.

15.15. בחינת הלומדה מעלה, כי כלל העובדים מחוייבים להשלים את כלל התכנים המופיעים בה, לרבות אבטחת מידע, עד לתאריך מוגדר.

15.16. הביקורת סבורה, כי השימוש בהודעות הדוא"ל אינו מבטיח, כי כולם קוראים אותן או/ו מבינים את המשמעות שלהן (להרחבה ראה פרק ג' סעיף 5). אי לכך,

הביקורת סבורה, כי ניתן להעביר את המידע גם באמצעים נוספים. יש להיערך לכך בשלבי תכנית העבודה כולל הקצאת תקציב.

#### **16. ניהול הרשאות גישה**

16.1. על-פי התקנות, יש לקבוע הרשאות גישה למאגר לכל עובד, רק במידה הנדרשת לו לצורך ביצוע תפקידו.

16.2. בנוסף, יש לנהל "רשימת הרשאות תקפות" מעודכנת של בעלי התפקידים, וההרשאות שניתנו להם. לא נמצאה רשימה כאמור (להרחבה ראה פרק ג' סעיף 6).

16.3. באמצעות רשימה זו והשוואתה לבעלי התפקידים וההרשאות שיש להם בפועל (AD), ניתן יהיה לבדוק אם קיימים משתמשים להם ישנה הרשאה, אולם הם לא מופעים ברשימת ההרשאות התקפות.

#### **17. זיהוי ואימות**

17.1. על-פי התקנות, יש לוודא:

17.1.1. כי הגישה למאגר נעשית על-ידי בעל הרשאה מתאימה על-פי "רשימת

ההרשאות התקפות".

17.1.2. גישה מרחוק למאגרים (עבודה מהבית) ייעשה על בסיס אמצעי פיזי (אימות דו-שלבי).

17.2. לביקורת לא הועברו אסמכתאות לבקרה שבוצעה, כי הגישה למאגר נעשית על-ידי בעל הרשאה מתאימה כאמור בתקנות. בקרה כאמור הינה בחינת רשומות משתמשים אשר ניגשו למערכות הממוחשבות של העירייה, והופעתם ברשימה המאושרת על ידי המנהלים.

17.3. הביקורת העלתה, כי חיבור עובדים לעבודה מרחוק, אינו מתבצע בשיטת אימות דו-שלבי אשר מפחית את סיכון ההתחברות מרחוק על-ידי מי שאינו בעל הרשאה.

17.4. שיטת האימות הדו-שלבי הינה שליחת הודעה עם סיסמה חד פעמית לטלפון האישי של העובד, לצורך התחברות למערכות העירייה.

17.5. בחינת עמידות הסיסמה הנהוגה בעירייה העלתה, כי היא עומדת בדרישות שיטות העבודה הנהוגות בתחום (להרחבה ראה פרק ג' סעיף 7).

#### **18. בקרה ותיעוד גישה**

18.1. על-פי התקנות, יש לנהל "מנגנון בקרה אוטומטי" שיאפשר בקרה על הגישה למערכות המאגר.

18.2. הביקורת לא מצאה אסמכתאות לקיום בקרה אחר הגישה למערכות כנדרש בתקנות (להרחבה ראה פרק ג' סעיף 8). יש לציין, כי בחלק מהמערכות קיים רישום אוטומטי, אולם הרישום אינו נבדק.

#### **19. תיעוד אירועי אבטחה**

19.1. על-פי התקנות, בעל מאגר המידע אחראי לתיעוד כל מקרה שבו התגלה אירוע המעלה חשש לקיום אירוע אבטחה (פגיעה בשלמות המידע או שימוש במידע ללא הרשאה). ככל-האפשר יבוסס התיעוד האמור על רישום אוטומטי.

19.2. עוד קובעות התקנות, כי יש לדווח לרשם מאגרי מידע באופן מיידי על אירוע אבטחה חמור ועל הצעדים שננקטו.

19.3. על-פי הוראת העבודה "תגובה לאירועי סייבר", ממונה אבטחת מידע, יכין דוח ובו יוצגו הרכיבים הבאים: מועדי תחילת האירוע וסיומו, גורמים מעורבים, מערכות מחשוב מעורבות, אופן זיהוי, פעולות שננקטו, מחוללי האירוע, נזקים, ובדיקות לאחר אירוע (להרחבה ראה פרק ג' סעיף 9).

19.4. לדברי הממונה לאבטחת מידע, לא היו אירועי אבטחה אשר מצריכים תיעוד או דיווח לרשם כאמור בתקנות.

## **20. התקנים ניידים**

20.1. על-פי התקנות, בעל המאגר יגביל או ימנע אפשרות לחיבור התקנים ניידים למערכות המאגר במתכונת ההולמת את רמת אבטחת המידע שחלה על המאגר.

20.2. במהלך הביקורת נחסמה האפשרות לשימוש בהתקנים ניידים באתרי העירייה. שימוש בהתקן נייד מצריך פנייה לממונת אבטחת מידע ובחינה פרטנית של כל פנייה.

## **21. ניהול מאובטח ומעודכן של מערכות המאגר**

21.1. על-פי התקנות, בעל מאגר מידע יקפיד על ניהול ותפעול תקין של מערכות המאגר לרבות עדכונים שוטפים של תוכנה וחומרה, וכן לא יעשה שימוש במערכות שהיצרן לא תומך בהיבטי אבטחה.

21.2. הביקורת העלתה, כי עדכוני תוכנה לשרתי העירייה מותקנים אחת לחודש. עדכונים דחופים מותקנים מיידי. לדברי סגן מנהל האגף המערכות מידע ומחשוב, עדכוני גרסה המועברים על-ידי הספקים, לעיתים יוצרים בעיות לא צפויות אשר עלולות לגרום ליותר נזק מתועלת. סגן מנהל האגף מערכות מידע ומחשוב מנהל בקרה רבעונית אחר עדכונים לעמדות-קצה ושרתים (להרחבה ראה פרק ג' סעיף 11).

## **22. אבטחת תקשורת**

22.1. על-פי התקנות, בעל מאגר מידע לא יחבר את מערכות המאגר לרשת האינטרנט ללא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית.

22.2. הביקורת העלתה, כי "החברה לאוטומציה" מספקת לעירייה מעטפת הגנה על בסיס תקן ISO 27001.

22.3. סגן מנהל האגף מבצע בקרה אחר "החברה לאוטומציה", ובוחן את עמידת החברה בדרישות התקנות.

22.4. הביקורת העלתה קיום שרת FW (פיירוול) אשר מדיניותו מנוהלת על-ידי מנהלת תפעול מחשוב יחד עם "החברה לאוטומציה".

22.5. הביקורת מציינת, כי לא קיימת בקרה אחר מדיניות ה-FW (להרחבה ראה פרק ג' סעיף 12).

22.6. נציין, כי בחינת מדיניות ה-FW תתבצע שנת 2021.

### **23. העברות מידע**

23.1. על-פי התקנות:

23.1.1. העברת מידע ממאגר המידע באינטרנט, תיעשה תוך שימוש בשיטות הצפנה מקובלות.

23.1.2. ייעשה שימוש באמצעים שמטרתם לזהות את המתקשר והמאמתים את הרשאתו לביצוע הפעילות, באמצעות אמצעי פיזי הנתון לשיטתו הבלעדית של בעל ההרשאה.

23.1.3. הביקורת העלתה, כי החיבור מרחוק למערכות העירייה נעשה ללא אמצעי פיזי, כמתבקש מהתקנות.

23.1.4. הביקורת ממליצה, להשתמש באימות דו-שלבי אשר עונה על דרישות הרגולציה. המלצה זו נמצאת בתהליך לקראת סיום.

### **24. העברת מידע בין גופים ציבוריים**

24.1. על-פי התקנות, קיימת החובה למנות וועדה לבחינת העברת מידע בין גופים ציבוריים. העירייה מינתה ועדה כנדרש. חברי הוועדה הינם מנכ"לית, יועמ"ש, עובדי ניהול מידע ואבטחתו.

24.2. מעיון בפרוטוקולי הוועדה אשר הועברו לביקורת עולה, כי בשנת 2020 התקיימו שתי פגישות (ביום 09/12/2020 וכן ביום 21/07/2020) של הוועדה. בפגישה נכחו חברי הוועדה בהתאם לתקנות.

### **25. מיקור חוץ**

25.1. על-פי התקנות, בעת התקשרות עם ספק יש לתת את הדעת בהסכם ההתקשרות לסיכוני אבטחת מידע.

25.2. בבדיקת מדגמית שנערכה נמצא, כי הסכמי עבר שנחתמו, לא עומדים כלל בדרישות התקנות.

25.3. בבדיקה מול סגן מנהל האגף מערכות מידע עולה, כי להסכמים חדשים המגיעים לסגן מנהל האגף מערכות מידע ומחשוב, מצורף נספח "אבטחת מידע ושמירת סודיות" אשר מחייב את הספק לעמידה בדרישות התקנות (להרחבה ראה פרק ג' סעיף 13).

### **26. ביקורת תקופתית**

26.1. על-פי התקנות, בעל המאגר אחראי לכך שתיערך ביקורת, אחת לשנתיים, כדי לוודא את עמידתו בהוראות תקנות אלה.

26.2. הביקורת העלתה, כי בשנת 2020 בוצע "סקר סיכונים תהליכי" על-ידי יועץ חיצוני.

26.3. התקיימו מספר דיונים בממצאי הסקר באגף מערכות מידע ומחשוב, ונקטו פעולות הנגזרות מממצאי הסקר, וכן פעולות מעקב על ממצאי הסקר, אולם הנושא לא נידון בהנהלת העירייה (להרחבה ראה פרק ג' סעיף 14).

**27. גיבוי ושחזור נתוני אבטחה**

27.1. הביקורת העלתה, כי נוהל האבטחה הארגוני לא עוסק בפירוט בתחומי גיבוי ושיחזור מידע כנדרש מהתקנות. תחומים אלו מופיעים בנהלים אחרים של האגף אשר לא עודכנו זמן רב.

27.2. עד היום לא נערך תרגול שחזור מידע. אולם, מתבצע שחזור מידע אופרטיבי לפי הצורך (להרחבה ראה פרק ג' סעיפים 15-16).

## **הביקורת ממליצה :**

- א. לוודא, כי ממונת אבטחת מידע תהיה כפופה למנהל בכיר בעירייה ולא למנמ"ר כפי שקיים היום. יש לוודא, כי יהיו לה הידע המקצועי והנסיון הנדרשים על פי התקנות, ותיאור תפקידים של משרד הפנים. בסיכום הביקורת, הורתה מנכ"לית העירייה להכפיף את ממונת אבטחת המידע ישירות לסמנכ"לית שירות.
- ב. לפעול להכשרת ממונת אבטחת המידע של העירייה, על מנת שהיא תרכוש את הידע המקצועי בתחום זה, ותוכל לפעול בהתאם. מנכ"לית העירייה הנחתה לוודא, כי ממונת האבטחה תרכוש ידע מקצועי זה.
- ג. להכין תוכנית לשיפור יכולות אבטחת המידע של העירייה, בהתאם לממצאי סקר הסיכונים. לאור העובדה, כי העירייה נמצאת בתוכנית הבראה ומונה לה חשב מלווה, יש לשקול את האפשרויות בהתאם ליכולתה הכלכלית.
- ד. לפעול מול החברה המועסקת ע"י העירייה להשלים את הדיווח למשרד הממשלתי הרלוונטי, על מנת לעדכן את ההוצאה בתב"ר מספר 4173, ולקבל את התקציב.
- ה. לערוך תוכנית עבודה שנתית בנושא אבטחת המידע, המפרטת משימות בעלת יעדים מדידים, לוחות זמנים וגורמים אחראים. על תוכנית העבודה להיות מותאמת לתקציב האגף.
- ו. לערוך את הוראות העבודה הישנות בנושאי אבטחת המידע, לעדכן או לבטלן בהתאם לצורך. יש לוודא, כי ינתן ביטוי גם לנושא גיבויים ושחזורים.
- ז. יש לכתוב נוהל בנושא "התאוששות מאסון" – בהקשר למערכות הממוחשבות.
- ח. לפעול לאישורם הסופי של הוראות העבודה החדשות על-ידי מנכ"לית העירייה, ולהכלילם בפורטל העירוני, ככל שתוכנם אינו חסוי. במקביל, יש להטמיען בקרב העובדים הרלוונטיים.
- ט. לעדכן את מסמך הגדרות המאגר בהתאם לזהות המנהלים בפועל.
- י. לוודא, כי כלל התוכנות (כולל "ספרת") ינוהלו מול אגף מערכות מידע ומיחשוב.
- יא. להמשיך וליישם את המלצות סקר הסיכונים, מוקדם ככל האפשר.
- יב. לבחון את הצורך בהצפנת תיק האתר, וככל שקיים הצורך, להצפינו.
- יג. לתעד בכתב כניסה ופעילות בחדרי השרתים על-ידי בעלי התפקידים, על מנת לוודא, כי יהיו אלו מורשים בלבד.
- יד. לוודא העברת דוחות אוטומטיים חודשיים מאגף משאבי אנוש לממונת אבטחת מידע לצורך בחינת עדכון חשבונות המשתמשים במקרים של גיוס עובדים, סיום העסקתם, ושינוי תפקיד.
- טו. לדרוש מהמנהלים לעדכן את אגף מחשוב ומערכות מידע בכל המקרים בהם משתמש שאינו עובד עירייה (כגון: ספקים ונותני שירות) אשר סיימו עבודתם בעירייה, על מנת שיוסרו חשבונות המשתמשים.

- טז. לעדכן בהתאם להוראת מנכ"לית העירייה את הנוהל העוסק בגיוס עובדים וסיום העסקתם, כך שחשבונותיהם יסגרו והמידע המקצועי והרלוונטי ישאר לשימושם של בעלי התפקידים הרלוונטיים.
- יז. לשלוח הודעות בנושא אבטחת מידע למשתמשים מתיבת דואר ייעודית ("סייבר"). המלצה זו יושמה בעת תהליך הביקורת.
- יח. לוודא ככל האפשר באמצעות המנהלים, כי העובדים נחשפו לתכנים אלו, וזאת על-מנת להעלות את מודעות העובדים לנושא.
- יט. לנהל באמצעות המנהלים, רשימת הרשאות תקפות בכל המערכות הממוחשבות בעירייה על-מנת לעמוד בדרישות התקנות. בנוסף, לדרוש באמצעות ממונת אבטחת מידע אחת לשנה ממנהלי המאגרים רשימת הרשאות תקפות, ולבחון אותה אל מול רשימת המורשים במערכות הממוחשבות השונות.
- כ. לערוך בקרה אחת לתקופה, אחר הגישה למאגרי המידע על מנת לוודא, כי כל מי שנכנס הוא מורשה. יש לתעד בקרה.
- כא. לעדכן בהוראת העבודה את ההנחייה, כי ככל שמתקיים "אירוע אבטחה חמור", יש לדווח לרשם, לציין את מועד הדיווח ומי אחראי לדווח.
- כב. לערוך בקרה שנתית אחר מדיניות ה-FW, על-מנת לוודא גישה לרשת העירייה על-ידי מורשים בלבד.
- כג. להשתמש באימות דו-שלבי בהתחברות מרחוק למערכות העירייה. שיטת זיהוי זו משתמשת באמצעים הנמצאים בידי העובד (כגון הודעת SMS עם סיסמה) לטלפון הנייד של העובד לצורך אימות רצונו להתחבר למערכת מרחוק. המלצה זו יושמה כבר בתהליך הביקורת. עם זאת, יש לציין כי עדיין חסרים פרטים של טלפונים סלולריים פרטיים של בעלי תפקידים אשר יש להשלימם.
- כד. לבצע תרגיל שחזור יזום.

## פרק א' – אגף מערכות מידע ומחשוב

### 1. כללי

1.1. אגף מערכות מידע ומחשוב מספק שירות לכלל יחידות העירייה וגופי הסמך, כגון: בית המשפט לעניינים מקומיים, ספרייה עירונית, ועוד. השירות כולל רכישה, אחזקה, והדרכה של חומרה ותוכנה, הפקת דוחות מורכבים, כולל קשרי עבודה עם ספק התוכנה.

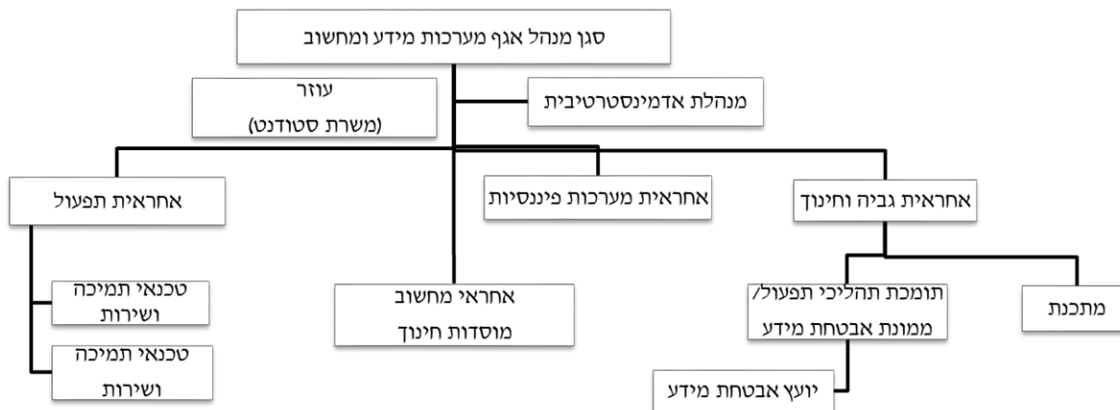
1.2. לאגף תקציב המיועד לתפעול שוטף, שיפור יכולות והגנות, ורכש לחטיבות השונות.

### 2. מבנה ארגוני

2.1. אגף מערכות מידע ומחשוב כפוף לחטיבת השירות המנוהלת על-ידי סמנכ"לית שירות.

2.2. האגף כולל 11 אנשי צוות: עובדי עירייה ועובדים חיצוניים.

להלן המבנה הארגוני של אגף מחשוב:



2.3. תומכת תהליכי תפעול משמשת בנוסף לתפקידה זה, גם בתפקיד ממונת אבטחת מידע.

2.4. השוואת המבנה הארגוני לזו של עירייה בסדר גודל של עיריית בת ים מעלה, כי בעירייה זו קיימת מחלקת אבטחת מידע המונה מנהל ועובד.

### 2.5. בעלי תפקידים - סמכויות ואחריות

2.5.1. סקירת המבנה הארגוני של אגף מחשוב מעלה את בעלי התפקידים הבאים:

א. סגן מנהל האגף מערכות מידע ומחשוב- אחריות על תחום מערכות מידע ומחשוב, לרבות רכש חומרה ותוכנה.

ב. סגנית מנהל מחלקת מערכות מידע ומחשוב - אחריות על תפעול שוטף של מערכת הגביה והחינוך וניהול הקשרים מול מטרופולינט ומול גופים חיצוניים נוספים בתחום זה.



- ג. סגנית מנהל מחלקת מערכות מידע ומחשוב - אחראית על תפעול שוטף של המערכת הפיננסית וניהול הקשרים מול מטרופולינט ומול גופים חיצוניים נוספים.
- ד. תומך בתהליכי תפעול שוטף - מערכת הגבייה והחינוך וניהול הקשרים מול מטרופולינט ומול גופים חיצוניים נוספים בתחום זה.
- ה. ממונת אבטחת מידע ואחראי על תפעול פרויקטים - בנוסף על תפקידה כממונה על אבטחת המידע, אחראית על ניהול קשרי עבודה עם גורמים חיצוניים מבחינת תפעולית ומבחינה כספית וכן תמיכה בתהליכי תפעול שוטף של מערכת הגבייה.
- ו. ממונה מחשוב מוסדות חינוך- אחראי על ניהול הקשרים והפעילויות מול מוסדות החינוך אשר נמצאים באחריות העירייה.
- ז. מנהלת תפעול מחשוב- אחראית על תפעול רשת העירייה.
- ח. טכנאי תמיכה ושירות- מספקים תמיכה טכנית לעובדי העירייה.
- ט. מזכירת סגן מנהל האגף – אחראית על מתן מענה אדמניסטרטיבי לסגן מנהל האגף.
- י. עוזר- משרת סטודנט המסייע לסגן מנהל האגף.

### 3. שירותי ייעוץ אבטחת מידע

- 3.1. העירייה התקשרה עם יועץ אבטחת מידע חיצוני- מ. שפר (להלן: "היועץ").
- 3.2. בשנת 2018 נחתם הסכם מסגרת עם חברת "שפר אבטחת ענ"א ומערכות מידע".
- 3.3. על פי ההסכם על היועץ לספק: "שירותי ייעוץ ליישום חוק הגנת הפרטיות".
- 3.4. תוקף ההסכם עד ליום 31/12/2020. לעירייה זכות להאריך את תוקף ההסכם בשנה אחת בכל פעם, אך כלל ההתקשרות לא תעלה על 5 שנים.
- 3.5. סקירת הזמנת עבודה 20201051 מעלה, כי שירותי היועץ הוגדרו כ: "שירותי ממונה אבטחת מידע".
- 3.6. סוכם כי היקף פעילות היועץ תהיה 8 שעות שבועיות בלבד, כלומר יום בשבוע. היקף הפעילות נקבע בהתאם לתקציב שהוקצה לצורך כך.
- 3.7. על-פי ממונת אבטחת מידע של העירייה, היקף שעות זה אינו מספק, ויש להגדיל את היקף שעות פעילות היועץ על-מנת לעמוד בהיקף המשימות.
- 3.8. פעילות היועץ כללה ייעוץ טכנולוגי מקיף. הערה: בסעיף זה הושמטו פרטים חסויים.

**4. תקציב האגף**

**תקציב רגיל**

4.1. סקירת סעיפי התקציב (ללא תב"ר) של אגף המחשוב (1769100) לשנים 2018-2020 מעלה את הנתונים הבאים:

2020 (אש"ח)			2019 (אש"ח)			2018 (אש"ח)			תאור	סעיף
%	ביצוע	תקציב	%	ביצוע	תקציב	%	ביצוע	תקציב		
97	191	197	105	209	200	95	200	210	הדפסת שוברים	470
<b>99.9</b>	<b>1,097</b>	<b>1,100</b>	<b>100</b>	<b>270</b>	<b>270</b>	<b>104</b>	<b>662</b>	<b>635</b>	<b>עיבוד נתונים</b>	<b>571</b>
<b>99.9</b>	<b>2,251</b>	<b>2,253</b>	<b>73</b>	<b>1,665</b>	<b>2,290</b>	<b>106</b>	<b>1,339</b>	<b>1,260</b>	<b>שירותי חישובי</b>	<b>572</b>
100	98	98	101	101	100	88	132	150	חומרים למחשוב	740
99.9	48	49	114	57	50	98	49	50	ציוד קהילה	741
<b>100</b>	<b>1,820</b>	<b>1,820</b>	<b>101</b>	<b>1,873</b>	<b>1,850</b>	<b>101</b>	<b>1,267</b>	<b>1,250</b>	<b>תחזוקת ציוד</b>	<b>751</b>
---	---	---	---	---	---	---	2	---	מדיה דיגיטלית	752
100	39	39	56	14	25	82	49	60	הוצאות שונות	780
				---	---		---	---	הדרכה	781
<b>99.9</b>	<b>5,353</b>	<b>5,359</b>	<b>87</b>	<b>3,980</b>	<b>4,585</b>	<b>103</b>	<b>3,498</b>	<b>3,405</b>	<b>סה"כ</b>	

4.2. מהטבלה עולה, כי:

4.2.1. בכל שנה קיימת עלייה משמעותית בסך הכול תקציב אגף המחשוב. העלייה בשנת 2019 הסתכמה בשיעור של 35% ביחס לשנת 2018, ואילו בשנת 2020 חלה עלייה של 17%.

4.2.2. כפי שניתן להתרשם, ניצול התקציב בשנת 2018 ו-2020 עמד על 103%-ו-99.9% בהתאמה, ואילו ניצול התקציב בשנת 2019 עמד על 87% בלבד.

4.2.3. אחוז הניצול הנמוך יחסית (73%) בסעיף תקציבי 572 - שירותי חישובי, נבע מהעובדה כי הפעילות של מטרופולינט החלה רק בחודש נובמבר שנה זו.

4.2.4. חלק מסעיפי התקציב עברו בשנים מסוימות לניצול באמצעות תב"ר משום שמדובר בתהליכי פיתוח. לדוגמא בסעיף עיבוד נתונים בשנים 2018 ו-2019 הוקצה תקציב נמוך יחסית.

4.3. הביקורת בחנה את סעיפי התקציב העיקריים הבאים: עיבוד נתונים (571), שירותי חישובי (572), וכן תחזוקת ציוד (751) המסתכמים יחד בשנת 2020 בכ-5.1 מליוני שקלים.

4.3.1. בחינת סעיף התקציב **עיבוד נתונים (571)** מעלה, כי ההוצאות הגבוהות הינן עבור:

א. שירותי טכנאי מחשבים הנאמד ב-264 אלפי ₪.

## אבטחת מערכות מידע

ב. פיתוח תוכנת גביה וחינוך הנאמד ב-162 אלפי ₪.  
 ג. שרותי ממונה אבטחת מידע הנאמד ב-96 אלפי ₪.  
 ד. איש תמיכה לליווי מערכת הגבייה הנאמד ב-86 אלפי ₪.  
 4.3.2. בחינת סעיף התקציב **שירותי מחשוב חיצוני** (572) מעלה, כי ההוצאות הגבוהות הינן עבור:

א. הרשאת שימוש בתוכנת גביה הנאמד ב-630 אלפי ₪.  
 ב. שרותי מחשוב ע"ב הסכם הנאמד ב-273 אלפי ₪.  
 ג. דמי שימוש במערכת שכר ומשאבי אנוש הנאמד ב-317 אלפי ₪.  
 ד. פיתוח תוכנת גבייה וחינוך הנאמדים ב-163 אלפי ₪ (נמצא גם בסעיף תקציבי 751).

ה. איש תמיכה ללווי מערכות פיננסיות הנאמד ב-146 אלפי ₪.  
 4.3.3. בחינת סעיף התקציב תחזוקת ציוד (751) מעלה, כי ההוצאות הגבוהות הינן עבור:

א. רישוי תוכנת מייקרוסופט הנאמדת במיליון ₪.  
 ב. תמיכה בחוות השרתים הנאמדת ב-77 אלפי ₪.  
 ג. תחזוקת מחשבים במשרדי העירייה הנאמדת ב-64 אלפי ₪ (נמצא גם בסעיף תקציבי 751).

## תב"רים

4.4. בחינת תב"ר פעילים בין השנים 2018-2020 באגף מחשוב מעלה:

<u>אחוז ביצוע</u>	<u>סכום</u>	<u>תאריך התחלה</u>	<u>תאור</u>	<u>#</u>
<u>%</u>	<u>(אש"ח)</u>			
29%	200	05/02/2020	מערכות מידע ומחשוב	4250
25%	1,000	05/06/2019	משרד הפנים פיתוח מערכות מידע	4219
94%	1,040	01/01/2018	פ 2018 החלפת מרכזיות טלפונים	4182
100%	1,250	01/01/2018	פ 2018 פיתוח מערכות מידע	4175
8%	299	01/01/2018	הקמה שדרוג רשת דיגיטל	4173
68%	250	01/01/2017	שדרוג מערכת CRM	4149
99%	1,300	01/01/2017	פ 2017 פיתוח מערכות מידע	4138
99%	1,200	01/01/2016	פ 2016 פיתוח מערכות מידע	4095
100%	578	01/01/2016	פיס 2016 מחשבים בת"ס	4084
100%	1,200	01/01/2015	פ 2015 פיתוח מערכות מידע	4044
84%	8,339	<b>סה"כ</b>		

4.5. מנתוני מהטבלה עולה, כי:

4.5.1. סכום תקציב התב"רים בין השנים 2016-2019 עומד על 8.3 מליון ₪.

4.5.2. בתב"ר מספר 4173 משנת 2018 נוצל סכום של 8% בלבד מכלל התקציב (סעיף 2041732750). בחינת התב"ר מעלה, כי התקציב מיועד לפיתוח ושדרוג האתר העירוני.

4.5.3. לדברי סגן מנהל אגף מערכות מידע ומיחשוב, מדובר בתב"ר שיועד לביצוע קול קורא "אמצעים דיגיטליים" לשנים 2018-2020 שביצעו הסתיים. סגן מנהל האגף יפעל מול החברה המועסקת ע"י העירייה להשלים את הדיווח למשרד הממשלתי הרלוונטי, על מנת לעדכן את ההוצאה בתב"ר, לקבל את התקציב.

4.5.4. התקציב שהיה מיועד להיות מנוצל באמצעות תב"ר נוצל מהתקציב הרגיל. הביקורת ממליצה להקפיד על ביצועם של תקציבים מהמקורות להם יועדו מלכתחילה. כמו כן, לבחון את ניצול מלוא התקציבים.

## **5. תוכנית עבודה שנתית**

5.1. תוכניות העבודה לשנים 2020 הועברה לעיון הביקורת בחודש ינואר 2021.

5.2. לביקורת לא הועברו תוכניות עבודה משנים קודמות.

5.3. סקירת תוכנית העבודה מעלה, כי אכן מתקיימות ומתוכננות משימות אשר נוגעות לתחום אבטחת המידע בעירייה לרבות רכישת מערכות וביצוע תרגול לעובדי העירייה.

5.4. עם זאת נמצא, כי:

5.4.1. תוכנית העבודה אינה מכילה לוחות זמנים.

5.4.2. תוכנית העבודה אינה מכילה יעדי ביצוע.

5.5. סגן מנהל האגף מערכות מידע ומחשוב מסר לביקורת, כי מאחר ותוכנית העבודה של האגף תלויה בגורמים רבים שאינם בשליטת האגף, אין זה ריאלי לקבוע תוכניות עבודה בעלות לוחות זמנים. בנוסף, היעדר תקציב אינו מאפשר תכנון מוקדם להחלפת ושדרוג מיכון מיושן.

5.6. הביקורת ממליצה שתוכנית העבודה השנתית תגובה בתקציב אשר הנהלת העיר תחליט להקצות לאגף המחשוב לשדרוג המיכון.

## **6. מדיניות**

6.1. הביקורת בחנה את מדיניות אבטחת המידע של העירייה.

6.2. לביקורת הועברו מסמכי מדיניות אבטחת המידע של העירייה, אשר נערכו בחודש יולי 2020, ומכילים את הנושאים הבאים, כמפורט:

6.2.1. "מדיניות הגנת הפרטיות" - יעדים, סמכויות, אופן סיווג מאגרים, בקרות.

6.2.2. "מדיניות אבטחת מידע בעירייה" – יעדים, סמכויות, נהלים, סיווגים, יישום.

6.3. מסמכי המדיניות הוכנו על-ידי סגן מנהל אגף מערכות מידע ומחשוב ואושרו על-ידי מנכ"לית העירייה.

**7. נהלים והוראות עבודה**

- 7.1. סעיף 4 (א) לתקנות קובע, כי בעל מאגר המידע יקבע במסמך "נוהל אבטחת מידע" אשר יחייב כל בעל הרשאה.
- 7.2. סעיף 4 (ב) קובע, כי בעל מאגר מידע ישמור את נהל האבטחה כך שפרטים ממנו יימסרו לבעלי הרשאה רק בהיקף הנדרש לצורך ביצוע תפקידיהם.
- 7.3. סקירת הפורטל העירוני העלתה את הוראות עבודה הבאות בתחום מחשוב ומערכות המידע (להלן: "הוראות העבודה הישנות") :

שם הנוהל	תאריך עדכון
"ניהול מערכות מידע ומחשוב"	01/06/2010
"בקשת מידע ממאגר נתונים עירוני"	07/05/2009
"תחזוקת מערכות מידע בעירייה"	01/04/2021
"רכישת חומרה, תוכנה וציוד היקפי, פיתוח ושדרוג תוכנה"	01/04/2021

- 7.4. מהטבלה עולה, כי הנהלים "ניהול מערכות מידע ומחשוב" ו- "בקשת מידע ממאגר נתונים עירוני", לא עודכנו כבר מעל ל-10 שנים.
- 7.5. הביקורת ממליצה לבחון את הוראות העבודה הישנות, לעדכןם או לבטלם בהתאם לצורך.
- 7.6. על-פי סגן מנהל האגף מערכות מידע ומחשוב הוראות העבודה אכן עודכנו לאורך השנים אך ללא ציון מועד העדכון.
- 7.7. במהלך הביקורת הועברו 9 הוראות עבודה אשר אושרו באגף המחשוב, כמפורט (להלן: "הוראות עבודה חדשות") :

שם ההוראה	מתאריך
נוהל אבטחה ארגוני למאגרי מידע	01/01/2021
נוהל אבטחה פיסית וסביבתית	
נוהל בקורות גישה	
נוהל הגנת הפרטיות	
נוהל העברת מידע לגורמים חיצוניים	
נוהל התחברות ספק לצרכי תמיכה ותחזוקה	
נוהל שימוש בהתקנים ניידים	
נוהל תגובה לאירועי סייבר	
ניהול משתמשים והרשאות	

7.8. הביקורת סבורה, כי יש לפעול לאישורם הסופי של הוראות העבודה החדשות על-ידי מנכ"לית העירייה ולהכלילם בפורטל העירוני- ככל שתוכנם אינו חסוי. כמו כן, לפעול להטמעתן בקרב העובדים הרלוונטיים.

## פרק ב' - מערכות המידע בעירייה

### 1. כללי

- 1.1. סעיף 7 לחוק הגנת הפרטיות (התשמ"א, 1981), (להלן: "החוק") מגדיר:
- 1.1.1. **מאגר מידע**: "אוסף נתוני מידע המוחזק באמצעי מגנטי או אופטי המיועד לעיבוד ממוחשב..."
- 1.1.2. **אבטחת מידע**: "הגנה על שלמות המידע, או הגנה מפני חשיפה, שימוש או העתקה, והכל ללא רשות או דין".
- 1.2. סעיף 17 לחוק זה קובע, כי על בעל מאגרי המידע, המחזיק או המנהל חלה האחריות על אבטחת המידע שבמאגר.
- 1.2.1. **מנהל המאגר**: "מנהל פעיל של גוף שבבעלותו או אחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לעניין זה".
- 1.3. תקנות הגנת הפרטיות אשר נכנסו לתוקף בחודש מאי 2018 מחייבות את בעל המאגר, המנהל והמחזיק במאגר בביצוע שורה של הנחיות אשר מקנות רמה סבירה של ביטחון, כי מערך המחשוב הארגוני בתחום אבטחת המידע מנוהל באופן נאות.
- 1.4. התקנות מגדירות 3 רמות מאגרי מידע:
- 1.4.1. רמת אבטחה נמוכה.
- 1.4.2. רמת אבטחה בינונית.
- 1.4.3. רמת אבטחה גבוהה.
- 1.5. על-פי נוהל האבטחה הארגוני מאגרי המידע ברשות העירייה מוגדרים ברמת האבטחה הבינונית.
- 1.6. לביקורת הועברה רשימת מאגרי מידע אשר מופו בעירייה על-ידי הממונה לאבטחת מידע, וכן הסטטוס שלהם בשנים 2018 ו-2020, כמפורט בנספח א'.
- 1.7. ניתוח סטטוס רישום מאגרי המידע מעלה:

<u>יחס מכלל המאגרים</u>	<u>מספר מאגרים</u>	<u>סטטוס טיפול</u>
15%	4	נרשם
17%	5	נדרש עדכון מנהל ומחזיק המאגר
52%	15	בטיפול לרישום
8%	2	העברת בעלות
4%	1	ביטול רישום
4%	1	בבחינה נוספת
<b>100%</b>	<b>28</b>	<b>סה"כ</b>

1.8. מהטבלה עולה כי :

1.8.1. על פי הרשימה שהועברה לביקורת קיימים בעירייה 28 מאגרי מידע.

1.8.2. 32% בלבד מכלל המאגרים רשומים כנדרש (לרבות המאגרים המצריכים עדכון).

1.8.3. 52% מהמהאגרים נמצאים בתהליכי רישום.

1.9. על-פי סגן מנהל האגף מערכות מידע ומחשוב המאגרים בתהליכי רישום מאחר ובוצעו שינויים מבניים בזהות הבעלים ומנהלי המאגרים.

## 2. מסמך הגדרות המאגר

2.1. סעיף 2 לתקנות הגנת הפרטיות קובעות, כי על בעל מאגר מידע חלה האחריות לתאר במסמך "הגדרות המאגר" מספר נושאים, כמפורט :

2.1.1. תיאור כללי של פעולות האיסוף והשימוש במידע.

2.1.2. תיאור מטרות השימוש במידע.

2.1.3. סוגי המידע השונים הכלולים במאגר המידע (צנעת הפרט, מידע רפואי, מידע גנטי \ ביומטרי, דעות פוליטיות \ דתיות, עבר פלילי, נתוני תקשורת, מידע כלכלי, הרגלי צריכה).

2.1.4. פעולות עיבוד מידע באמצעות מחזיק.

2.1.5. הסיכונים העיקריים של פגיעה באבטחת המידע, ואופן ההתמודדות עמם.

2.1.6. שמו של מנהל מאגר המידע, של מחזיק המאגר ושל הממונה על אבטחת מידע.

2.2. לביקורת הועברו 10 מסמכי הגדרות המאגר.

2.3. הביקורת דגמה 5 מסמכי "הגדרת במאגר" והשוואתם לתקנות, נמצא כי :

<u>שם המאגר</u>				<u>הנושא</u>
<u>אובלוסין</u>	<u>שכר וכ"א</u>	<u>חינוך</u>	<u>קידום נוער</u>	
✓	✓	✓	✓	תאור כללי
✓	✓	✓	✓	מטרות
✓	✓	✓	✓	סוגי המידע
✓	✓	✓	✓	העברת מידע
✓	✓	✓	✓	עיבוד באמצעות מחזיק
✓	✓	✓	✓	סיכונים והתמודדות
✓	✓	✓	✓	זהות הבעלים
✓	x	x	x	זהות המנהל
לא רלוונטי	לא רלוונטי	לא רלוונטי	לא רלוונטי	זהות המחזיק
✓	✓	✓	✓	ממונה אבטחת מידע

2.4. מנתוני הטבלה עולה, כי מסמכי הגדרות המאגר מתועדים בהתאם לתקנות.



- 2.5. עם זאת, זהות מנהל מאגרי המידע אינה מעודכנת. הדבר נובע גם מהעובדה שלאחרונה התחלפו מספר רב של בעלי תפקידים בעירייה.
- 2.6. הביקורת ממליצה לשמור על מסמך הגדרות המאגר מעודכן בהתאם לזהות מנהל המאגר בפועל.

## פרק ג' - עמידה בדרישות הרגולציה

### 1. כללי

1.1. חוק הגנת הפרטיות והתקנות שהותקנו בעקבותיו החל משנת 2017 מהווים בסיס לעבודת אגף המחשוב בתחום אבטחת המידע.

### 2. מינוי ממונה על אבטחת מידע

#### 2.1. ממונה אבטחת מידע

2.1.1. סעיף 17 ב. לחוק הגנת הפרטיות קובע כי: "הגופים המפורטים להלן מחוייבים במינוי אדם בעל הכשרה מתאימה שיהיה ממונה על אבטחת מידע... (2) רשויות מקומיות".

2.1.2. בהתאם ל"כתב מינוי ממונה אבטחת מידע" נמצא, כי ביום 04/09/2019 אישרה מועצת העיר את מינויה של עובדת באגף מערכות מידע ומחשוב בתפקיד ממונה אבטחת מידע בעירייה.

2.1.3. על פי דרישות תקנות משרד הפנים על ממונה אבטחת מידע לעמוד בדרישות להלן:

א. השכלה: בעל תעודת טכנאי או הנדסאי.

ב. ניסיון מקצועי: שלוש שנים לפחות כמנהל או כסגן מנהל מערכות מידע, או מנהל אבטחת מידע בחברה בעלת 55 עובדים ומעלה.

2.1.4. הביקורת סבורה כי לממונה אבטחת מידע אין את הידע המקצועי הנדרש על מנת להקים תוכנית בקרה על מערכות העירייה. סגן מנהל אגף מערכות מידע מסכים לכך.

2.1.5. להלן בטבלה תוצאות הבדיקה בנוגע לדגשים אלו:

התקנה	תקין / לא תקין
כפיפות למנהל בכיר (שאינו בניגוד עניינים)	x
כתיבת נוהל עירוני לאבטחת מידע	✓
הקמת תוכנית בקרה שוטפת	x
לא ימלא תפקיד נוסף מחשש לניגוד עניינים	x
הקצאת משאבים מספקים	x

2.2. מהטבלה עולה, כי :

2.2.1. על-פי התקנות, ממונה על אבטחת מידע אמור להיות כפוף למנהל בכיר, אולם בשל העובדה שעליו לבצע בקרה בנושא זה, אין הוא יכול להיות כפוף לסגן מנהל אגף מערכות מידע כפי שקיים היום.

2.2.2. הממונה על אבטחת המידע בעירייה כפופה לסגן מנהל האגף מערכות מידע ומחשוב, והדבר מהווה ניגוד עניינים שכן הגורם המבקר (ממונה אבטחת מידע) הינו כפוף של הגורם המבוקר (סגן מנהל אגף מערכות מידע).

2.2.3. על הממונה על אבטחת מידע מוטלים תפקידים נוספים באגף מערכות מידע ומחשוב, וקיים ניגוד עניינים כך שהממונה אבטחת מידע אינה יכולה לערוך בקרה אחר הפעולות שהיא עצמה מבצעת.

2.2.4. הממונה על אבטחת מידע כתבה הוראות עבודה חדשות בשנת 2021 בתחום אבטחת מידע על-פי התקנות.

2.2.5. בהוראות העבודה קיימות הנחיות לביצוע בקרות שונות בתחום אבטחת המידע. טרם הועברו לביקורת בקרות שבוצעו בפועל.

2.2.6. לדברי סגן מנהל אגף מערכות מידע ומחשוב, הקמת בקרות שוטפות בנושאי אבטחת מידע הינו תחום ידע מקצועי אשר אינו קיים כיום בעירייה, בשל היעדר כוח אדם מקצועי לעניין זה. בנוסף, היקפה של מצבת כח-האדם הקיימת באגף, אינה מאפשרת ביצוע בקרות בנושאי אבטחת מידע.

2.2.7. מנכ"לית העירייה הנחתה את סמנכ"לית שירות וסגן מנהל אגף מערכות מידע ומיחשוב להכין תוכנית לשיפור יכולות אבטחת המידע של העירייה בהתאם לממצאי סקר הסיכונים. לאור העובדה, כי העירייה נמצאת בתוכנית הבראה ואושר לה חשב מלווה, הדבר יתבצע בהתאם ליכולות הכספיות של העירייה.

**2.3. מסקנות והמלצות**

2.3.1. מינוייה של ממונת אבטחת המידע בעירייה אינו תואם את הוראות החוק, משום שהיא כפופה לסגן מנהל אגף מערכות מידע ומיחשוב ואין לה את הידע המקצועי והנסיון לבצע את מטלות התפקיד.

2.3.2. יש למנות ממונה אבטחת מידע אשר לא יהיה כפוף לסגן מנהל אגף מערכות מידע ומיחשוב, ושיהיו לו הידע המקצועי והנסיון כנדרש לתפקיד זה.

2.3.3. יש להכין תוכנית בקרה שוטפת אחר מאגרי המידע.

2.3.4. הביקורת סבורה, כי לאור העובדה שלממונת אבטחת מידע אין את הידע המלא הדרוש לנושא זה, וככל שהיא תמשיך בתפקידה זה בכפיפות למנהל בכיר אחר, יש לפעול להכשירה באופן מקצועי. כגון: בימי עיון וכנסים מקצועיים.

2.3.5. יש לציין, כי העירייה שכרה יועץ מקצועי המשלים את הפעילות המקצועית בתחום אבטחת המידע, אולם מדובר על ביצוע חלק ממטלות התפקיד והיקף משרה מצומצם (יום בשבוע בלבד).

#### 2.4. החלטות מנכ"לית העירייה

2.4.1. מנכ"לית העירייה הורתה, כי הכפיפות הארגונית של ממונת אבטחת מידע, בנושאי זה תהיה ישירות לסמנכ"לית שירות. בנוסף החליטה מנכ"לית העירייה כי יש להכשיר את ממונת אבטחת מידע לתפקידה.

### 3. ביצוע סקר סיכונים ומיפוי המאגר

#### סקר סיכונים

3.1. על פי סעיף 5 (ג) על בעל המאגר האחריות לערוך סקר לאיתור סיכוני אבטחת מידע אחת ל-18 חודשים לפחות ולפעול לתיקון הליקויים.

3.2. הביקורת בחנה ביצוע סקר סיכונים על-ידי העירייה.

3.3. לביקורת הועברו 2 סקרי סיכונים אשר נערכו על-ידי יועץ חיצוני בשנת 2020, כמפורט:

3.3.1. "סקר סיכוני אבטחת מידע בדיקת חוסן תשתיתית".

3.3.2. "סקר סיכונים תהליכי לנושא אבטחת מידע".

3.4. הביקורת בחנה את יישום המלצות סקרי הסיכונים.

3.5. לצורך כך הועבר לביקורת מסמך "יישום המלצות ונושאים מסקר סיכונים- בדיקת חוסן" (להלן: "מסמך יישום המלצות").

3.6. סקירת תוכנית העבודה השנתית 2021 אשר הועברה לביקורת מעלה, כי עתיד להתקיים מעקב אחר ביצוע המלצות סקר הסיכונים.

3.7. נדגיש, כי מסמך יישום ההמלצות מכיל מספר ליקויים אשר מחייבים תיקון מיידי.

3.8. בחינת הביקורת העלתה שעד מועד הביקורת לא תוקנו כל הליקויים המחייבים תיקון מיידי, לרבות:

3.8.1. "יש לבצע ריענון של חתימות עובדים על טופס שמירת סודיות".

3.8.2. "לבצע ניטור במערכת ה-WSUS אשר מתריעה על ביטול העדכון האוטומטי דרך מערכת העדכונים".

3.9. על-פי סגן מנהל האגף מערכות מידע, תיקון הליקויים באופן מיידי מחייב גיוס כוח-אדם מקצועי במשרה מלאה ורכישת כלים טכנולוגיים. כח-האדם באגף כיום אינו מסוגל לעמוד בהיקף המשימות וברמת המקצועיות הנדרשת.

3.10. הביקורת ממליצה ליישם את המלצות סקר הסיכונים בהקדם.

3.11. על-פי סעיף 5 (ד) על בעל המאגר האחריות לערוך מבדקי חדירות למערכות המאגר אחת ל-18 חודשים לפחות - על מנת לבחון עמידותן בפני סיכונים פנימיים וחיצוניים.

3.12. בדיקת הביקורת העלתה, כי כחלק מביצוע סקר הסיכונים בוצעו מבדקי חדירות למערכות העירייה.

3.13. מיפוי המאגר

- 3.13.1. סעיף 5 לתקנות קובע כי על בעל מאגר מידע להחזיק מסמכי "מבנה המאגר" וכן "רשימת מצאי" מעודכנת של מערכות המאגר.
- 3.13.2. מהביקורת עולה, כי לעירייה "תיק אתר" אשר הוכן בסיוע חברת "יוביטק" המעודכן באופן שוטף על ידי מנהל תפעול מחשוב.
- 3.13.3. סעיף 6.8 ל"נוהל תגובה לאירועי סייבר" קובע, כי: "באחריות סגן מנהל האגף מערכות מידע ומחשוב לתחזק ולשמור בצורה מוצפנת תיק אתר..."
- 3.13.4. הביקורת העלתה, כי תיק האתר אינו מוצפן ונמצא ברשת הארגונית בידי מנהלת תפעול מחשוב.
- 3.13.5. הביקורת ממליצה לבחון את הצורך בהצפנת תיק האתר מאחר אינה נדרשת מהתקנות.
- 3.13.6. בחינת תיק האתר בהשוואה לתקנות העלתה כי:

#	הדרישה	קיים
1.	כלל תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע	✓
2.	מערכות התוכנה המשמשות להפעלת מאגר המידע, לניהול המאגר ולתחזוקתו, לתמיכה בפעילותו, לניטורו ולאבטחתו	✓
3.	תוכנות וממשקים המשמשים לתקשורת אל מערכות המאגר ומהן	✓
4.	תרשים הרשת שבה פועל המאגר, הכולל תיאור הקשרים בין רכיבי המערכת השונים ומיקומם הפיזי של הרכיבים	x
5.	תאריך העדכון האחרון של המסמך ושל רשימת המצאי	✓

- 3.13.7. מסקירת תיק האתר עולה, כי:
- א. קיימת רשימת מצאי של מערכות חדר השרתים.
- ב. קיימת רשימת תוכנות המשמשות להפעלת מאגרי המידע.
- ג. לא קיים תרשים רשת בה פועלים המאגרים, נציין כי קיימת רשימת מצאי מתגים.
- 3.13.8. סעיף 5 (ב) המסמך המעודכן של מבנה מאגר המידע ורשימת המצאי יישמרו כך, שפרטים מהם יימסרו לבעלי הרשאה רק בהיקף הנדרש לצורך ביצוע תפקידיהם.
- 3.13.9. הביקורת העלתה, כי תיק האתר אכן נשמר בידי מנהלת תפעול מחשוב.

**4. אבטחה פיזית וסביבתית**

4.1. סעיף 6 (א) לתקנות קובע, כי בעל מאגר מידע יבטיח, כי רכיבי המערכות- תשתיות, חומרה, תקשורת ואבטחה יישמרו במקום מוגן, המונע חדירה וכניסה אליו בלא הרשאה.

4.2. סעיף 6 (ב) קובע, כי בעל המאגר ינקוט אמצעים לבקרה ולתיעוד של הכניסה והיציאה מאתרים שבהם מצויים רכיבי המערכות- תשתית, חומרה, תקשורת ואבטחה ושל הכנסה והוצאה של ציוד אל מערכות המאגר ומהן.

4.3. השוואת "נוהל אבטחה ארגוני למאגרי מידע", וכן "נוהל אבטחה פיזית וסביבתית" לדרישות התקנות מעלה כי:

התייחסות בהוראות העבודה	דרישות התקנות
✓	בטיחות חשמל אש ומים
✓	מניעת כניסה של אדם וציוד ללא אישור
✓	קיום אמצעים לבקרה ותיעוד גישה לאתרי המחשוב

4.1. סקירת הוראת העבודה מעלה, כי קיימת התייחסות לשרתים הממוקמים באתרי העירייה וכן לשרתים בבעלות ספקים.

**בדיקות שגרתיות למערכות ההגנה הפיזית**

4.2. הביקורת בחנה קיום בדיקות שגרתיות למערכות ההגנה על השרתים ונמצא, כי על-פי סעיף 5.6 "נוהל אבטחה ארגוני למאגרי מידע": "התייחסות לסיכוני אש ומים יהיו על פי הנחיות ממונה הבטיחות של העירייה".

4.3. בבדיקה מול ממונה הבטיחות של העירייה, שנקלט לעבודה חודשים ספורים טרם הביקורת, עולה, כי טרם הועברו המלצות לאגף מערכות מידע ומחשוב בנושא בטיחות מים ואש.

4.4. בדיקה נוספת שנערכה מול רע"ן מקלטים וכיבוי-אש בעירייה עולה, כי מערכות כיבוי אש נבדקות אחת לשנה, ובנוסף נערכת בדיקה וויזואלית אחת לחצי שנה.

4.5. סקירת הביקורת העלתה, כי קיים ציוד מחשוב הממוקם במספר מוקדים באתרי העירייה השונים, בין היתר, כמפורט:

- |                   |                   |
|-------------------|-------------------|
| 1. חשמונאים       | 7. שח"ם נגבה 13   |
| 2. מוקד עירוני    | 8. שח"ם נגבה 12   |
| 3. שרות פסיכולוגי | 9. שחם רוטשליד 29 |
| 4. הנדסה          | 10. שח"ם רונין    |
| 5. בית המשפט      | 11. מכללה         |
| 6. משק            | 12. בניין העירייה |

4.6. חדר השרתים המרכזי של העירייה ממוקם בבניין העירייה, ושרת המצלמות במוקד העירוני אשר שוכן במתחם החשמונאים.

4.7. בסיור מדגמי בחדרי השרתים וחדרי התקשורת אשר התקיים ביום 02/03/2021 בבניין העירייה ברחוב נורדאו ובמתחם חשמונאים נמצא, כי:

אתר		דרישות
חשמונאים	בניין העירייה	
✓	✓	כיבוי-אש
✓	✓	מיזוג
✓	✓	נעילה אפקטיבית
x	x	תיעוד כניסה
✓	✓	מצלמות

4.1. הערה: בסעיף זה הושמטו פרטים חסויים.

4.2. הביקורת ממליצה לתעד כניסה ופעילות בחדרי השרתים על-ידי בעלי התפקידים.

## 5. אבטחת מידע בניהול כוח-אדם

### גיוס עובדים

ממצאי הסעיף, מסקנות והמלצות ירוכזו בהמשך

5.1. סעיף 7 (א) לתקנות קובע, כי יש לתת התייחסות, באמצעים סבירים, על כך שאין חשש, כי בעל הרשאה אינו מתאים לקבלת גישה למידע המצוי במאגר.

5.2. בבדיקה מול מנהלת מחלקת תנאי שירות בחטיבת הון-אנושי נמצא, כי על-פי שיטות העבודה הנהוגות בחטיבת הון-אנושי:

5.2.1. עובדים מתבקשים למלא טופס שאלון אישי אשר בו קיימת הצהרת העדר הרשאה פלילית.

5.2.2. בנוסף על העובד למלא טופס "הצהרה והתחייבות להימנע ממסירת מידע ממאגר מידע" (להלן: "הצהרת שמירת סודיות").

5.2.3. לעובד ניתן דף הנחיות "אבטחת מידע והגנת הפרטיות- דף הנחיות לעובד".

5.3. הביקורת מעלה, כי טפסי השאלון האישי וכן הצהרת שמירת סודיות נשמרים בתיק האישי של העובד בחטיבת הון אנושי, כנדרש.

### סיום העסקת עובד

5.4. סעיף 9 (ג) לתקנות אבטחת מידע קובע, כי בעל המאגר ידאג לביטול הרשאות של בעל הרשאה שסיים את תפקידו, ובמידת האפשר לשינוי סיסמאות, מיד עם סיום תפקידו של בעל הרשאה.

5.5. סעיף 6.3 לנוהל משתמשים והרשאות קובע את סדר הפעולות הבא בסיום העסקה:

א. מנהל ישיר יעביר דיווח מידי לממונה אבטחת מידע.

ב. ממונה אבטחת מידע ישהה את העובד בקובץ מורשי הגישה.

ג. אגף משאבי אנוש יעביר אחת לחודש רשימת עובדים שסיימו את עבודתם בעירייה.

- 5.6. הביקורת העלתה, כי ממונת אבטחת מידע אינה מקבלת דוחות ממשאבי אנוש על עובדים שגוייסו, סיימו את העסקתם.
- 5.7. סגן מנהל האגף מערכות מידע ומחשוב מקבל הודעות דוא"ל על גיוס, סיום העסקה של עובדים. אותם הוא מעביר למנהלת תפעול מחשוב, לסגנית מנהל המחלקה ולחברת מטרופולינט לביצוע סגירת חשבונות משתמשים.
- 5.8. הביקורת מצאה חשבונות משתמשים פעילים על-אף שסיימו את תפקידם בעירייה. במהלך הביקורת משתמשים אלו נסגרו.
- 5.9. מנכ"לית העירייה הנחתה את סגן מנהל אגף מערכות מידע ומיחשוב לעדכן את הנוהל העוסק בגיוס עובדים וסיום העסקתם, כך שחשבונותיהם יסגרו והמידע המקצועי והרלוונטי ישאר לשימושם של בעלי התפקידים הרלוונטיים.

#### **שינוי תפקיד**

- 5.10.1. סעיף 6.4 לנוהל משתמשים והרשאות קובע:
- 5.10.2. המנהל החדש יעביר בקשה להרשאות חדשות.
- 5.10.2. אגף משאבי אנוש יעביר אחת לחודש לממונה אבטחת המידע את רשימת עובדים ששינו תפקידם.
- 5.11. סעיף 5.2.1 ג' לנוהל "קליטה וחניכת עובד חדש" מחודש יולי 2014 קובע, כי: "המנהל הישיר יעדכן את אגף המחשוב ואת אגף משאבי אנוש לגבי שינוי שיבוצו של העובד על מנת לבצע את העדכונים הנדרשים במערכות עוד שבועיים לפני סיום תפקידו."
- 5.12. סעיף 5.2.2 א' לנוהל "קליטה וחניכת עובד חדש" קובע, כי: "מנהל המחלקה הישיר במחלקה החדשה יטפל בהרשאות הנדרשות לעבודת העובד הנכנס ולבטל הרשאות קודמות שאינן רלוונטיות לתפקידו החדש".
- 5.12.1. הביקורת ביקשה לבחון חסימת הרשאות לעובדי עירייה אשר שינו את תפקידם, אך עקב קושי בהשגת הנתונים ממערכת משאבי-אנוש, בחינה זו לא בוצעה.
- 5.13. הביקורת ממליצה על הקמת דוח המרכז את כלל העובדים אשר שינו את תפקידם.
- 5.13.1. על דוח זה לעבור לבחינת הממונת אבטחת מידע אחת לרבעון / שנה.
- 5.14. בבדיקה מדגמית של עובד בעל הרשאות באגף הפיקוח ששינה תפקיד לאגף אחר בעירייה בשנת 2020 עולה, כי הפרופיל הישן נסגר, וכי לא ניתן לעשות בו שימוש.
- 5.15. הביקורת ממליצה על העברת דוחות אוטומטיים חודשיים ממערכת משאבי-אנוש לממונת אבטחת מידע לצורך ביצוע בקרה על גיוס, סיום העסקה, ושינוי תפקיד, לשם סגירת משתמשים שאין בהם צורך.

#### **הדרכות בעלי הרשאות**

- 5.16. סעיף 7 (ב) לתקנות קובע, כי יש לקיים הדרכות לבעלי הרשאות, בטרם יקבלו גישה למאגר המידע או לפני שינוי הרשאותיהם.
- 5.17. על פי סעיף 7 (ג) יש לקיים פעילות הדרכה תקופתית אחת לשנתיים לפחות לבעלי ההרשאות וסמוך ככל הניתן בעת מתן הרשאה חדשה.



- 5.17.1. הממונה על אבטחת מידע מסרה, כי במועד מיפוי מאגרי המידע בעירייה הועברו הנחיות להתנהלות עם מאגר מידע לכלל מנהלי המאגרים.
- 5.17.2. בנוסף, סקירת תוכנית העבודה לשנת 2021 העלתה, כי עתידה להתקיים הדרכה למנהלי מאגרי המידע.

### **העלאת מודעות עובדים**

- 5.18. על-פי מערך הסייבר הלאומי, תרבות של הגנת סייבר בארגון חשובה לצמצום סיכוני התקיפה של הארגון. עובדי העירייה מהווים כלי משמעותי בידי התוקף, ועל-כן, יש לקיים הדרכות והעלאת מודעות להתמודד עם סיכונים אלו.
- 5.19. לצורך העלאת מודעות עובדים משתמש מנהל מערכות מידע ומחשוב בהודעות דוא"ל בעלות מידע על סיכוני אבטחה, והדרך שבה על העובד לנהוג באם נתקל במצב דומה.
- 5.20. סקירת הודעות דוא"ל מעלה, כי בשנת 2020 נשלחו 18 הודעות ע"י סגן מנהל האגף מערכות מידע ומחשוב שעניינן לימוד, התראות, ודרכי התמודדות עם אירועי אבטחת מידע (להרחבה ראה **נספח ב**).
- 5.21. הודעות הדוא"ל נשלחות מתיבת הדוא"ל הפרטית של מנהל מערכות מידע ומחשוב, והן אינן כתובות בשפה המובנת לכל קורא.
- 5.22. לצורך העלאת מודעות העובדים הביקורת ממליצה על:
- 5.22.1. הנגשת הטקסט לקורא.
- 5.22.2. שליחת ההודעה מכתובת דוא"ל ייעודית לנושא אבטחת מידע.
- 5.22.3. נציין כי בעקבות הערת הביקורת החל שימוש בכתובת דוא"ל "אבטחת מידע".
- 5.23. בנוסף להודעות הדוא"ל, שלח סגן מנהל האגף מערכות מידע ומחשוב קישור ללומדה מקוונת בנושא אבטחת מידע שפותחה על-ידי מערך הסייבר הלאומי.
- 5.24. הביקורת מציינת בחיוב את השימוש בתכנים חיצוניים אשר חוסכים משאבים לעירייה.
- 5.25. לאחרונה, הועברה לומדה באמצעות חטיבת הון אנושי לכלל עובדי העירייה בה נכלל גם נושא הדרכה בתחום אבטחת המידע. העובדים נבחנו על תוכן המידע. הדבר נותן אינדקציה מסויימת לגבי העברת המידע וקבלתו על ידי העובד.
- 5.26. על-פי סגן מנהל אגף מערכות מידע, לאחרונה בוצעו פעולות רבות על-ידי אגף מערכות מידע ומיחשוב יחד עם חטיבת הון אנושי אשר מייעלות את תהליך פתיחת חשבונות משתמשים וסגירתם ברשת העירונית.

### **6. ניהול הרשאות גישה**

- 6.1. תקנה 8 (א) קובעת, כי יש לקבוע הרשאות גישה למאגר לכל עובד, רק במידה הנדרשת לו לצורך ביצוע תפקידו.
- 6.2. בדיקת הביקורת העלתה, כי חלק מהמערכות בשימוש העירייה אינן מאפשרות הגדרת הרשאות כאמור בתקנות, וכי הרשאות הגישה לעובדים נעשות בצורה המיטבית בנסיבות הקיימות.

- 6.3. סעיף 8 (ב) קובע, כי יש לנהל "רשימת הרשאות תקפות" מעודכנת של תפקידים, ההרשאות שניתנו להם, ובעלי התפקידים שקיבלו את ההרשאות הללו.
- 6.4. ממונת אבטחת מידע מוסרת כי לצורך ביצוע בקרה על הרשאות העובדים יש לשלוח לכל מנהל מאגר רשימת עובדים בעלי הרשאה. על בעל המאגר לבחון כי כלל העובדים.
- 6.5. לביקורת לא הועברה "רשימת הרשאות תקפות" אשר על בסיסה, יש לעדכן את המשתמשים במערכות הממוחשבות של העירייה השונות.
- 6.6. הביקורת ממליצה על יצירת רשימת הרשאות תקפות לכל מערכות העירייה על-מנת לעמוד בדרישות התקנות.
- 6.7. לביקורת לא הועברו אסמכתאות לבקרות שבוצעו אחר תהליך נאותות ההרשאות במערכות העירייה השונות.
- 6.8. הביקורת ממליצה, כי ממונת אבטחת מידע תדרוש אחת לשנה ממנהלי המאגרים רשימת הרשאות תקפות, ותבחן אותה אל מול רשימת המורשים במערכות העירייה השונות.
- 6.9. סגן מנהל האגף מוסר כי פתיחת הרשאות הינה נושא בעל חשיבות, על כן נקבע תהליך עבודה בו לא תיפתח הרשאה לעובד ללא אישור מנהל. כלל הבקשות מגיעות לסגן מנהל האגף אשר בוחן את הצורך בהרשאה ומעביר לביצוע.

## 7. זיהוי ואימות

- 7.1. תקנה 9 (א) קובעת, כי יש לוודא שהגישה למאגר נעשית על-ידי בעל הרשאה מתאימה על-פי "רשימת ההרשאות התקפות".
- 7.2. בחינת סעיף 6.9 לנהל האבטחה הארגוני קובע, כי:
- 7.2.1. כל משתמש או עובד מחשב יוגדר בטבלאות ההרשאה למערכות הממוחשבות השונות.
- 7.2.2. כל מנהל/ת אחראי יעביר באופן שוטף רשימה של שינויים של עובדים משתמשי מחשב.
- 7.2.3. מידי שנה תתבצע בדיקת נאותות של ההרשאות.
- 7.3. לביקורת לא הועברו רשימת הרשאות תקפות ו/או אסמכתאות לבדיקות כאמור.
- 7.4. תקנה 14 (ג) קובעת, כי במאגר מידע שניתן לגשת אליו מרחוק (עבודה מהבית) באמצעות רשת האינטרנט, ייעשה שימוש נוסף על אמצעי אבטחה המפורטים לעיל, שמטרתם לזהות את המתקשר והמאמתים את הרשאתו לביצוע הפעילות מרחוק ואת היקפה באמצעות אמצעי פיזי הנתון לשיטתו הבלעדית של בעל הרשאה.
- 7.5. הביקורת העלתה, כי חיבור עובדים לעבודה מרחוק אינו מתבצע באמצעות אמצעי פיזי כגון מכשיר הטלפון של העובד.
- 7.6. לדברי סגן מנהל האגף, נעשית פעילות לקדם נושא זה.
- 7.7. תקנה 9 (ב) (2) קובעת, כי יש לקבוע בנהל האבטחה התייחסות לבאים:
- 7.7.1. אופן הזיהוי - אם אופן הזיהוי מבוסס על סיסמאות:

7.7.2. חוזק הסיסמה.

7.7.3. מספר הניסיונות השגויים.

7.7.4. תדירות החלפת הסיסמאות- לתקופה שלא תעלה על 6 חודשים.

7.7.5. ניתוק אוטומטי לאחר פרק זמן של אי-פעילות.

7.7.6. אופן הטיפול בתקלות הקשורות באימות זהות.

7.7.7. בעל המאגר ידאג לביטול ההרשאות של בעל ההרשאה שסיים את תפקידו, ובמידת האפשר לשינוי סיסמאות, מיד עם סיום תפקידו של בעל ההרשאה.

7.8. הביקורת בדקה ומצאה, כי מדיניות הסיסמאות כפי שבאה לידי ביטוי בנוהל אבטחה ארגוני בסעיף 6.8. עומדת בדרישות התקנות.

7.9. הביקורת בדקה ומצאה כי:

התקנה	ביצוע בפועל
קשיחות הסיסמה	9 תווים, אות גדולה, אות קטנה וסימן
תדירות החלפת ססמאות	3 חודשים
ניתוק אוטומטי	15 דק'
אופן הטיפול בתקלות הקשורות לאימות זהות	העובד נחסם עד לשחרור החסימה על-ידי עובדי אגף המחשוב

## 8. בקרה ותיעוד גישה

8.1. תקנה 10 קובעת, כי יש לנהל "מנגנון בקרה אוטומטי" שיאפשר ביקורת על הגישה למערכות המאגר.

8.2. מנגנון הבקרה כאמור מפיק רשומות (LOG) הניתנות לניתוח וזיהוי חריגים ומכיל נתונים כגון זהות המשתמש, מועד נסיון ההתחברות ואישור או שלילת ניסיון ההתחברות.

8.3. הביקורת העלתה, כי מנגנון כאמור לא נמצא בשימוש על-ידי ממונת אבטחת מידע בעירייה.

8.4. על-פי ממונת אבטחת מידע בחלק ממערכות המידע קיים תיעוד חלקי של המשתמשים אך עקב חוסר במשאבים לא נבחן לזיהוי חריגים.

8.5. תקנה 10 (ב) קובעת, כי מנגנון הבקרה לא יאפשר ביטול או שינוי של הפעלתו. עליו לאתר שינויים או ביטולים בהפעלתו ולהפיץ התראות לאחראים.

8.6. על פי תקנה 10 (ג) בעל מאגר המידע נדרש לקבוע נוהל בדיקה שגרתית של נתוני התיעוד של מנגנון הבקרה, ויערוך דו"ח של הבעיות שהתגלו וצעדים שננקטו בעקבותיה.

8.7. בדיקת הביקורת העלתה כי על-פי סעיף 6.10 בנוהל האבטחה הארגוני: "מידי חודש תתבצע בדיקה מלאה של קובץ וייבדקו אירועים חריגים".

8.8. ממונת אבטחת מידע מוסרת כי עקב ריבוי משימות הרשומות אינן נבדקות.

8.9. תקנה 10 (ד) קובעת, כי נתוני התיעוד של מנגנון הבקרה יישמרו למשך 24 חודשים לפחות.

8.10. תקנה 10 (ה) קובעת, כי בעל המאגר יידע את בעלי ההרשאות במאגר בדבר קיום מנגנון הבקרה למערכות המאגר.

8.11. הביקורת ממליצה על הקמת בקרה אחר הגישה למאגרי המידע, כנדרש מהתקנות. במערכות ממוחשבות מסויימות, יש רישום אוטומטי של הניגשים לפעילות במערכת, אולם לא מתקיימת בקרה שוטפת אחר זהותם.

### **9. תיעוד של אירועי אבטחה**

9.1. **אירוע אבטחה חמור** - אירוע שנעשה בו שימוש במידע מן המאגר, בלא הרשאה או בחריגה מהרשאה או שנעשתה פגיעה בשלמות המידע.

9.2. סעיף 11 (א) לתקנות קובע, כי בעל מאגר המידע אחראי לתיעוד כל מקרה שבו התגלה אירוע המעלה חשש לקיום אירוע אבטחה. ככל-האפשר יבוסס התיעוד האמור על רישום אוטומטי.

9.3. ממונת אבטחת מידע מסרה, כי בחלק ממערכות המידע קיים רישום אוטומטי חלקי של משתמשים במערכת.

9.4. סעיף 11 (ב) לתקנות קובע, כי בנוהל האבטחה יקבע בעל מאגר מידע גם הוראות לעניין התמודדות עם אירועי אבטחת מידע, לפי חומרת האירוע ומידת רגישות המידע, לרבות:

9.4.1. לעניין ביטול הרשאות.

9.4.2. צעדים מיידיים אחרים הנדרשים.

9.4.3. לעניין דיווח לבעל המאגר על אירועי אבטחה ועל פעולות שננקטו.

9.5. בחינת "נוהל תגובה לאירועי סייבר" מעלה כי הנוהל מפרט את הצעדים הנדרשים בעת אירועי סייבר.

9.6. סעיף 11 (ג) לתקנות קובע, כי בעל המאגר יקיים דיון אחת לרבעון על אירועי האבטחה שהתרחשו, ויבחן את הצורך בעדכונו של נוהל האבטחה.

9.7. על-פי הממונה לאבטחת מידע לא התקיימו אירועי אבטחה המצריכים דיונים כאמור. סגן מנהל האגף מערכות מידע ומחשוב מאשר זאת.

9.8. סעיף 11 (ד) קובע, כי יש לדווח לרשם מאגרי מידע באופן מיידי על אירוע אבטחה חמור ועל צעדים שננקטו.

9.9. בחינת "נוהל תגובה לאירועי סייבר" מעלה, כי הצורך בדיווח לרשם לא מצויין בנוהל, כנדרש מהתקנות.

9.10. הביקורת ממליצה על עדכון הוראת העבודה בזהות המדווח לרשם וכן מועד הדיווח.

### **10. התקנים ניידים**

10.1. סעיף 12 לתקנות קובע, כי בעל המאגר יגביל או ימנע אפשרות לחיבור התקנים ניידים למערכות המאגר במתכונת ההולמת את רמת אבטחת המידע שחלה על המאגר.

- 10.2. במהלך הביקורת נחסמה האפשרות לשימוש בהתקנים ניידים באתרי העירייה.  
10.3. שימוש בהתקן נייד מצריך פנייה לממונת אבטחת מידע ובחינה פרטנית של כל פנייה.

### **11. ניהול מאובטח ומעודכן של מערכות המאגר**

- 11.1. סעיף 13 (א) לתקנות קובעות, כי בעל מאגר מידע יקפיד על ניהול ותפעול תקין של מערכות המאגר.  
11.2. סעיף 13 (ג) קובע, כי בעל מאגר מידע ידאג לכך שיערכו עדכונים שוטפים של מערכות המאגר, לרבות חומר המחשב הנדרש לפעולתן. לא ייעשה שימוש במערכות שהיצרן לא תומך בהיבטי אבטחה שלהן אלא אם כן ניתן מענה אבטחתי מתאים.  
11.3. על-פי סגן מנהל האגף מערכות מידע ומחשוב עדכוני תוכנה לשרתי העירייה מותקנים אחת לחודש. עדכונים דחופים מותקנים מיידית על ידי מנהלת תפעול מחשוב.  
11.4. יש לציין, כי עדכוני גרסה המועברים על-ידי הספקים לעיתים יוצרים בעיות לא צפויות אשר עלולות לגרום ליותר נזק מתועלת. לכן הוחלט שלא לעדכן במייד, אלא לחכות לגרסאות עדכניות ללא פגמים ניכרים.  
11.5. הביקורת העלתה כי קיימת מערכת ניהול עדכונים (SCCM) אשר צוברת עדכונים, ומתקינה אותם באופן אוטומוטי בסוף כל חודש.  
11.6. על-פי "יישום המלצות ונושאים מסקר הסיכונים" אשר נערך על-ידי יועץ אבטחת המידע עולה, כי: "בבדיקה נמצא, כי בפועל חסרים עדכונים קריטיים על תחנות רבות".

### **12. אבטחת תקשורת**

#### **חיבור לרשת האינטרנט**

- 12.1. סעיף 14 (א) לתקנות קובע, כי 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.  
12.2. הביקורת העלתה, כי "החברה לאוטומציה" מספקת לעירייה מעטפת הגנה על בסיס תקן ISO 27001 אשר מפרט דרישות להקמה, יישום, תחזוקה ושיפור מתמיד של מערכת ניהול אבטחת מידע.  
12.3. סגן מנהל האגף מערכות מידע מבצע בקרה אחר "החברה לאוטומציה", ובוחן את אופן עמידת החברה בדרישות התקנות.  
12.4. ממכתב שהתקבל מ"החברה לאוטומציה" ביום 19/01/2021 עולה, כי החברה מבצעת בדיקות, מבדקי חדירה, שיפורים טכנולוגיים, וחדשה את ההסמכה לתקן ISO27001.  
12.5. הביקורת העלתה כי קיים שרת FW (פיירוול) אשר מדיניותו מנוהלת על-ידי מנהלת תפעול מחשוב יחד עם "החברה לאוטומציה".

- 12.6. על-פי מערך תורת ההגנה לסייבר בארגון, יש לבצע תהליך בדיקה וטיוב של חוקי מערכת הפיירוול לצורך שמירה על כשירות המערכת, וכן לצורך וידוא כי לא קיימים חוקים אשר עלולים לחשוף את הארגון שלא לצורך.
- 12.7. הביקורת מציינת, כי לא קיימת בקרה שגרתית אחר מדיניות ה-FW.
- 12.8. הביקורת ממליצה על הקמת בקרה שנתית אחר מדיניות ה-FW.

#### **העברות מידע**

- 12.9. סעיף 14 (ב) קובע, כי העברת מידע ממאגר המידע, ברשת ציבורית או באינטרנט, תיעשה תוך שימוש בשיטות הצפנה מקובלות.
- 12.10. תקנה 14 (ג) קובעת, כי במאגר מידע שניתן לגשת אליו מרחוק, באמצעות רשת האינטרנט, ייעשה שימוש נוסף על אמצעי אבטחה המפורטים לעיל, באמצעים שמטרתם לזהות את המתקשר והמאמתים את הרשאתו לביצוע הפעילות מרחוק ואת היקפה באמצעות אמצעי פיזי הנתון לשיטתו הבלעדית של בעל ההרשאה.
- 12.11. הביקורת העלתה כי החיבור מרחוק למערכות העירייה נעשה ללא אמצעי פיזי, כמתבקש מהתקנות.
- 12.12. על-פי מנהלת תפעול מחשוב הועברה דרישה לשימוש באימות דו-שלבי.
- 12.13. הביקורת ממליצה על השימוש באימות דו-שלבי בהתחברות מרחוק למערכות העירייה. שיטת זיהוי זו משתמשת באמצעים הנמצאים בידי העובד (כגון הודעת SMS עם סיסמה) לטלפון הנייד של העובד לצורך אימות רצונו להתחבר למערכת.

#### **העברת מידע בין גופים ציבוריים**

- 12.14. על-פי "תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים) תשמ"ו-1986", קיימת החובה למנות וועדת העברת מידע בין גופים ציבוריים.
- 12.15. חברי הוועדה יהיו:
- 12.15.1. מנכ"ל.
  - 12.15.2. יועמ"ש.
  - 12.15.3. עובדי ניהול מידע ואבטחתו.
- 12.16. הביקורת בדקה ומצאה, כי אכן הוקמה וועדה כנדרש.
- 12.17. מעיון בפרוטוקולי הוועדה בשנת 2020 אשר הועברו לביקורת עולה, כי התקיימו 2 פגישות ביום 09/12/2020 וכן ביום 21/07/2020. בפגישה נכחו חברי הוועדה בהתאם לתקנות שלעיל.

#### **13. מיקור חוץ**

- 13.1. תקנה 15 לתקנות הגנת הפרטיות קובעת, כי בעת התקשרות עם ספק, שאינו יחיד, יש להתייחס לסיכוני אבטחת מידע.
- 13.2. בחינת 6.14 "מהימנות עובדים, יועצים, ספקים וקבלנים" לנוהל האבטחה הארגוני בהתייחס לתקנות, קובע:

- 13.2.1. עובדים, ספקים וקבלנים של העירייה, יוחתמו על טפסים להתחייבות על שמירת סודיות המידע המגיע לידיעתם בתוקף תפקידם ועיסוקם בעירייה.
- 13.2.2. לגבי ספקים וקבלנים, תהיה התחייבות כי יפעלו למען ישמרו אנשיהם על סודיות זו, וכי ידווחו על כל מקרה בו ייודע להם על חריגה מנהלי אבטחת מערכות מידע.
- 13.2.3. כל הסכם התקשרות יכלול התייחסות לגבי תום ההתקשרות לגבי התחייבות לשמירת סודיות והחזרת חומר של העירייה.
- 13.3. להלן הפרטים עליהם לתת את הדעת בעת התקשרות עם ספקים בנושאי אבטחת מידע:

<b>הדרישה</b>
<p>בחינה לפני ביצוע ההתקשרות של סיכוני אבטחת המידע הכרוכים בהתקשרות, ואם הם גבוהים מדי בהתחשב ברגישות המידע, להימנע ממיקור החוץ לחלוטין.</p>
<p>לקבוע במפורש בהסכם את כל אלה:</p> <ul style="list-style-type: none"> <li>- מידע שהגורם החיצוני רשאי לעבד ומטרות השימוש המותרות בו לצורכי ההתקשרות.</li> <li>- מערכות המאגר שהגורם החיצוני רשאי לגשת אליהן.</li> <li>- סוג העיבוד או הפעולה שהגורם החיצוני רשאי לעשות.</li> <li>- משך ההתקשרות, אופן השבת המידע לידי הבעלים בסיום ההתקשרות, השמדתו מרשותו של הגורם החיצוני ודיווח על כך לבעל מאגר המידע.</li> <li>- אופן יישום החובות בתחום אבטחת המידע שהמחזיק חייב בהן לפי תקנות אלה, וכן הנחיות נוספות לעניין אמצעי אבטחת מידע שקבע בעל מאגר המידע.</li> <li>- חובתו של הגורם החיצוני להחתיים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק לפי האמור בהסכם, וליישם את אמצעי האבטחה הקבועים בהסכם.</li> <li>- 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.</li> <li>- 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.</li> </ul>
<p>יפרט בנוהל האבטחה של המאגר גם את העניינים המנויים בפסקה לעיל, וכן יפנה בו במפורש להסכם עם הגורם החיצוני ולנוהל האבטחה שלו.</p>
<p>ינקוט אמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות תקנות אלה, בהיקף הנדרש בשים לב לסיכונים האמורים בפסקה 1.</p>

13.4. הביקורת בחנה מדגם של 3 הסכמי התקשרות עם ספקים כמפורט:

תוקף	מועד חתימה	מהות ההתקשרות	שם הספק
25/06/2024	25/06/2018	מערכות הנדסה	החברה לאוטומציה
02/03/2021	02/03/2016	מערכת שכר	מל"ם שכר
31/10/2021	01/11/2020	מערכת רישום תלמידים	ספרת

13.5. בחינת הסכמי ההתקשרות העלתה כי:

ספרת	שכר	אוטומציה	סעיף
x	x	✓	מידע שהספק רשאי לעבד ומטרות השימוש.
x	x	x	מערכות המאגר שהגורם החיצוני רשאי לגשת אליהן.
x	✓	✓	אופן השבת המידע לידי הבעלים בסיום ההתקשרות.
x	x	✓	אופן יישום התקנות בתחום אבטחת המידע.
x	x	✓	חתימה על סודיות המידע של עובדי הספק.
x	x	x	חתימת הסכמים מול צד ג' ואופן יישום התקנות.

- 13.6. מנתוני הטבלה עולה, כי הסכמי עבר שנחתמו, לא עומדים בכלל דרישות התקנות.
- 13.7. על-פי סגן מנהל האגף מערכות מידע ומחשוב ישנה בעיה בלהכיל דרישות חדשות בהסכמי עבר שנחתמו עם ספקי העירייה.
- 13.8. תוכנת ספרת מנוהלת באגף החינוך ואינה מנוהלת מול אגף מערכות מידע ומיחשוב. הביקורת ממליצה, כי תוכנה זו וכלל התוכנות בעירייה ינוהלו מול האגף.
- 13.9. בבדיקת הסכמים חדשים עולה, כי סגן מנהל האגף מערכות מידע מצרף נספח "אבטחת מידע ושמירת סודיות" אשר מחייב את הספק לעמידה בדרישות התקנות, זאת בתנאי שהמנהל המקצועי האחראי על ההסכם מיידע אותו בדבר ההסכם.

#### בחינת טיוטת מכרזים

- 13.10. הספק "משיק" נשכר על ידי העירייה במטרה לסייע בהפקת מכרזים עירוניים.
- 13.11. בחינת טיוטת מכרז "הפעלה וגבייה של מערך חנייה עירוני" אשר הופקה על-ידי "משיק" העלתה, כי העירייה מחייבת את הזוכה במכרז ברשימת דרישות על בסיס תקנות אבטחת הפרטיות ופרקטיקות נהוגות.
- 13.12. הביקורת מציינת בחיוב את ההתייחסות המפורטת לדרישות תקנות הפרטיות.

#### 14. ביקורת תקופתית

- 14.1. תקנה 16 קובעת, כי בעל המאגר אחראי לכך שתיערך, אחת לשנתיים ביקורת פנימית או חיצונית, כדי לוודא את עמידתו בהוראות תקנות אלה.



- 14.2. כפי שצויין לעיל, בשנת 2020 בוצע "סקר סיכונים תהליכי" על-ידי יועץ חיצוני. בסקר צויין, כי: "בחינת מערך אבטחת המידע מורכב ממספר תקנים ותקנות רלוונטיים אשר אין העירייה מחוייבת להן, עם זאת, אלו הם המסמכים המנחים אשר עוזרים לקיים את מערך אבטחת המידע לפי ה-BEST PRACTICE".
- 14.3. הביקורת בדקה את קיום דרישות התקנות ומצאה כמפורט:

#	התקנה	קיים
1.	בדוח הביקורת ידווח המבקר על התאמת אמצעי האבטחה לנוהל האבטחה ולתקנות אלה, יזהה ליקויים ויציע אמצעים הדרושים לתיקון המצב.	✓
2.	בעל מאגר המידע ידון בדוחות הביקורת שיועברו לו, ויבחן את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהם.	x

14.4. נמצא כי, עד לתום הביקורת לא התקיימה ישיבה בהנהלת העיר על מנת לדון בממצאי סקר הסיכונים, להסיק מסקנות ולהנחות בהתאם את המנהלים האחראים.

14.5. להדגשה, דיון בממצאי דוח ביקורת זה זה מהוים עמידה בדרישות התקנות.

### 15. שמירת נתוני אבטחה

- 15.1. תקנת 17 קובעת, כי יש לשמור את הנתונים בטבלה שלהלן במשך שנתיים.
- 15.2. בנוסף קובעת התקנה, יש לדאוג לגיבוי באופן שניתן יהיה לשחזר בכל עת את הנתונים הבאים למצבם המקורי.
- 15.3. הביקורת בדקה ומצאה, כי:

#	הדרישה	קיים
1.	בקרה ותייעוד של כל כניסת מורשים וציוד מאתרי תשתיות, חומרה, רכיבי תקשורת ואבטחת מידע.	לא קיים תיעוד
2.	רשימת ההרשאות התקפות והשינויים שבוצעו בה.	לא קיימת רשימת הרשאות תקפות
3.	אופן זיהוי ואימות.	קיים במערכת ניהול המשתמשים
4.	מנגנון הבקרה אשר מתעד אוטומטית גישה ונסיונות גישה למערכת.	קיים באופן חלקי בחלק מהמערכות
5.	תיעוד אירועי אבטחה, לרבות שחזורים שבוצעו, זהות המשחזר והנתונים ששוחזרו.	לא קיים תיעוד

15.4. מהטבלה עולה, כי בעירייה אין בקרה על רשומות (LOG) אשר מתבקשת מהתקנות.

### 16. גיבוי ושחזור נתוני אבטחה

- 16.1. תקנה 18 קובעת, כי יש לשמור במסמך "נוהל גיבויים", את הפרטים הבאים:
- 16.1.1. ביצוע גיבויים באופן תקופתי שגרתי.

- 16.1.2. אבטחת שחזור הנתונים.
- 16.1.3. ביצוע שחזור באישור מנהל המאגר בלבד.
- 16.1.4. במסגרת תיעוד אירועי אבטחה, יש לשמור שחזורים שבוצעו, זהות המשחזר והנתונים ששוחזרו.
- 16.2. על-פי סעיף 6.15 לנוהל האבטחה הארגוני על הממונה לאבטחת מידע להנחות על ביצוע גיבויים באופן שלא תפגע בהמשכיות העסקית והתפעולית של העירייה.
- 16.3. בנוסף אחת לחצי שנה יש לבצע שחזור יזום של המידע בכדי לבחון את ההתכנות והיכולת בנושא.
- 16.4. באחריות הממונה לאבטחת מידע להכנית תוכנית התאששות במקרה של כשל שרתים כללי.
- 16.5. הביקורת העלתה, כי נוהל האבטחה הארגוני לא עוסק כלל בתחומי גיבוי ושחזור מידע כנדרש מהתקנות.
- 16.6. הביקורת העלתה, כי עד היום לא נערך תרגול שחזור מידע.
- 16.7. סגן מנהל האגף מערכות מידע ומחשוב מסר לביקורת, כי טעינת הגיבויים נעשית לעיתים על-פי דרישה ממחלקות שונות בעירייה הדורשות מידע שהיה קיים בעבר במערכות המחשוב.
- 16.8. הביקורת ממליצה על כתיבת נוהל ביצוע גיבויים ושחזורים, וכן על כתיבת נוהל התאוששות מאסון.
- 16.9. הביקורת ממליצה על ביצוע תרגיל שחזור יזום.

## נספחים



## נספחים

נספח א' – רשימת מאגרי מידע אשר מופו בעירייה על-ידי הממונה לאבטחת מידע.

<u>סטטוס</u>		<u>שם המאגר</u>
<u>2020</u>	<u>2018</u>	
נרשם ואושר		יועצים
בטיפול לרישום		מאגר צלום בבתי הספר
בטיפול לרישום		הנדסה
בטיפול עדכון הרישום	רשום	רווחה
בטיפול לרישום		משפחות ילדים חריגים
בטיפול לרישום		הכנסות
בתהליך עדכון מנהל המאגר + מחזיק	רשום	שכר וכ"א
בתהליך עדכון מנהל מאגר	רשום	גזברות/ ספקים
בתהליך עדכון מנהל המאגר + מחזיק	רשום	פיקוח עירוני וחניה
נרשם ואושר		מוקד עירוני
בטיפול לרישום		ניהול צי רכב
בטיפול לרישום		אישורי כניסה לבתי הספר
נרשם ואושר		רישוי עסקים
בטיפול לרישום		וטרינר
בטיפול לרישום		שירות פסיכולוגי חינוכי
בטיפול לרישום		תביעות
בטיפול לרישום		רישום גני ילדים, כיתות א', כיתות ז'
בטיפול העברת בעלות לתאגיד עירוני	רשום	תרבות הדיור
בטיפול לרישום		מכללת בת ים- תלמידים בוגרים
ללא שינוי	רשום	אוכלוסין
בטיפול לרישום		מצלמות חופים
בטיפול לרישום		מח' משק/ ספקים, קבלנים ונותני שרותים
יועבר לבעלות החברה לתרבות נוער וספורט	רשום	תרבות
הרישום יבוטל, הפעילות מתבצעת במסגרת מאגר הרווחה.	רשום	קידום נוער
בטיפול לרישום		אזרחים ותיקים

<u>סטטוס</u>		<u>שם המאגר</u>
<u>2020</u>	<u>2018</u>	
בוצע עדכון מנהל המאגר	רשום	חינוך
בטיפול לרישום		מצלמות בבתי ספר
בבחינה נוספת		היחידה לקיימות ואיכות הסביבה

**נספח ב' – הודעות דואל שנשלחו ע"י סגן מנהל האגף מערכות מידע ומחשוב בשנת 2020.**

תאריך	נושא
13/12/2020	הודעת "פשינג" על העירייה.
11/12/2020	דף הנחיות לעובד- אבטחת מידע.
11/12/2020	כללי זהירות קניות און-ליין.
05/12/2020	התראת אבטחת מידע- חשוב- דחוף.
08/11/2020	התראה לבעלי אייפון.
31/10/2020	לומדה להערכה עצמית למוכנות סייבר.
16/10/2020	התראת דיוג מטעם אגף הסייבר.
24/09/2020	התראה דחופה אודות קמפיין להפצת דוא"ל זדוני.
01/09/2020	ידיעון אבטחת מידע חודשי אודות אירועי סייבר- משרד הפנים.
03/08/2020	שינוי במדיניות הגדרת סיסמאות ברשת העירייה.
21/05/2020	אירוע השחתת אתרי אינטרנט בישראל- משרד הפנים.
21/05/2020	מתקפת סייבר איראנית על מתקנים ישראלים.
16/04/2020	הגנת הפרטיות - סרטון רענון ומיקוד.
15/03/2020	כללי בטיחות לעבודה מהבית במערכות המחשוב העירוניות.
03/03/2020	ידיעון אבטחת מידע וסייבר 2020-02.
28/02/2020	ניצול נגיף הקורונה לביצוע מתקפות סייבר.
27/01/2020	ידיעון אבטחת מידע וסייבר.
13/01/2020	התראה על מייל דיוג.
08/01/2020	התראת הודעת הונאה.