דוח מבקר
עיריית קריית ביאליק
2014

דברים טובים

ביקורת בנושא:

אבטחת מידע במערכות המידע

לשנים 2010 - 2012

<u>ביקורת בנושא אבטחת מידע במערכות המידע</u>

<u>תקציר מנהלים</u>

להלן עיקרי ממצאים, מסקנות והמלצות מדו"ח ביקורת שנערך בעיריית קריית ביאליק בנושא: אבטחת מידע במערכות המידע.

*** לשם קבלת החלטות רצוי לעיין בדו"ח המלא.**

1. **<u>רקע כללי</u>**

בעיריית קריית ביאליק קיימים כ-10 אתרים המבוזרים במשרדי העירייה, בכל משרד קיים לפחות מחשב נייח אחד. כל המחשבים מחוברים למערכת הממוחשבת העירונית (המערכות נרכשות מספק חיצוני ולא מפותחות בעירייה) המנוהלת ע"י מחלקת המחשוב ומערכות המידע שנמצאת באגף הכספים אותו מנהל גזבר העירייה.

בראש המחלקה עומד מנהל מערכות מידע שהינו העובד היחיד במחלקה. מנהל מערכות המידע מועסק בהתאם לחוזה התקשרות עם חברת "מטרופולינט" ומועסק במשרה מלאה דרך חברה זו.

מאגרי המידע הקיימים בעירייה כגון: גביה, הנהלת חשבונות, רכש, חינוך, עיקולי בנקים, רווחה, שירות פסיכולוגי, שירותי וטרינריה, משאבי אנוש, פקוח עירוני וכו' הינם תחת ניהולה של המחלקה. תפקידה העיקרי של המחלקה הינו איתור וטיפול בתקלות וכן ניתוחן. הטיפול בשרתים ובמערכות הליבה והחנייה כולל השירות הטכני ניתנים ע"י החברה החיצונית "מטרופולינט".

2. **מבנה ארגוני (פרק 1)**

הביקורת מעירה כי מנהל מערכות המידע לא מונה באופן רשמי לתפקיד מנהל אבטחת מידע בעירייה. בעקבות הערת הביקורת מסר גזבר העירייה כי הוא פועל להוצאת המינוי כנדרש.

לדעת הביקורת יש לעגן בהסכם עם חברת "מטרופולינט", קבלת עובד בעת היעדרות מנהל מערכות מידע בגין יציאה לחופשה, מחלה, מילואים או כל סיבה אחרת, על מנת שיוכל לשמש ממלא מקום מנהל מערכות המידע זאת מאחר ונמצא כי לא מונה עד כה ממלא מקום.

3. **רישום מאגרי המידע (פרק 3)**

בתקנות הגנת הפרטיות (אגרות), התשס"א-2000 ובנוהל "אבטחת מידע", קיימת חובת תשלום בגין אגרת הרישום וכן מפורטים ההליכים שינקטו במידה והאגרה לא תשלום במועדה או בכלל. הביקורת מעירה כי לא בוצע חידוש רישום ותשלום אגרה בגין מאגרי המידע מזה 9 שנים, דבר העלול לגרור קנסות בגין אי תשלום ואף שלילת רישום המאגר בפנקס הרשם.

4. **נהלים ומדיניות (פרק 4)**

הביקורת מעירה כי קיימים בעירייה 2 נהלים: נוהל אבטחת מידע בעירייה ו-נוהל גיבויים אולם הם טרם אושרו ע"י היועמ"ש והנהלת העירייה והם מפרטים חלקית בלבד את הפעולות שנדרשות לביצוע בנושאי אבטחת המידע.

לדעת הביקורת על מנהל מחלקת מערכות המידע להכין קובץ נהלים מפורט שיכלול בהרחבה את התחומים והדגשים בנוגע לאבטחת המידע במערכות המידע.

5. **תקציב (פרק 8)**

תקציב מחלקת המחשוב ואבטחת המידע הינו נגזרת מתקציב הגזברות. הביקורת מעירה כי מניתוח נתוני התקציב מול הביצוע לאורך השנים הנסקרות ניתן לראות שישנה חריגה מיעדי התקציב ואף מגמת עלייה בחריגה לאורך אותן השנים. מגזברות העירייה נמסר כי החריגות נבעו מתקלות לא צפויות, רכישת ציוד בלתי צפויה, תחזוקה מונעת.

הביקורת מעירה כי לא נערך מכרז בגין התקשרות עם חברת "אוטומציה" אשר מספקת תוכנה. יש לציין כי היקף ההתקשרות עולה על 142,000 ₪ (לא כולל מע"מ) היקף המחייב ביצוע מכרז. מגזברות העירייה נמסר כי מדובר בחוזה ישן שמתחדש מעת לעת. כלל יחידות העירייה מקבלות שירות מחברת "מטרופולינט" למעט מחלקת השכר שמקבלת שירות מחברת "אוטומציה" כך שההתקשרות של מחלקה זו עם החברה מתבצעת ללא מכרז וכך גם התשלום.

6. **שרידות ומערך גיבוי מערכות המידע (פרק 9)**

הביקורת מעירה כי חדר המחשב בו נמצא רובוט הגיבוי אינו מוגן מפני אש.

הביקורת מציינת, כי בעירייה קיימת תכנית מגירה לגיבוי שטרם מומשה, שרידות והתאוששות לאחר אירוע DRP. לדברי מנהל מערכות המידע עלות מימוש משוערת של התוכנית הינה 500 אלף ₪.

לדעת הביקורת יש למפות את רגישות המידע ולגבותו בהתאם, לקבוע נהלי התאוששות מאסון פוטנציאלי, לתרגל הנהלים ולעדכנם בהתאם לצורך.

7. **אבטחת מידע לוגית (פרק 10)**

הביקורת מעירה כי לא מתבצעות בדיקות יזומות של יומני האירועים במטרה לאתר אירועים חריגים ברשת.

הביקורת מצאה כי במחלקת משאבי אנוש (עפ"י דיווח העובדת) כאשר עובדת נעדרת מעבודתה, משתמשת העובדת שמחליפה אותה בסיסמה של העובדת שנעדרה ומעדכנת נתונים. לפיכך, הביקורת ממליצה לחדד את הנהלים וההנחיות בנוגע לשימוש בסיסמאות האישיות ואיסור מוחלט על העברתן לידי אדם אחר, לבצע הרחבת הנעילה האוטומטית לאחר זמן קצוב של אי שימוש לכלל עמדות העבודה בעירייה, בחינת חסימה מלאה של משתמשים לאתרי האינטרנט.

הביקורת מציינת כי ביום 28/5/2014 הועבר ריענון לעובדי עיריית קריית ביאליק ע"י מנהל מערכות המידע, המדגיש בפרק השני את כל נושאים שצוינו לעיל, ביניהם איסור גלישה באינטרנט באתרים שלא לצרכי עבודה, איסור הורדת תוכנות "חינם" מהאינטרנט או התקנת תוכנות/חומרות באופן עצמאי, כמו כן מודגש נושא הסיסמאות ואיסור העברתן מאדם לאדם, מודגש גם עניין נעילת תחנות העבודה ועוד נושאים נוספים שעלו בזמן הביקורת .

8. **<u>אבטחת מידע פיזית (פרק 11)</u>**

הביקורת מעירה כי חדר המחשב אינו מוגן מפני אש, דבר שמהווה בעיה מהותית במידה ותפרוץ שריפה בחדר המחשב. קלסרים ובתוכם מידע רגיש במרבית החדרים אינם נעולים בארונות, כמו כן ניירת המכילה מידע רגיש נותרת לעיתים על שולחנות העובדים ללא השגחה. בנוסף, ישנם עובדים אשר שומרים את סיסמאותיהם למחשב במקום חשוף או במקום אשר קל למצוא אותן ולהשתמש בהן.

הביקורת ממליצה למפות את כל משרדי העירייה ולבצע תכנית למיגון מפני אש וכן מפני פריצות (ע"י סורגים בחלונות בהם הם חסרים).

הביקורת מציינת כי ריענון ותקציר נהלי אבטחת מידע שנשלח לכלל העובדים ביום 28/5/2014, מדגיש את העלאת המודעות של המשתמשים גם בתחום אבטחת המידע הפיזית ועמידה בנהלים.

9. **<u>מערך ההרשאות (פרק 12)</u>**

הביקורת מעירה כי נושא ניהול המשתמשים (פתיחה, גריעה, הקצאה ושינוי הרשאות) מטופל לפי נוהג עבודה בלתי פורמאלי ואינו מעוגן באופן מפורט וברור בנהלי העירייה. יישום הרשאות גישה מתבצע באופן סלקטיבי לפי צרכי העובד והגדרות של מנהל המחלקה שלו ואין למנהל מערכות המידע רשימה מסודרת שלהן. בנוסף, הודעות על עובד שעזב או הועבר לתפקיד אחר ובקשות לביטולי ההרשאות לא מועברות אל מנהל מערכות המידע בזמן אמת, אלא רק לאחר שהעובד כבר עזב או מכהן בתפקיד אחר זמן מה.

הביקורת מציינת כי לספקים החיצוניים, הנותנים שירות למאגרי המידע, ישנן הרשאות מלאות לכל הקבצים והמידע בעירייה, עד כה הם לא היו חתומים על טפסי התחייבות על סודיות, אך במהלך הביקורת הוחתמו הספקים של חברת "מטרופולינט" על טפסים אלו.

לדעת הביקורת יש לבצע בחינה תקופתית וריענון של הרשאות משתמשים ברשת הפנימית.

10. **חברות חיצוניות (פרק 13)**

רוב המערכות המוניציפאליות מסופקות, מוטמעות בעירייה ומנוהלות על-ידי ספקית שירותי מחשוב חיצונית "חברת מטרופולינט בע"מ" וחברה חיצונית נוספת המספקת שרותי מחשוב לעירייה, חברת "אוטומציה".

הביקורת מעירה כי ישנו חוזה בין חברת "אוטומציה" לעירייה בגין העסקת עובד של האוטומציה במחלקת משאבי אנוש, אולם העירייה משלמת לחברה סכום כספי נוסף מעבר לתשלום בגין העסקת העובד.

עפ"י נהלי מחלקת התקציבים והחשבות כל התקשרות עם חברה חיצונית שהיקפה בין 142,000 ₪ ועד 347,000 ₪ מחייבת מכרז זוטא (כלומר קבלת הצעות מחיר מ-4 ספקים) כשבסופו של דבר, הזוכה יחתום על הסכם מול עיריית קריית ביאליק. היקף ההתקשרות של חברת אוטומציה הינו בין 259,000 ₪ ועד 349,999 ₪ אולם לא נחתם עמם הסכם עדכני למעט חתימה על ספחים.

הביקורת מעירה כי עפ"י סעיף 1.71 להסכם שנחתם עם חברת "מטרופולינט" על העירייה להחתים את עובדי החברה על התחייבויות לשמירת סודיות, אולם בפועל רק במהלך הביקורת עובדי חברת "מטרופולינט" הוחתמו על ההתחייבויות הנ"ל.

הביקורת מעירה כי לא מונה עובד עירייה כמתחייב עפ"י סעיף 3.4 לחוזה עם חברת "מטרופולינט".

הביקורת מציינת כי מנהל מערכות המידע הינו העובד היחיד במחלקה ואין לו כל מחליף.

הביקורת ממליצה לבצע בחינה של רמת אבטחת המידע והבקרה במערכות המנוהלות על יד חברת "מטרופולינט". בנוסף, מומלץ במועד חידוש החוזה לכלול בו סעיף המאפשר לעירייה לקיים ביקורת מערכות מידע ואבטחת מידע בכל הנוגע לתחומים הרלוונטיים למערכות התוכנה שבשימוש העירייה.

ביקורת בנושא אבטחת מידע במערכות המידע בעיריית קריית ביאליק

להלן הדו"ח המלא

1. **רקע כללי**

1.1. בעידן הנוכחי של הקדמה הטכנולוגית, מערכות המידע הממוחשבות מהוות חלק בלתי נפרד מפעילויות משרדי הממשלה מוסדותיה ורשויות על פי חוק.

1.2. מבחינת העירייה השימוש הנרחב במערכות המידע חשף אותה לסיכונים רבים ומצריך ביצוע בדיקות תקופתיות המוודאות את נכונות שלמות ודיוק המידע שנקלט במערכות, מופק מהן ומועבר בין מע' מידע שונות.

1.3. פגיעה בחיסיון המידע, בשלמותו או בשרידותו עלולה לגרום נזק לעירייה עצמה וגם לגורמים שפרטיהם כלולים במאגרי המידע שלה, ולפיכך, חלים על העירייה חוקים ותקנות הנוגעים לאבטחת המידע.

1.4. חוק הגנת הפרטיות התשמ"א -1981 נועד להגן על אדם מפני פגיעה בפרטיות העלולה להיגרם בין היתר ע"י חשיפת מידע כהגדרתו בחוק "נתונים על אישיותו של האדם, מעמדו האיש, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונותיו", ובכך מאפשרים באופן פשוט לנתח את אותם נתונים לרבות נתונים אישיים ולשלוף אותם בכל עת. לפיכך יש חשיבות רבה להיערך בצורה יסודית ומתאימה למניעת דליפת/חשיפת המידע למי שאינו מורשה לכך בחוק.

1.5. חוק המחשבים התשנ"ה -1995 הינו חוק הקובע את הענישה בגין "עבירות מחשב" כגון: שיבוש או הפרעה למחשב או לחומר ממוחשב, מידע כוזב או פלט כוזב, חדירה לחומר מחשב שלא כדין וכו'. החוק הנ"ל כולל בתוכו גם תיקונים לחוקים משפטיים אחרים כגון פקודת נזיקין, דיני ראיות, דיני חופש ותפיסה וכו'.

1.6. בשנת 2012 פורסמה טיוטת תקנות הגנת הפרטיות (אבטחת המידע) התשע"ב, התקנות נשענות בהגדרותיהן על חוק המחשבים התשנ"ה - 1995 ומגדירות את העובדים מטעם העירייה אשר יעסקו בעניין אבטחת המידע, ממונה על אבטחת המידע. על הממונה לקבוע את נהלי אבטחת המידע בהתאם לדרישת התקנות הנ"ל ומחייב את אותו אחראי למפות ולבצע סקרי סיכונים בנוגע למבנה מאגרי המידע שבארגונו. בנוסף, מגדיר אבטחה פיסית וסביבתית (כגון בקרות כניסה ויציאה) וכן מגדיר את אבטחת המידע בנוהל כח אדם, ניהול הרשאות גישה, זיהוי ואימות,

בקרה ותיעוד גישה, תיעוד של אירועי אבטחה, התקנים ניידים, ניהול מאובטח ומעודכן של מערכות המאגר, אבטחות תקשורת, מיקור חוץ, ביקורות תקופתיות וכו'.

2. **רקע ייחודי**

2.1. בעיריית קריית ביאליק קיימים כ-10 אתרים המבוזרים במשרדי העירייה, בכל משרד קיים לפחות מחשב נייח אחד. כל המחשבים מחוברים למערכת הממוחשבת העירונית המנוהלת ע"י מחלקת המחשוב ומערכות המידע (המערכות נרכשות מספק חיצוני ולא מפותחות בעירייה).

2.2. בעיריית קריית ביאליק פועלת מחלקת המחשוב ומערכות המידע שנמצאת באגף הכספים אותו מנהל גזבר העירייה. בראשה של המחלקה עומד מנהל מערכות מידע שהינו העובד היחידי ביחידה זו. מנהל מערכות המידע מועסק בהתאם לחוזה התקשרות עם חברת "מטרופולינט" ומועסק במשרה מלאה דרך חברה זו.

2.3. מאגרי המידע הקיימים בעירייה כגון: גביה, הנהלת חשבונות, רכש, חינוך, עיקולי בנקים, רווחה, שירות פסיכולוגי, שירותי וטרינריה, משאבי אנוש, פקוח עירוני וכו' הינם תחת ניהולה של המחלקה. תפקידה העיקרי של המחלקה הינו איתור וטיפול בתקלות וכן ניתוחן.

2.4. הטיפול בשרתים ובמערכות הליבה והחנייה כולל השירות הטכני ניתנים ע"י חברה חיצונית.

2.5. בימים אלו מערכות המידע משמשות תחליף כמעט מושלם, לכל המסמכים שעד ליום זה אוחסנו בקלסרים וארכיבים. מערכות המידע עוזרות לעירייה, הן במתן שירותים שונים לתושבים והן בביצוע העבודה השוטפת בצורה יעילה ומאורגנת.

3. **חוקים, הוראות ונהלים**

3.1. חוק יסוד כבוד האדם וחירותו.

3.2. חוק הגנת הפרטיות התשמ"א 1981.

3.3. חוק המחשבים, התשנ"ה – 1995.

3.4. חוק העונשין, התשל"ז-1977.

3.5. חוק הארכיונים, התשט"ו 1955.

3.6. חוק חופש המידע, התשנ"ח 1998.

3.7. תקנות הגנת הפרטיות (אגרות), התשס"א-2000.

3.8. תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו-1986.

3.9. תקנות הגנת הפרטיות, התשע"ב-2012.*

3.10. פקודת העיריות (נוסח חדש).

3.11. נהלים פנימיים של אגף המחשוב בעיריית קירית ביאליק.

* מדובר בטיוטה שפרסם משרד המשפטים ועברה מס' שלבים, כעת עומדת הטיוטה לפני אישור. הביקורת הסתמכה על טיוטה זו כ-GUIDE LINE לבדיקת התנהלות הממונה על אבטחת המידע בעיריית ק. ביאליק .

4. **<u>מטרת הביקורת -</u>**

4.1. איתור חריגות מחוקים, הוראות ונהלי עבודה.

4.2. איתור חריגות מסמכויות.

4.3. איתור סיכונים עסקיים ותפעוליים.

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

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

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

4.7. לבחון אם בעירית קריית ביאליק מערכות המידע מנוהלות ומתוחזקות בהתאם לעקרונות של חוקיות, יעילות, חסכון, סדירות, שוויון, שקיפות, מניעת פגיעה בטוהר המידות ואפקטיביות בהתאם להוראות החוקים והתקנות.

4.8. הביקורת בחנה את נושא אבטחת המידע במערכות המידע בעירייה, לרבות הנושאים הבאים: מבנה ארגוני ומינוי מנהל אבטחת מערכות מידע, פעילות המחלקה, רישום מאגרי המידע, נהלים ומדיניות, קיום מיפוי של מערך המחשוב, קיום סקרי סיכונים בנושא מערכות מידע, אבטחת המידע בצורה לוגית תוך כדי התייחסות לנושא נאותות המידע – שלמות, דיוק, זמינות, עקביות ותקפות. אבטחת המידע פיזית. מערך הרשאות. ניהול גיבויים (DB) ושרידות/המשכיות – היכולת להמשיך לתת שירותים והגנה על נכסי המידע. התקשרויות עם חברות חיצוניות בנושא המחשוב. תקציב, הערכת רמת הבקרה הפנימית בתהליכי העבודה הקשורים לאבטחת מערכות המחשב ולהמליץ על דרכים לתיקון הליקויים שנמצאו.

5. **היקף הביקורת ואופן הבדיקה**

5.1. במהלך החודשים נובמבר 2013 ועד אוקטובר 2014 התבצעה ביקורת בעיריית קריית ביאליק במחלקת המחשוב ומערכות המידע, בנושא אבטחת מידע במערכות המידע. הביקורת בחנה את מערך אבטחת המידע בעיריית קריית ביאליק בתקופה שבין השנים 2010-2012.

5.2. הביקורת בוצעה בהתאם לתוכנית העבודה של מבקר העירייה לשנת 2014. הנושא נכלל בתוכנית העבודה השנתית, בשל הסיכונים האפשריים בתחומו היכולים להשפיע על כלל העירייה הן מבחינה כלכלית והן מבחינת יכולת התנהלותה הכללית.

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

5.4. הביקורת בוצעה ע״י גב׳ אורטל אדראי וגב׳ אורלי אביטן בורוש סטודנטיות לביקורת באוניברסיטת חיפה וע״י מר אייל לוי, המבקר הפנימי.

5.5. **לצורך ביצוע המטלה, הביקורת קיבלה נתונים:**

5.5.1. ממחלקת המחשוב ומערכות המידע.

5.5.2. מספרי הנהלת החשבונות של הרשות לגבי הנתונים הכספיים של מחלקת המחשוב.

5.5.3. בנוסף, הביקורת הוציאה וניתחה נתונים שונים מתוך המערכת הממוחשבת.

5.5.4. נתוני חוזים והתקשרויות בנושא המחשוב ואבטחתו עם גורמי חוץ.

5.5.5. נתונים מפרוטוקולים והתכתבויות בנושא אבטחת מערכות המחשוב.

להלן ממצאי הביקורת

1. מבנה ארגוני- מחלקת המחשוב

1.1. סעיף 17 לחוק הגנת הפרטיות, התשמ"א – 1981, קובע את החובה למנות ממונה על אבטחת המידע שיהיה אחראי בפועל על אבטחת המידע במאגרים להלן ציטוט מהחוק:

" בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע".

1.2. סעיף 17ב. (תיקון: תשנ"ו) לחוק הנ"למגדיר את הגופים המחויבים במינוי ממונה על אבטחת המידע, להלן החוק כלשונו:

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

(1) מחזיק בחמישה מאגרי מידע החייבים ברישום לפי סעיף 8;

(2) גוף ציבורי כהגדרתו בסעיף 23;

(3) בנק, חברת ביטוח, חברה העוסקת בדירוג או בהערכה של אשראי.

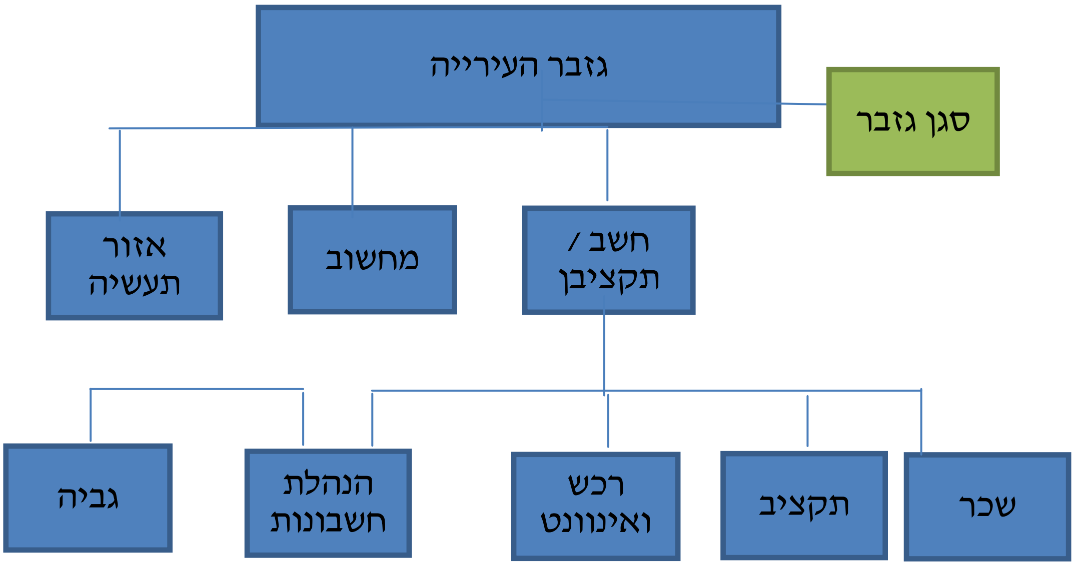
(ב) בלי לגרוע מהוראות סעיף 17, הממונה יהיה אחראי לאבטחת המידע במאגרים המוחזקים ברשות הגופים כאמור בסעיף קטן (א).

(ג) לא ימונה כממונה מי שהורשע בעבירה שיש עמה קלון או בעבירה על הוראות חוק זה".

סעיף 23(1) לחוק הנ"ל מגדיר את הגופים הציבוריים החייבים במינוי ממונה אבטחת מידע:

"גוף ציבורי" -(1) משרדי הממשלה ומוסדות מדינה אחרים, רשות מקומית וגוף אחר הממלא תפקידים ציבוריים על פי דין...

1.3. **המבנה הארגוני של המחלקה:**



1.4. מחלקת המחשוב ומערכות המידע מתנהלת תחת אגף הכספים בניהולו של גזבר העירייה.

1.5. מערכת המחשוב בעירייה בנויה בתצורת כוכב. כל המחשבים מחוברים לעירייה בחיבורי RG45 תקניים תקן CAT7E. המחשבים שממוקמים במבנים אחרים מחוברים לרשת העירונית, חלקם באמצעות סיבים אופטיים חלקם באמצעות כבל נחושת. בכל בניין יש ריכוז תקשורת עצמאי המחובר לארון תקשורת מרכזי בבניין העירייה. לכל ארון תקשורת פרוס כבל המיוצג ע"י PATCH PANEL לצרכי טלפוניה אחודה. מחוץ לבניין העירייה, הוקמה רשת VPDN ובאמצעות ראוטרים של חברת סיסקו, הם יוצאים לעולם האינטרנט עם הפניות מתאימות לעירייה לצרכי מיילים וקבצי נתונים בלבד. ישנם מספר שרתים מרכזיים בארגון. כל הרשת נמצאת על AD אחד.

1.6. בעיריית קריית ביאליק מחלקת המחשוב ומערכות המידע כוללת אדם אחד בלבד אשר אחראי על כל מערך המחשוב ואבטחתו בעירייה, תפקידו מוגדר כמנהל מערכות המידע. מנהל מערכות המידע הינו עובד Outsourcing אשר מועסק במשרה מלאה ע"י חברת "מטרופולינט" המספקת את שירותי המחשוב לעירייה. מנהל מערכות המידע מכהן 9 שנים בתפקידו.

1.7. **הביקורת מעירה כי מנהל מערכות המידע לא מונה באופן רשמי לתפקיד מנהל אבטחת מידע בעירייה.**

1.8. **בעקבות הערת הביקורת מסר גזבר העירייה כי הוא פועל להוצאת המינוי כנדרש.**

1.9. **הביקורת ממליצה לעגן בהסכם עם חברת "מטרופולינט", קבלת עובד בעת היעדרות מנהל מערכות המידע בגין חופשה, מחלה, מילואים או כל סיבה אחרת, על מנת שיוכל לשמש ממלא מקום מנהל מערכות המידע זאת מאחר ונמצא כי לא מונה עד כה ממלא מקום.**

1.10. **במקרה של היעדרותו של מנהל מערכות המידע ישנה חשיבות לקיומה של רוטציה בעיקר בשל הצורך לתת מענה למחלקות העוסקות בתחומי הליבה של העירייה בזמן אמת.**

2. <u>פעילות מחלקת המחשוב ומערכות המידע</u>

מאתר האינטרנט של עיריית קריית ביאליק עולה כי תפקידי המחלקה הם:

2.1. **ניתוח מערכות מידע** –תפקיד ניתוח המערכות לאפיין את צרכי המשתמשים ולתכנן את הפתרון, להציע מערכות מדף מתאימות או לפתח מערכת, להטמיע את המערכת ושוב לבחון את הצורך בשיפור וייעול.

2.2. **תשתיות המחשוב** –בדיקת היתכנות תשתיתית, התקנה וחידוש חומרה ותוכנה.

2.3. **תקשורת וטלפוניה**– אחזקה שוטפת של מרכזיות העירייה הכוללות כ – 200 שלוחות וכ – 200 קווים. קשר עם חברות נותנות שירותים כגון: תדיראן תקשורת, בזק ובזק בינלאומי כולל הפעלת הטכנאים של חברות אלה. תמיכה באחזקת מרכזות יחידות העירייה שאינן מחוברות למרכזת הראשית, קווי טלפון שאינם מחוברים למרכזיות כלשהן וקווי נתונים כמו fram-realy סיפרנט ונל"נים. מעקב שוטף אחר החידושים בשוק התקשורת , להגדלות ושדרוג ציוד ותוכנות. תכנון וביצוע הגדלות ושדרוג ציוד ותוכנות. הפקת מדריך הטלפון של העירייה ופרסומים ביומן השנה ומדריך הטלפון של בזק.

2.4. **תמיכה ואחזקת מוסדות חינוך** - פתרון תקלות בכל מוסדות החינוך בעיר הכוללים בתי ספר, גני ילדים ועוד.

2.5. **אבטחת מערכות המידע.**

3. רישום מאגרי מידע

3.1. חוק הגנת הפרטיות, התשמ"א – 1981 (להלן: "החוק") הינו הבסיס החוקי לכל הקשור למאגרי מידע, שמירה עליהם ודרך ניהולם.

3.2. סעיף 8 לחוק קובע את החובה שלא להחזיק מאגר נתונים אלא לאחר שהוגשה בקשה לרישום המאגר, והמאגר נרשם ע"פ חוק. סעיף 9 (ב) לחוק קובע מה תכלול הבקשה לרישום מאגר מידע :

(ב) בקשה לרישום מאגר מידע תפרט את -

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

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

(3) סוגי המידע שייכללו במאגר;

(4) פרטים בדבר העברת מידע מחוץ לגבולות המדינה;

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

3.3. בתקנות הגנת הפרטיות (אגרות), התשס"א-2000, קיימת חובת תשלום בגין אגרת הרישום וכן מפורטים ההליכים שינקטו במידה והאגרה לא תשלום במועדה או בכלל:

2. אגרות רישום

בעד רישום מאגר מידע בפנקס יגבה הרשם אגרה בסכום של 200 שקלים חדשים.

3. אגרה תקופתית

(א) הרשם יגבה אגרה תקופתית, לתקופה של שנה, בעבור מאגר מידע הרשום בפנקס, למעט מאגר מידע שבבעלות המדינה...

(ג) האגרה התקופתית תשולם לא יאוחר מ-1 במרס של כל שנה (להלן - מועד התשלום).

4. אי תשלום אגרה במועד

(א) לא שולמה האגרה התקופתית במועד התשלום, היא תשולם עם תוספת אגרה .....

(ב) לא שולמה האגרה התקופתית או תוספת האגרה בתוך שישה חודשים מן המועד האחרון לתשלום תוספת האגרה, יותלה רישומו של מאגר המידע בפנקס כאמור בסעיף 36א(ג) לחוק, והודעה על כך ימסור הרשם לבעל המאגר ולמחזיקו, לפי הרשום בפנקס.

3.4. בעירייה קיים נוהל "אבטחת מידע" (הנוהל טרם אושר סופית ע"י הנהלת העירייה והיועמ"ש) כאשר בסעיף 5.3 לנוהל מודגשת חובת

רישום המאגרים במשרד המשפטים שהינה באחריות מנכ"ל העירייה ומנהל מערכות המידע:

" 5.3.1 כל מאגרי המידע בעירייה מחויבים ברישום ב"פנקס מאגרי המידע" שבמשרד המשפטים, באחריות מנכ"ל העירייה ובאמצעות אחראי המחשוב".

3.5. **הביקורת מעירה כי לא בוצע חידוש רישום ותשלום אגרה בגין מאגרי המידע מזה 9 שנים, דבר העלול לגרור קנסות בגין אי תשלום ואף שלילת רישום המאגר בפנקס הרשם.**

בתגובה לממצאי הדו"ח נמסר לביקורת כי חידוש רישום ותשלום האגרה יבוצע במהלך שנת 2015.

4. **נהלים ומדיניות**

4.1. הגדרת מדיניות אבטחת מידע איננה פעולה חד פעמית של כתיבת מסמך, אלא תהליך מתמשך ומתחדש בהתאם לאיומים וסיכונים. מדיניות אבטחת המידע כוללת: קווי מדיניות, סטנדרטים, הנחיות ונהלים, כללי גישה והרשאות, סיווג מידע לפי רגישותו ועוד.

4.2. על המדיניות להיות מתועדת במסמך שיופץ בכל הארגון וישמש כבסיס לפיתוח בקרות אבטחת מידע ולכתיבת נהלי אבטחת מידע.

4.3. בתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו-1986, בפרק ב' מופיעה תקנה 3(ב)(2)-(3) **המפרטת את אחריות מנהל המאגר** :

3 (ב) מנהל מאגר אחראי לאבטחת המידע במאגר המידע שעליו הוא מופקד ובכלל זה בתחומים אלה:

*(2) **קביעת סדרי ניהול של מאגר מידע, וכללים** להרשאת גישה למידע, לאיסוף, לסימון, לאימות, לעיבוד ולהפצה של המידע, הכל בהתאם להוראות החוק והתקנות; **סדרים וכללים כאמור יחולו גם על נותן שירותים חיצוני לגוף שבבעלותו מאגר המידע;***

(3) קיום הוראות תפעול של המערכת תוך אבטחת המידע ושמירה על שלמות המידע;

בנוסף בפרק ד' לתקנות הנ"ל מופיע סעיף מס' 9 המחייב הכנת קובץ נהלים להלן התקנה:

*" **למאגר מידע,** כאמור בתקנה 8, **יהיה קובץ נהלים שבו יפורטו אמצעי האבטחה והבקרה על הטיפול הפיסי באמצעי האחסון של המידע. בקובץ ייוחד פרק לטיפול במידע בידי נותן שירותים חיצוני המבצע עבודות עבור המאגר בתחומי הקלידה, עיבוד הנתונים, הפצת דו"חות והובלת קבצים".***

4.4. **הביקורת מעירה כי קיימים בעירייה 2 נהלים: נוהל אבטחת מידע בעירייה ונוהל גיבויים אולם הם טרם אושרו ע"י היועמ"ש והנהלת העירייה והם מפרטים חלקית בלבד את הפעולות שנדרשות לביצוע בנושאי אבטחת המידע.**

4.5. **הביקורת ממליצה כי מנהל מערכות מידע יכין קובץ נהלים שיכלול את הנושאים הבאים:**

4.5.1. נוהל מפורט בנוגע לכניסת עובדים למערכות המידע.

4.5.2. נוהל מפורט לגבי מתן סיסמאות ו/או חסימתן (ראה נושא זה בהרחבה בסעיף 12.3 לדו"ח זה).

4.5.3. נוהל מפורט לביצוע ניתוח סיכונים.

4.5.4. נוהל אזהרה בגין הפרת סודיות.

4.5.5. נוהל מפורט של אבטחת מידע לגבי כניסת קבלנים ועובדי חוץ למערכות המידע.

4.5.6. נוהל התקנת תוכנות במחשבים ע"י המשתמשים.

4.5.7. נוהל מפורט בנוגע לשימוש בחומרה אשר הובאה מחוץ לארגון.

4.5.8. נוהל מפורט בנוגע להורדות מרשת האינטרנט.

4.5.9. נוהל מפורט בנוגע לשימוש בדואר אלקטרוני.

4.5.10. נוהל קבלת עובד הכולל הצהרת סודיות, הצהרה בדבר קבלת ציוד וכו', וכן נוהל זהה בנוגע לפרישה או עזיבת עובד. דבר המשפיע באופן ישיר על האבטחה הפיזית והלוגית שיורחבו בהמשך (סעיפים 11 ו-12).

4.6. יצוין כי בעקבות הערת הביקורת בתאריך 28 למאי 2014 הוצאו הנחיות וריענון נהלי אבטחת מידע לעובדים הנוגעים באופן ישיר לנושאים שהועלו בביקורת (ראה סעיפים 10-11 לדו"ח ביקורת זה) . למרות האמור לעיל, ההנחיות הנ"ל אינן מכסות את כל נושא אבטחת המידע ואינן מהוות תחליף למדיניות אבטחת מידע מפורטת יותר ונהלים נפרדים לכל נושא.

4.7. **הביקורת ממליצה לקיים הדרכה לעובדים חדשים בתחום אבטחת מידע.**

בתגובה לממצאי הדו"ח נמסר לביקורת כי תתקיים הדרכה לעובדים במהלך שנת 2015.

5. <u>קיום מיפוי של מערך המחשוב</u>

5.1. מנתונים שהתקבלו ממחלקת המחשוב עולה כי קיים מיפוי חלקי בלבד של מערך המחשוב בעירייה לשנת 2013 ולא קיימים מיפויים לשנים 2010-2012, להלן המיפוי לשנת 2013 :

5.1.1. 180 מחשבים נייחים.

5.1.2. כ-8 מחשבים ניידים.

5.1.3. 12 שרתים.

5.1.4. תוכנת גיבוי אחת.

5.2. יש לציין כי תקנה מס׳ 5(א) בטיוטת תקנות הגנת הפרטיות (אבטחת מידע), התשע״ב-2012, מפרטת את חובת המיפוי של מאגרי המידע :

(א) בעל מאגר מידע יחזיק מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי מעודכנת של מכלול רכיבי המערכות המשמשות את המאגר (להלן – מערכות
המאגר), ובכלל זה -
(1) תשתיות ומערכות חומרה, רכיבי תקשורת ואבטחת מידע, לרבות ציון של מיקומם הפיזי ;
(2) מערכות התוכנה המשמשות להפעלת מאגר המידע, לניהול המאגר ולתחזוקתו, לתמיכה בפעילותו, לניטור שלו ולאבטחתו ;
(3) תוכנות וממשקים המשמשים לתקשורת אל מערכות המאגר ומהן ;
(4) תיאור מבנה הרשת שבה פועל המאגר ותיאור של הקשרים בין מרכיבי המערכת השונים ;
(5) תאריך עדכון אחרון של המסמך ושל הרשימה.

5.3. **הביקורת ממליצה כי מנהל מערכות המידע יאמץ כבר עתה את התקנות המופיעות לעיל ויפעל בהתאם אליהן, זאת על מנת להשיג האפשרות לשליטה על כמויות המחשבים, שרתים, החומרות, התוכנות ומיקומן ביחידות/מחלקות השונות בעירייה שכן, המערכות הללו הן בתחום אחריותו של מנהל מערכות המידע.**

מנהל מערכות המידע מסר כי הוא אימץ את התקנות החדשות והחל לפעול על פיהם

6. **ביצוע סקר סיכונים בנושא מערכות מידע ממוחשבות**

6.1. מערכות אבטחת מידע אמורות להתבסס על הנחות יסוד המגדירות איומים, נקודות חולשה ונקודות חוזק במערכת. הנהלת העירייה אחראית לנקוט בפעולות מניעה אשר יש בהן כדי לזהות את הסיכונים/איומים הקיימים ולהפחית משמעותית את החשיפה להם. אחת מפעולות המניעה החשובות בנושא זה היא **עריכת סקר סיכונים** (Risk Analysis) בנושא אבטחת מידע. מתפקידו של הממונה על אבטחת מידע לדאוג לעריכת סקר הסיכונים ולבצע שינויים משמעותיים בהתאם לממצאי הסקר. סקר סיכונים מקיף ישיג את היעדים הבאים: איתור סיכונים ואיומים להם חשופה מערכת המחשב, זיהוי מערכות המידע הרגישות בעירייה, הצגת הסיכונים שנמצאו עפ"י משקלם היחסי, הצגת הפעולות המתקנות שיאפשרו את הקטנת הסיכונים.

6.2. **הביקורת מצאה כי בשנים 2010-2012 לא בוצע כל סקר סיכונים.**

6.3. יש לציין כי תקנה מס' 5 (ב) ו-(ג) בטיוטת תקנות הגנת הפרטיות (אבטחת מידע), התשע"ב-2012 מפרטת את חובת ביצוע סקר הסיכונים. כמפורט להלן:

"5(ב) במאגר מידע שחלה עליו רמת האבטחה הגבוהה ,בעל המאגר אחראי לכך שייערך סקר בלתי תלוי לאיתור סיכוני אבטחת מידע ומבדקי חדירות (להלן – סקר סיכונים) בהתאם לשיטה מקובלת; תוצאות סקר הסיכונים יועברו לבעל המאגר, אשר ידון בהם ויבחן את הצורך בעדכון הגדרות המאגר או נוהל האבטחה בעקבותיהן , ויפעל לתיקון הליקויים שנתגלו במסגרת הסקר ,ככל שנתגלו .

(ג) רשימת מצאי וסקר סיכונים ייערכו אחת לשמונה עשר חודשים לפחות".

6.4. **הביקורת ממליצה לאמץ כבר עתה את התקנה המופיעה לעיל ולדאוג לעריכת סקר כולל לכל מערך המחשוב, כדי לאתר את הסיכונים להם חשופה המערכת וליקויים נוספים במידה וקיימים. לשם עריכת הסקר מומלץ לפנות לגורם המוסמך לכך.**

הביקורת מציינת כי עד כה טרם בוצע סקר הסיכונים בשל עלויות כספיות גבוהות.

7. <u>פיקוח ובקרה על מחלקת המחשוב ומערכות מידע</u>

7.1. הבקרות משמשות ככלי לפיקוח על התקנה ועדכון של רכיבי חומרה ותוכנה על מנת להבטיח כי המערכת תפעל כמצופה ממנה ולא תגרם לה פגיעה עקב עדכונים.

7.2. יש לציין כי תקנה מס' 16 בטיוטת תקנות הגנת הפרטיות (אבטחת מידע), התשע"ב-2012, מחייבת ביקורות תקופתיות ומפרטת את התהליך:

(א) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, תיערך פעם בשנתיים לפחות, ביקורת פנימית או חיצונית, על ידי גורם בעל הכשרה מתאימה לביקורת בנושא אבטחת מידע, שתוודא את עמידתו בהוראות תקנות אלה.

(ב) אם נערכת ביקורת פנימית, לא יהיה המבקר מי שנושא בתפקיד ממונה אבטחה של המאגר.

(ג) דו"ח הביקורת ידוות על התאמת אמצעי האבטחה לנוהל האבטחה ולתקנות אלה, יזהה ליקויים ויציע אמצעים הדרושים לתיקון המצב, ויסתמך גם על ממצאים ממערכות המחשוב של בעל המאגר.

(ד) דוחות הביקורת יועברו לבעל המאגר, אשר ידון בהם ויבחן את הצורך בעדכון הגדרות המאגר או נוהל האבטחה בעקבותיהם.

7.3. **הביקורת ממליצה לאמץ התקנה המופיעה לעיל כבר עתה ולפעול בהתאם למפורט בה.**

7.4. **הביקורת ממליצה לנהל מנגנון תיעוד אוטומטי שיאפשר בקרה וביקורת הגישה למערכות המאגר (ראה נושא זה בהרחבה בסעיף 12).**

8. **<u>תקציב</u>**

מהנתונים שהתקבלו מאגף הכספים עולה כי:

8.1. תקציב מחלקת המחשוב ואבטחת המידע הינו נגזרת של תקציב הגזברות.

8.2. להלן טבלה המרכזת את התקציב מול הביצוע של מחלקת המחשוב ואבטחת המידע במהלך השנים 2010-2012:

<u>תקציב וביצוע לפי שנה</u>

שנה	מספר כרטיס	שם כרטיס	תקציב	ביצוע	חריגה
2012	1621100570	גזברות - מיכון	775,000	954,259	-179,259
	1913000570	מים - הוצאות מיכון	312,500	312,500	0
	1972000570	ביוב - הוצאות מיכון	312,500	312,500	0
	סה"כ		**1,400,000**	**1,579,259**	**-179,259**
2011	1621100570	גזברות - מיכון	1,000,000	1,130,122	-130,122
	1913000570	מים - הוצאות מיכון	312,500	312,500	0
	1972000570	ביוב - הוצאות מיכון	312,500	312,500	0
	סה"כ		**1,625,000**	**1,755,122**	-130,122
2010	1621100570	גזברות - מיכון	725,000	783,748	-58,748
	1913000570	מים - הוצאות מיכון	312,500	312,500	0
	1972000570	ביוב - הוצאות מיכון	312,500	312,500	0
	סה"כ		**1,350,000**	**1,408,748**	-58,748

כרטסת מס' 1621100570

חו"ז ספק	שם ספק	2010	2011	2012	סך, ₪
6001308900	מדיאטק בע"מ	5289	0	6902	12191
6000283000	בזק בינלאומי	113105.52	110222.8	121638.89	344967.21
6001309300	מטרופולי-נט בע"מ	892313.61	888010.51	904401.88	2684726
6000807000	חברה לאוטומציה	259929.48	349983.92	296657.12	906570.52
6001061000	יורוסוניק	5124.88	0	0	5124.88
6001900010	קיו.אי.אס.בע"מ	127476	109055	146770	383301
6001558800	סופט מאסטר בע"מ	2900	6252.4	15486	24638.4
6002049000	ראש פסגה בע"מ	2610	0	0	2610
6001434000	נאות מחשבים	0	11596	9367	20963
6001310100	מלם-תים בע"מ	0	1096.2	0	1096.2
6000106210	אם.פי.אל. מערכות לניהול	0	11053	0	11053
6002155110	שמרת מחשבים	0	250	0	250
6001576000	סינאל מלל פיוויי בע"מ	0	42166	0	42166
6000870000	חשבים ה.פ.ס מידע עסקי בע"מ	0	5290	0	5290
6001369000	מסייג'נט בע"מ	0	10026	0	10026
6000300200	גל מד בע"מ	0	1786.4	0	1786.4
6000102120	אלון ק.מיזוג אויר בע"מ	0	0	4698	4698
6001306910	ממטל מערכות וטכנולוגיה לתשתית......	0	0	30032.4	30032.4
6002255100	תדיראן טלקום-מערכות	0	0	22069.22	22069.22
6001508000	סינאל תעשיות בע"מ	0	0	21235.57	21235.57
סך, ₪		1408748.49	1546788.23	1579258.08	4534794.8
העמסת עלויות מיכון		-625000	-416666	-625000	-1666666
סך יתרה, ₪		783748.49	1130122.23	954258.08	2868128.8

8.3. **יש לציין כי הוצאות המיכון של המים והביוב הינן חיוב רישומי של תאגיד המים שטרם הוקם.**

8.4. **הביקורת מעירה כי מניתוח נתוני התקציב מול הביצוע לאורך השנים הנסקרות ניתן לראות שישנה חריגה מיעדי התקציב ואף מגמת עלייה בחריגה לאורך אותן השנים.**

8.5. **מגזברות העירייה נמסר כי החריגות נבעו מתקלות לא צפויות, רכישת ציוד בלתי צפויה ותחזוקה מונעת.**

8.6. **יש לציין כי רכישת מחשבים וציוד נלווה מתבצעת ע"י המחלקות השונות מתקציביהן.**

8.7. **מכרטסת הספקים עולה כי קיימת התקשרות עם חברת "אוטומציה" לשם אספקת תוכנה וסך ההתקשרות לשנה עולה על 142,000 ₪ + מע"מ. מבדיקתנו עולה כי לא נערך מכרז בגין התקשרות זו. (ראה הרחבה בנושא בסעיף 13 לדו"ח זה).**

8.8. **מגזברות העירייה נמסר כי מדובר בחוזה ישן שמתחדש מעת לעת. חברת "אוטומציה" הוחלפה כספק תוכנה וכעת נותנת השירות בתחום הינה חברת "מטרופולינט". כלל יחידות העירייה מקבלות שירות מחברת "מטרופולינט" למעט מחלקת השכר כך שההתקשרות של מחלקה זו עם חברת אוטומציה מתבצעת ללא מכרז וכך גם התשלום.**

8.9. **הביקורת ממליצה כי נושא אבטחת המידע בעיריית קריית ביאליק יהיה מתוקצב באופן נפרד מתקציב מחלקת המחשוב, מאחר ולצורך ביצוע עבודתו של הממונה על אבטחת המידע בצורה נאותה ומספקת, עליו לקבל המשאבים הנדרשים לכך. תקציב נפרד יאפשר לממונה על אבטחת מידע להקצות משאבים להגנת המערכת שלא על חשבון החומרה.**

9. **שרידות ומערך גיבוי מערכות המידע**

9.1. תהליך האבטחה כולל שמירת גיבוי של המידע לפני השינויים ואחריהם, על מנת לאפשר שחזור של המידע במקרה של כשל. מערכת הגיבויים נועדה לאפשר התאוששות ממצב בלתי צפוי של קריסת שרתים ואבדן מידע, הן כתוצאה של פעולה בזדון, בשגגה, או כתוצאה מכשל מערכתי.

9.2. לפיכך, במערכות המידע ישנו צורך במערכת גיבויים יעילה שתאפשר אחזור הנתונים שאבדו וכך ימנע נזק לארגון. בנוסף, יש צורך בתכנית חלופית כדי להתמודד עם מצבים לא מתוכננים כמו פגיעה מווירוס או אפילו אסון טבע שהרס את מתקני האחסון.

9.3. בעיריית קריית ביאליק ישנו נוהל בנוגע לגיבויים. הנוהל חל על מנהל מערכות המידע ועל נציגו במידה שימונה ע"י מנכ"ל העירייה או הגזבר. הנוהל מגדיר את תהליך הגיבויים בעירייה, על אחראי הגיבויים הווה אומר מנהל מערכות המידע להחזיק 2 סטים של קלטות גיבוי, לאחסן את

הקלטת האחרונה לחודש בכספת נפרדת, להחזיק קלטת ניקוי לכל טייפ

ובמקרה של תקלה לאבחן את הסיבה ולטפל בה.

9.4. תכנת הגיבוי בה משתמשת העירייה הינה BACKUPEXEC.

9.5. קיים בעירייה נוהל גיבויים אשר טרם אושר סופית ע"י הנהלת העירייה והיועמ"ש להלן לשון הנוהל:

"5.2.ביצוע גיבוי

5.2.2 תזמון פעולת הגיבוי יתוכנן לסוף יום העבודה כשכל המשתמשים אינם (מאחר שפעולת הגיבוי צורכת משאבי רשת), זאת במטרה לאפשר גיבוי כל הקבצים הסגורים כמו גם למנוע הפרעות למהלך העבודה הסדיר. הגדרה מיוחדת תינתן לשרתים אותם יש צורך לגבות במהלך שעות העבודה.

5.2.3 הטיפול בגיבויים על ידי אחראי גיבויים בעירייה/ תאגיד כולל את סדר הפעולות הבא:

1) ווידוי תקינות הגיבוי מהלילה הקודם ע"י בדיקת LOG בתוכנת ה-BACKUPEXEC...

2) כל קלטות הגיבוי נמצאות ברובוט הגיבוי .על אחראי המחשוב לוודא תקינות

הקלטות ושהגיבוי בוצע כהלכה.

3) ווידוא שהכונן קורא את הקלטת(יש לוודא שהקלטת לא נפלטת החוצה.)

5.2.4. יש להעביר קלטות ולאחסנם לא רק בכספת הארגון אלא גם בכספת הנמצאת במקום פיזי אחר. תאגידי העירייה יאחסנו אחת לשבועיים קלטות בעירייה, והעירייה תאחסן אחת לשבועיים קלטות בכספת העירייה."

9.6. בעירייה ישנן 7 קלטות ברובוט גיבוי שבחדר המחשב. אחת לשבוע נשמרת קלטת אחת במקום אחר מוגן מאש ופריצה בכספת (שבמחלקת הגזברות הנמצאת בבניין אחר). מתבצעים גיבויים שוטפים יומיים שבועיים וחודשיים. חלק מהמערכות נמצאות בענן ביניהן מערכת הגביה, הנהלת חשבונות, רווחה ומוקד והן מגובות ע"י נוהל מסודר ולפי הסכם בחברה חיצונית.

9.7. **הביקורת מעירה כי חדר המחשב בו נמצא רובוט הגיבוי אינו מוגן מפני אש (ראה ממצא שפורט בהרחבה בנושא 11.7 לדו"ח זה).**

9.8. **הביקורת מציינת בנוסף, כי בעירייה קיימת תכנית מגירה לגיבוי שטרם מומשה, שרידות והתאוששות לאחר אירוע DRP. לדברי מנהל מערכות המידע עלות מימוש משוערת של התוכנית הינה 500 אלף ₪.**

9.9. **הביקורת ממליצה למפות את המידע עפ"י מידת רגישותו ולגבותו בהתאם לכך.**

9.10. **הביקורת ממליצה לקבוע נהלי התאוששות, בנוסף לתכנית המגירה DRP שקיימת בארגון, בהתאם למצוין בטיוטת תקנות הגנת הפרטיות (אבטחת מידע), התשע"ב-2012 תקנה מס' 17(א)(2):**

"במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יקבע בעל המאגר - נהלי התאוששות, כדי להבטיח שבכל עת ניתן יהיה לשחזר את המידע האמור בתקנה (1) למצבו המקורי ובלבד שביצוע השחזור יהיה באישור מנהל המאגר".

מומלץ לתרגל נהלים אלו ולעדכנם מעת לעת. זאת כדי להבטיח את היכולת לשחזר מידע בכל עת למצבו המקורי, ובכך להבטיח את שלמות המידע במקרה של אובדן או הרס.

בתגובה לממצאי הדו"ח נמסר לביקורת כי בשנת התקציב 2015, נלקח בחשבון הקמת אתר DRP.

10. <u>אבטחת מידע לוגית</u>

10.1. שלמות המידע הינה מרכיב מהותי באבטחת מידע. אבטחה לוגית, פירושה-האמצעים והנהלים הדרושים להגנה על מאגרי המידע ועל משאבי המידע, כגון: זיהוי המשתמשים באמצעות סיסמאות, מעקב ותיעוד הפעולות שמבוצעות במערכת, הטמעת מערכת תכנה וחומרה לגילוי ומניעת חדירת וירוס, בקרות על שלמות המידע ואמינותו, טיפול באירועים חריגים ועוד.

10.2. באמצעות הבקרות המיושמות על הגישה הלוגית, ניתן לדעת את זהות המשתמש שניגש למשאב מסוים במערכת ואילו פעולות הוא ביצע באותו משאב. האבטחה הלוגית משמשת את מנהלי מערכת האבטחה בסינון גישתם של המשתמשים לכלל המידע המצוי במערכת.

10.3. תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו-1986, פרק ב' תקנה מס' 3 מפרטת את תחומי אחריותו של מנהל מאגרי המידע (בעיריית קריית ביאליק זהו מנהל מערכות המידע). עפ"י סעיפים (3) (4) (5) ו-(15) בין תחומי האחריות קיימים גם:

(3)"קיום הוראות תפעול של המערכת תוך אבטחת המידע ושמירה על שלימות המידע;

(4) נקיטת אמצעי אבטחה סבירים, בהתאם לרמת רגישות המידע, שימנעו חדירה מכוונת או מקרית למערכת אל מעבר לתחומי המידע שאושרו למשתמש;

(5)"קביעת סדרי בקרה לגילוי פגיעות בשלימות המידע ותיקון ליקויים".

תקנות אלה מפרטות גם בתקנה מס' 15 את <u>החובה לניהול יומן אירועים חריגים</u>: *"(א) יומן אירועים חריגים (להלן - **היומן**) ינוהל בידי מנהל המאגר על גבי אמצעי נתיק מן המערכת לגבי פעולות הפקת מידע באצווה או פעולות תשאול שבוצעו במסוף הקשור למערכת; היומן יישמר במשך שלוש שנים; לגבי אירוע חריג יירשמו ביומן פרטי הזיהוי של הפונה, סוג השאילתה, הרשומות או סוגי הרשומות שהופקו בתשובה.*

(ב) מנהל המאגר אחראי לעריכת בדיקת חודשית של היומן, לצורך תיקון ליקויים".

10.4. קיים בעירייה נוהל אבטחת מידע אשר טרם אושר סופית ע"י הנהלת העירייה והיועמ"ש להלן סעיפי הנוהל בהם ישנה התייחסות לנושא אבטחת המידע הלוגית:

"5.1.5. בנוגע למידע ממוחשב, באחריות אחראי המחשוב:

1) לקיים מערכת אבטחת מידע בכל הרמות בעירייה כנגד חדירה חיצונית.

2) לדאוג לשלמות המידע, זמינותו וגיבויו.

3) לדאוג לחיסיון המידע.

4) לתת הרשאות למשתמשים בהתאם לצרכים.

5) הסרת הרשאות לעובד שנויד בתוך המערכת או לעובד שסיים את עבודתו בעירייה – יתואם בין אחראי מחשוב למנהל משאבי אנוש.

10.5. הביקורת מציינת כי קיימת בארגון תכנת אנטי וירוס מגרסה ESET NODE 32 4.2.76.0 לכל המחשבים, כמו כן קיימות מערכות הגנה "SPAM", "FIREWAL" מאובטחות ומעת לעת משודרגות גרסאותיהן.

10.6. **הביקורת מעירה כי לא מתבצעות בדיקות יזומות של יומני האירועים במטרה לאתר אירועים חריגים ברשת.**

10.7. בנוהל אבטחת המידע של העיריה בסעיף 5.8.4 לנוהל מובהרים המעשים שיחשבו לעבירות משמעת ביניהם מופיעה גם העברת סיסמא אישית לידי אדם אחר:

"המעשים שלהלן ייחשבו לעבירה משמעתית, מבלי לפטור את עושיהם מתוצאותיהם בתחום הדין הכללי:

1) *מסירת סיסמא לידי אדם אחר, זולת מה שמתחייב מהוראות כל דין.*
2) *שימוש בסיסמא של אדם אחר.*
3) *שימוש בסיסמא לכל מטרה שהיא, זולת עבודת העובד במערכת.*
4) *מסירת פלט לאדם לא מוסמך.*
5) *מסירת מידע כלשהו שהגיע לידיעת עובד המערכת במהלך עבודתו."*

10.8. **הביקורת מצאה כי במחלקת משאבי אנוש (עפ"י דיווח העובדת) כאשר עובדת נעדרת מעבודתה, משתמשת העובדת שמחליפה אותה בסיסמה של העובדת שנעדרה ומעדכנת נתונים.**

10.9. **הביקורת ממליצה לחדד את הנהלים וההנחיות בנוגע לשימוש בסיסמאות האישיות ואיסור מוחלט על העברתן לידי אדם אחר.**

10.10. הביקורת מציינת כי ביום 28/5/2014 הועבר ריענון לעובדי עיריית קריית ביאליק ע"י מנהל מערכות המידע, המדגיש בפרק השני את כל נושאים שצוינו לעיל, ביניהם איסור גלישה באינטרנט באתרים שלא לצרכי עבודה, איסור הורדת תוכנות "חינם" מהאינטרנט או התקנת תוכנות/חומרות באופן עצמאי, כמו כן מודגש נושא הסיסמאות ואיסור

העברתן מאדם לאדם, מודגש גם עניין נעילת תחנות העבודה ועוד נושאים נוספים שעלו בזמן הביקורת.

10.11. הביקורת מציינת כי קיימים ליקויים בנושא מערך ההרשאות (נושא זה יפורט בהרחבה בסעיף 12).

10.12. **במרבית עמדות העבודה מתבצעת נעילה אוטומטית לאחר זמן קצוב של אי שימוש. הביקורת ממליצה שתבוצע הרחבה שתכלול את כלל עמדות העבודה בארגון, דבר שימנע חשיפת מידע העלולה לאפשר פעילות בלתי מורשית באמצעות העמדות שלא ננעלות וכן לעגן זאת בנוהל.**

10.13. **הביקורת ממליצה להנהלת העירייה לבחון חסימה מלאה של משתמשים מרחבי הארגון לאתרי אינטרנט שונים ולהורדות.**

10.14. **הביקורת ממליצה לדאוג לעדכון תוכנת האנטי וירוס, מאחר וישנם איומים חדשים בכל יום ווירוסים המופצים ע"י רשת האינטרנט שהינה חלק בלתי נפרד מהארגון. נציין כי במהלך הביקורת בוצע עדכון לתוכנה.**

10.15. יש לציין כי בטיוטת תקנות הגנת הפרטיות (אבטחת מידע), התשנ"ב-2012, מפורטות מספר הפעולות שיש לנקוט בהן בנוסף לפעולות הננקטות כיום בארגון על מנת לאבטח את מאגרי המידע מבחינה לוגית. **הביקורת ממליצה לאמץ כבר עתה את התקנות ולעגן הנושאים בנהלים מתאימים, להלן לשון התקנות:**

"11.(ב) בנוהל האבטחה יקבע בעל המאגר הוראות לעניין התמודדות עם אירועי אבטחת מידע, בהתאם לחומרת האירוע ולמידת רגישות המידע, לרבות הוראות
לעניין ביטול הרשאות וצעדים מיידים אחרים הנדרשים ולעניין דיווח לבעל המאגר על אירועי אבטחה ועל פעולות שננקטו בעקבותיהם.
(ג) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יקיים בעל המאגר דיון תקופתי באירועי האבטחה. (ד) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, ייערך דיון כאמור בתקנת משנה (ג) אחת לרבעון לפחות.
(ה) ארע אירוע אבטחה חמור, יודיע על כך בעל המאגר לרשם באופן מיידי, וכן ידווח לרשם על הצעדים שנקט בעקבות האירוע. בתקנת משנה זו ובתקנת משנה (ו)- "אירוע אבטחה חמור" – א. במאגר מידע שחלה עליו רמת האבטחה הגבוהה –אירוע בו נעשה שימוש במידע מהמאגר בלא הרשאה; ב. במאגר מידע שחלה עליו רמת האבטחה הבינונית - אירוע בו נעשה שימוש בחלק מהותי של המידע מהמאגר בלא הרשאה.
(ו) ארע אירוע אבטחה חמור, רשאי הרשם להורות לבעל המאגר, למעט לבעל

מאגר מידע המנוי בסעיף 13(ה) לחוק, להודיע על אירוע האבטחה לנושא מידע שעלול להיפגע מן האירוע.

12.<u>התקנים ניידים-</u> (א) בעל מאגר המאפשר שימוש במידע מהמאגר בהתקן נייד או

העתקה שלו להתקן נייד ינקוט אמצעי הגנה בשים לב לסיכונים המיוחדים הקשורים לשימוש בהתקן נייד; לעניין זה, שימוש בשיטות הצפנה מקובלות ייחשב כנקיטת אמצעים סבירים".

14.<u>אבטחת תקשורת</u>-(א) מערכות המאגר לא יחוברו לרשת האינטרנט או לרשת ציבורית אחרת ללא התקנת אמצעי הגנה מתאימים המגנים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב.

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

(ג) במאגר מידע שניתן לגשת אליו מרחוק באמצעות רשת תקשורת, בנוסף לאמצעי אבטחה כאמור בתקנות משנה (א) ו-(ב), יעשה שימוש באמצעים שמטרתם לזהות את המתקשר ומאמתים את הרשאתו לביצוע הפעילות מרחוק

ואת היקפה; לעניין גישה של עובד למאגר מידע ברמה הבינונית ייעשה שימוש באמצעי פיזי הניתן לשליטתו הבלעדית של העובד.

11. <u>אבטחת מידע פיזית</u>

11.1. גישה פיזית למחשב (או לנתב) בדרך כלל נותנת למשתמש שליטה מלאה על אותו מחשב. במטרה למנוע גישה, או נזק פיזי למערכות המידע והפרעה לתהליכים הארגוניים מפני גורמים לא מורשים, יש ליישם אבטחה פיזית.

11.2. האבטחה הפיזית כוללת: מניעת גישה פיזית למערכות המידע ע"י שימוש במנעולים, בקרות גישה, סורגים ועוד; מניעת פגיעה לא מכוונת בציוד רגיש של העירייה, כגון שריפות, הצפות וכדומה, העלולות לגרום לנזק בלתי הפיך למערכות הארגון וכתוצאה מכך איבוד מידע יקר לעירייה; הגנה על המערכות הניידות של העירייה כגון מחשבים ניידים, מדיה ניידת (דיסקים, DISK ON KEY) מפני גניבות (גניבה פיזית של המערכות הניידות או גניבת מידע מתוכן) ושימוש לא מורשה; וכן ההגנה על ציוד ונײרת המכילים מידע רגיש.

11.3. תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו - 1986, פרק ב' תקנה מס' 3 (ב)(1) המחייבת את אחראי /מנהל המאגר:

" קיום הגנה פיסית על מערכת עיבוד הנתונים האוטומטית (להלן - המערכת), ועל תשתיתה לרבות מבנה, אמצעי תקשורת, מסופים ותשתית חשמלית מפני סיכונים סביבתיים ופגיעות".

11.4. קיים בעירייה נוהל אבטחת מידע אשר טרם אושר סופית ע"י הנהלת העירייה והיועמ"ש להלן לשון סעיפי הנוהל בהם ישנה התייחסות לנושא אבטחת המידע הפיזית:

"5.שיטה

5.1. אבטחת מידע

5.1.1. כל עובד ינקוט בתחום אחריותו, בכל האמצעים לשם אבטחת המידע שברשותו, לרבות:

1) נעילת ארונות ומגירות המכילים מידע.

2) נעילת דלתות וחלונות במשרדים.

3) כיבוי המחשב בסיום העבודה.

4) הזנת סיסמה/צופן/קוד אישיים למחשב האישי והחלפתם אחת לשנה.

5) גריסת מסמכים חסויים.

6) הפעלת מערכות אזעקה במקום בו הותקנו, כאשר לא נוכח בו עובד/מאבטח.

5.1.2. מידע רגיש יופקד בכספת המחלקתית (לדוגמא: מחלקת בטחון, מח' כספים וכד') והטיפול בו ייעשה על ידי עובד העירייה המוסמך (על ידי מנהל אותה מחלקה) מתוקף תפקידו, תוך נקיטת האמצעים לאבטחתו, ועל פי נוהלי והנחיות העירייה הנוגעים בדבר.

5.1.3. על כל עובד להפעיל שיקול דעת בהוצאת מסמכים מהארגון. בכל מקרה

בו הוצאו מסמכים מהארגון יש לשמור עליהם, אין להניח מסמכים גלויים בפרהסיה ואין לאחסן או להשאיר מסמכים רגישים במכוניות.

5.1.4. העברה והפצה של מידע בתוך העירייה ובין העובדים לביניהם תעשה תוך

נקיטת - כללי אבטחת מידע, הן בשימוש בדואר אלקטרוני של מסמכים

כתובים, והן במסירת פריטים פיזיים (מדיה מגנטית / קלטת / דיסק / תרשים וכו')...

5.7 כללי אבטחה פיזית של תחנת עבודה

5.7.1. עובד היוצא מחדר עבודתו בסוף יום העבודה יסגור את תחנת העבודה

בה הוא משתמש, ואם לא נוכח בחדר עובד אחר, ינעל את החדר.

5.7.2. אין להשאיר ציוד מחשבים דולק/פועל לאחר שעות העבודה אלא על פי

אישור אחראי המחשוב בעירייה."

11.5. השרתים של העירייה נמצאים בחדר השרתים הממוקם בקומת הכניסה בבניין הראשי של העירייה. החדר מסורג ונעול בדלת פלדלת.

11.6. בעיריית קריית ביאליק קיים אחסון גיבויים בכספת נעולה חסינת אש.

11.7. **הביקורת מעירה כי ארונות התקשורת אינם סגורים.**

11.8. **הביקורת מעירה כי יש מערכת אזעקה במבני העירייה אך לא כל החלונות מסורגים. רק חדר השרתים וחדר משאבי אנוש בקומת הכניסה נמצאו מסורגים.**

11.9. **הביקורת מעירה כי חדר המחשב אינו מוגן מפני אש, דבר שמהווה בעיה מהותית במידה ותפרוץ שריפה בחדר המחשב.**

11.10. **הביקורת מעירה כי בחדר משאבי אנוש בו ביקרנו מדגמית לא נמצאו מערכות לגילוי וכיבוי אש, וכן נמצאה דלת הזזה מעץ הניתנת בקלות לפריצה, וניצתת במהירות במקרה בו פורצת שריפה.**

11.11. **הביקורת מעירה כי במסגרת ביקור במחלקת הגבייה נמצא כי הקלסרים המכילים מידע רגיש לגבי אזרחים (בקשות להנחות, חובות וכיו') נמצאים במדפים חשופים ובארונות לא נעולים. עניין זה חזר גם במחלקת משאבי אנוש שם נמצא כי התיקים האישיים של העובדים נמצאים בארונות לא נעולים או מדפים חשופים.**

11.12. **הביקורת מעירה כי עובדת במחלקת משאבי אנוש מחזיקה את הסיסמאות לכניסה למחשב ולתוכנות רגישות מתחת למקלדת שלה. יש לציין כי בעת השיחה עמה העובדת הבינה את חומרת העניין והוציאה את הפתק ממקומו.**

11.13. **הביקורת מעירה כי מתשאול עובדים במחלקות הנ"ל ומצפייה בהם נמצא כי העובדים מותירים על שולחנם מידע רגיש בעת עזיבת העמדה במהלך שעות העבודה.**

11.14. **הביקורת מעירה כי בעת עזיבת העמדה אין העובדות סוגרות את המחשב או התוכנות – באם אזרח יושב וממתין להן הוא יכול לצפות בנתונים המופיעים על המסך.**

11.15. הביקורת מצאה כי אין הגבלה בשימוש בהתקנים חיצוניים כגון: CD, USB, ישנה חשיבות בהגבלת השימוש מאחר וקיימת סכנת חשיפת

הרשת לווירוסים שונים שהשלכותיהם בין היתר הן פגיעות שונות בשלמות וזמינות המידע, כמו כן ישנה סכנה מפני העתקה לא מורשית של מידע מסווג.

11.16. **הביקורת ממליצה למפות את כל משרדי העירייה ולבצע תכנית למיגון מפני אש, וכן להתקין דלתות פלדלת בכל מקום בו אינן בנמצא.**

11.17. **הביקורת ממליצה להתקין סורגים בכל החלונות הקיימים במבני העירייה כהגנה נוספת לאזעקה מפני פריצות. זאת מאחר ומדובר במבנים בעלי 2 קומות לכל היותר דבר שמאפשר פריצה לתוך המבנים ולחדרים אסטרטגיים במבנים בקלות.**

11.18. הביקורת מציינת כי ריענון ותקציר נהלי אבטחת מידע המצוין בסעיף 10.23 לדו"ח זה, מדגיש את העלאת המודעות של המשתמשים בתחום אבטחת מידע ועמידה בנהלים. בין היתר ריענון זה כלל את הדגשת הנושאים שעלו בפרק זה, כגון: איסור השארת מסמכים על שולחן העבודה או המדפסת/מכונת צילום, חובת השארת מסמכים רגישים נעולים במגירות/ארונות , איסור רשימת סיסמאות בסמוך למקלדת או במקום חשוף, הקפדה על נעילת עמדת העבודה כשהמחשב אינו בשימוש וכו'.

12. <u>מערך ההרשאות</u>

12.1. בתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו-1986, בפרק ב' מופיעה תקנה 3(ב)(2) על פיה יש לקבוע *"סדרי ניהול של מאגר מידע,* ***וכללים להרשאת גישה למידע,*** *לאיסוף, לסימון, לאימות, לעיבוד ולהפצה של המידע, הכל בהתאם להוראות החוק והתקנות;* ***סדרים וכללים כאמור יחולו גם על נותן שירותים חיצוני לגוף שבבעלותו מאגר המידע".***

בנוסף, בפרק ד' לתקנות, בתקנה מס' 14 מחויב מנהל המאגר ברישום מעודכן של כל הרשאות הגישה שניתנו: *" מנהל המאגר ינהל רישום מעודכן של הרשאות גישה אשר יכיל שמות ופרטי זיהוי של עובדי המערכת והמשתמשים המורשים לגשת למידע האגור במערכת, פירוט קוד הגישה וסוגי הפעולות המותרים למשתמשים; סיסמאות הגישה יוחלפו לעיתים בלתי קבועות אך לא פחות מאשר אחת לששה חודשים או בעת החלפת עובדים".*

12.2. קיים בנוהל אבטחת מידע של עיריית קריית ביאליק (יש לציין כי טרם אושר סופית ע"י הנהלת העירייה והיועמ"ש) סעיף המתייחס מתן הרשאות:

5.6 רשות כניסה למאגרי המידע

5.6.1. הגישה למאגרי המידע תתאפשר רק באמצעות קוד גישה וסיסמה שיאמתו את בלעדיות הגישה על יד המורשים לצפות או להשתמש בו.

5.6.2. קוד הגישה בנוי משני מרכיבים

1) שם משתמש הנקבע על ידי מנהל הרשת, לדוגמה: OFRAB

2)סיסמה הנקבעת על ידי המשתמש:

א. על הסיסמה להיות מורכבת מאותיות, מספרים.

ב. המערכת מאלצת להחליף את הסיסמה מעת לעת באופן אוטומטי.

3) המנהל יקבע לגבי כל משתמש, את ההבחנה בין הרשאה לשלוף/לעיין במידע לבין ההרשאה לרשום או לתקן מידע קיים.

4) עם העברת עובד לתפקיד אחר או פרישתו, יודיע מנהל המחלקה הרלוונטית לאחראי המחשוב את שם המשתמש שהיה ידוע לעובד בתפקידו הקודם.

5) אחראי המחשוב ישנה לאלתר את סיסמת תיבת הדואר, כדי שלעובד לא תהיה אפשרות להתחבר הן מהמשרד והן מהבית.

12.3. בעיריית קריית ביאליק כדי לקבל הרשאה מועברים מיילים למנהל מערכות המידע וכל הרשאה או פתיחת הרשאה חדשה מלווה באישור הגזבר ומתויקת בקלסר אבטחת מידע.

12.4. **הביקורת מעירה כי נושא ניהול המשתמשים (פתיחה, גריעה, הקצאה ושינוי הרשאות) מטופל לפי נוהג עבודה בלתי פורמאלי ואינו מעוגן**

באופן מפורט וברור בנהלי העירייה. יישום הרשאות גישה מתבצע באופן סלקטיבי לפי צרכי העובד והגדרות של מנהל המחלקה שלו. בנוסף, הודעות על עובד שעזב או הועבר לתפקיד אחר ובקשות לביטולי ההרשאות לא מועברות אל מנהל מערכות המידע בזמן אמת, אלא רק לאחר שהעובד כבר עזב או מכהן בתפקיד אחר זמן מה.

12.5. **הביקורת מעירה כי אין ברשות מנהל מערכות המידע את רשימת ההרשאות כמתחייב בתקנות הגנת הפרטיות כאמור לעיל.**

12.6. **הביקורת ממליצה לעגן במסגרת נוהל בנושא ההרשאות נושאים כגון: סדר הפעולות שיש לבצע בתהליך הרשאה, קיום פרטים מספקים אודות תפקידי המשתמשים, גורם מאשר, גורם מבצע וזאת בהתאם לפירוט המופיע בטיוטה לתקנות הגנת פרטיות (אבטחת מידע) התשע"ב -2012 תקנה מס' 9:**

"9 <u>זיהוי ואימות</u> -

א) בעל המאגר יישם אמצעים לווידוא כי הגישה למידע במאגר המידע נעשית רק בידי עובד המורשה לכך ובהתאם לרשימת ההרשאות התקפות.

(ב) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יקבע נוהל האבטחה הוראות לעניין האמצעים כאמור בתקנת משנה (א), ובכלל זה לנושאים אלה:

(1) אופן ביצוע הזיהוי, שייעשה ככל הניתן על בסיס אמצעי פיזי הניתן לשליטתו הבלעדית של המורשה; במידה שאופן הזיהוי מבוסס על סיסמאות יתייחס הנוהל גם לחוזק הסיסמה, מספר הניסיונות השגויים, ותדירות החלפת הסיסמאות שתיקבע בהתאם לתפקיד של מורשה הגישה, ובכל מקרה לא תעלה על ששה חודשים.

(2) ניתוק אוטומטי לאחר פרק זמן של אי פעילות.

(3) אופן הטיפול בתקלות הקשורות באימות זהות;

(ג) בעל המאגר ידאג לביטול ההרשאות של עובד שסיים את תפקידו ובמידת האפשר לשינוי סיסמאות למאגר ולמערכות התומכות במאגר, שהעובד עשוי היה לדעת, מיד עם סיום תפקידו של העובד".

12.7. הביקורת מציינת כי לספקים החיצוניים, הנותנים שירות למאגרי המידע, ישנן הרשאות מלאות לכל הקבצים והמידע בעירייה, עד כה הם לא היו חתומים על טפסי התחייבות על סודיות, אך במהלך הביקורת הוחתמו הספקים של חברת "מטרופולינט" על טפסים אלו (ראה נושא זה בהרחבה בסעיף 13.12 לדו"ח זה).

12.8. תקנה מס' 10 בטיוטת תקנות הגנת הפרטיות 2012, מפורט כי מנהל מערכות המידע ינהל מנגנון תיעוד אוטומטי לשם בקרה וביקורת על הגישה למערכות המידע:

"(א) במערכות של מאגר מידע אשר חלה עליו רמת האבטחה הבינונית או הגבוהה ינהל מנגנון תיעוד אוטומטי שיאפשר בקרה וביקורת הגישה למערכות המאגר (בתקנה זו – מנגנון הבקרה), ובכלל זה את כל הנתונים האלה: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, והאם הגישה אושרה או נדחתה; אם הגישה אושרה, יישמרו הנתונים המאפשרים זיהוי רכיב המערכת שאליו בוצעה הגישה.(ב) מנגנון הבקרה לא יאפשר, ככל הניתן, ביטול או שינוי של הפעלתו. מנגנון הבקרה יאתר שינויים או ביטולים בהפעלתו ויפיץ התראות לאחראים.

12.9. **הביקורת ממליצה לאמץ את התקנה המוזכרת לעיל כבר עתה ולפעול בהתאם לכתוב בה.**

12.10. **הביקורת ממליצה לבצע בחינה תקופתית וריענון של הרשאות משתמשים ברשת הפנימית . דבר שנועד לוודא כי מערך ההרשאות הינו מתאים לנדרש בפועל. כדאי לכלול בסקירה זו את בדיקת אופן היישום של הפרדת תפקידים נאותה בארגון ,באמצעות הרשאות גישה למערכות מחשב.**

12.11. **הביקורת ממליצה להחתים את אנשי המחשוב (טכנאים בעיקר) שהינם ספקים חיצוניים על טפסי התחייבות על שמירת סודיות (זאת בהתאם לטיוטת תקנות הגנת הפרטיות(אבטחת מידע) התשע"ב-2012 תקנה מס' 15 (ו)) .**

13. **<u>חברות חיצוניות</u>**

13.1. העירייה מנהלת מאגרי מידע ממוחשבים מסוגים שונים. המידע הכלול בהם הינו חיוני לפעילותה השוטפת, ולכן חובה עליה לנקוט במכלול אמצעי אבטחה פיסיים ולוגיים, על מנת למנוע כל פגיעה בהם. אבטחת המידע הינה הכרחית, שכן פגיעה בחיסיון המידע, בשלמותו ו/או בשרידותו עלולה לגרום לנזקים רבים לעירייה עצמה וגם לכל מי שפרטיו כלולים במאגרי המידע שלה.

13.2. יש לוודא קיום אבטחת מידע כאשר האחריות על עיבוד המידע נמסרת לגורם חיצוני. יש להתייחס לסיכונים, לבקרות האבטחה ולנוהלי האבטחה עבור הסביבות השונות.

13.3. בתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו-1986 ,בפרק ב' מופיעה תקנה 3(ב)(2) על פיה יש לקבוע *"סדרי ניהול של מאגר מידע, וכללים להרשאת גישה למידע, לאיסוף, לסימון, לאימות, לעיבוד ולהפצה של המידע, הכל בהתאם להוראות החוק והתקנות;* ***סדרים וכללים כאמור יחולו גם על נותן שירותים חיצוני לגוף שבבעלותו מאגר המידע".***

כמו כן בפרק ד' סעיף 9 מוזכר החיוב בקובץ נהלים המפרטים את אמצעי האבטחה והבקרה של המידע בנוגע לטיפול הפיסי באמצעי האחסון התקנה מחייבת גם את נותן השירות החיצוני באותם נהלים:

"למאגר מידע, כאמור בתקנה 8, ***יהיה קובץ נהלים*** *שבו יפורטו אמצעי האבטחה והבקרה על הטיפול הפיסי באמצעי האחסון של המידע.* ***בקובץ ייוחד פרק לטיפול במידע בידי נותן שירותים חיצוני המבצע עבודות עבור המאגר בתחומי הקלידה, עיבוד הנתונים, הפצת דו"חות והובלת קבצים".***

13.4. **בהתאם לסעיף 197 לפקודת העיריות עפ"י סעיף 197** העירייה מחויבת להתקשר עם ספקים באמצעות מכרזים:

"לא תתקשר עירייה בחוזה להעברת מקרקעין או טובין, להזמנת טובין או לביצוע עבודה אלא על פי מכרז פומבי".

13.5. בנוהל אבטחת מידע של העירייה (אשר טרם אושר סופית ע"י הנהלת העירייה והיועמ"ש) ישנה התייחסות להתקשרות עם גורמי חוץ:

" 5.4.2 בהסכמי התקשרות של העירייה עם קבלנים וספקים חיצוניים המעניקים לחברה שירותים שונים, יעוגן בחוזה/הסכם נושא שמירת הסודיות ואבטחת המידע של אותם גופים כלפי העירייה". (ישנו נספח 7.1 לנוהל – "תצהיר סודיות גורמי חוץ").

13.6. רוב המערכות המוניציפאליות (מערכות הגביה, גזברות, רווחה, חינוך ,שכר, הנדסה, חנייה ופיקוח, ניהול נתוני אוכלוסין, פורטל שירותים לתושב, ארכיב ממוחשב, BI , גישה לאינטרנט ולמייל) מסופקות, מוטמעות בעירייה ומנוהלות על-ידי ספקית שירותי מחשוב חיצונית "חברת מטרופולינט בע"מ" שבנוסף מספקת שירותים טכניים למערך המחשוב, ומתחזקת את ה-FIREWALL.

13.7. חברה חיצונית נוספת המספקת שרותי מחשוב לעירייה הינה חברת "אוטומציה".

13.8. **הביקורת מעירה כי ישנו חוזה בין חברת "אוטומציה" לעירייה בגין העסקת עובד של "האוטומציה" במחלקת משאבי אנוש, אולם העירייה משלמת סכום כספי נוסף מעבר לתשלום בגין העסקת העובד. תגובת גזבר העירייה בנוגע לנושא הנ"ל הייתה כי ישנו חוזה ישן עם חברת "אוטומציה" בגין אספקת שירותי מחשוב. החוזה מתחדש מעת לעת אך ע"י ספחים בלבד ולא ע"י מכרז וחידוש חוזה, זאת מאחר ורק מחלקת השכר מקבלת את שירותי "החברה לאוטומציה", יתר המחלקות מתקשרות בחוזה נפרד עם חברת "מטרופולינט". עפ"י נהלי מחלקת התקציבים והחשבות כל התקשרות עם חברה חיצונית שהיקפה בין 142,000 ₪ ועד 347,000 ₪ מחייבת מכרז זוטא (כלומר קבלת הצעות מחיר מ-4 ספקים) כשסופו של דבר הזוכה יחתום על הסכם מול עיריית קריית ביאליק. היקף ההתקשרות של "חברת אוטומציה" הינו בין 259,000 ₪ ועד 349,999 ₪ (ראה כרטסת ספקי מחשוב בסעיף 8) אולם לא נחתם עימה הסכם עדכני למעט חתימה על ספחים.**

13.9. העירייה חתמה על חוזה מפורט עם חברת "מטרופולינט" שנכנס לתוקף בתאריך 02/12/09. בסעיף 3.4 לחוזה מצוין כי ימונה מטעם העירייה עובד עירייה שינהל את ההתקשרות עם החברה הן בנוגע לאי הסכמות ו/או הבנות לגבי ההסכם עצמו והן בנוגע לטיב השירות.

13.10. **הביקורת מעירה כי לא מונה עובד עירייה כמתחייב עפ"י סעיף 3.4 לחוזה עם חברת "מטרופולינט".**

13.11. מנהל מערכות המידע הינו עובד של חברת "מטרופולינט" ואיננו עובד עירייה. נושא העסקתו מעוגן באותו החוזה שנחתם ביום 02/12/2009 ולא נחתם עמו חוזה העסקה נפרד.

13.12. הביקורת מציינת כי מנהל מערכות המידע הינו העובד היחיד במחלקה ואין לו כל מחליף. במידה והעובד נעדר מעבודתו הנושאים נשארים לא מטופלים עד חזרתו. בנוסף לא קיימת רוטציה (ראה הרחבה לנושא זה בסעיף 1.10).

13.13. **הביקורת מעירה כי עפ"י סעיף 1.71 להסכם שנחתם עם חברת "מטרופולינט" על העירייה להחתים את עובדי החברה על התחייבויות לשמירת סודיות, אולם בפועל רק במהלך הביקורת עובדי חברת "מטרופולינט" הוחתמו על ההתחייבויות הנ"ל.**

13.14. בסעיף 81 לחוזה, העירייה מחייבת את החברה, לעמוד בדרישות אבטחת המידע במערכות הנ"ל.

13.15. **הביקורת מציינת כי לא נמצא כל סעיף המאפשר לעירייה לבצע ביקורת על פעילות ספקית השירות בתחום אבטחת המידע ולבדוק האם באמת עומדת החברה בדרישות אבטחת המידע.**
לפיכך, אין לעירייה אינפורמציה כלשהי על רמת הבקרות ואבטחת מידע במערכות המידע המתוחזקות על ידי חברת "מטרופולינט".

13.16. **הביקורת ממליצה לבצע בחינה של רמת אבטחת המידע והבקרה במערכות המנוהלות על יד חברת "מטרופולינט". בנוסף, מומלץ במועד חידוש החוזה לכלול בו סעיף המאפשר לעירייה לקיים ביקורת מערכות מידע ואבטחת מידע בכל הנוגע לתחומים הרלוונטיים למערכות התוכנה שבשימוש העירייה.**

13.17. יש לציין כי בטיוטת תקנות הגנת הפרטיות(אבטחת מידע) התשע"ב-2012, תקנה מס' 15(א)(2) ו-(4) מפורט נושא ההתקשרות עם חברות חיצוניות שלהן גישה למאגרי המידע וכן נושא הבקרה על אותן חברות ועל עבודתן:

בעל מאגר המתקשר עם גורם חיצוני לצורך קבלת שירות, אשר כרוך במתן גישה למאגר המידע (להלן בתקנה זו - השירות) - יקבע במפורש בהסכם עם הגורם החיצוני (בתקנה זו – ההסכם) את כל אלה, בשים לב לסיכונים לפי תקנת משנה (1): (ה) החובות בתחום אבטחת המידע החלות על הגורם החיצוני לפי תקנות אלה, וכן הנחיות נוספות לעניין אמצעי אבטחת מידע שקבע בעל המאגר, ככל שקבע;

(ו) חובתו של הגורם החיצוני להחתים את עובדיו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק בהתאם לאמור בהסכם וליישם את אמצעי האבטחה הקבועים בהסכם, כאמור בפסקת משנה (ה);

(4) בעל המאגר ינקוט אמצעי בקרה ופיקוח כדי לוודא את עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות תקנות אלה בהיקף הנדרש בשים לב לסיכונים בתקנה משנה (1).

13.18. **הביקורת ממליצה כי יש לאמץ כבר עתה את התקנות הרשומות מעלה ולהגדיר בפני החברה החיצונית, "מטרופולינט", את חובותיהם בתחום אבטחת המידע של המאגרים אותם מספקים לעירייה ומתחזקים ולנקוט באמצעי בקרה ופיקוח על מנת לוודא כי החברה מאבטחת את המידע כנדרש ובהתאם לסיכונים הרלוונטיים.**

להלן סיכום הממצאים וההמלצות

רקע כללי

בעיריית קריית ביאליק קיימים כ-10 אתרים המבוזרים במשרדי העירייה, בכל משרד קיים לפחות מחשב נייח אחד. כל המחשבים מחוברים למערכת הממוחשבת העירונית (המערכות נרכשות מספק חיצוני ולא מפותחות בעירייה) המנוהלת ע"י מחלקת המחשוב ומערכות המידע שנמצאת באגף הכספים אותו מנהל גזבר העירייה.

בראשה של המחלקה עומד מנהל מערכות מידע שהינו העובד היחיד במחלקה. מנהל מערכות המידע מועסק בהתאם לחוזה התקשרות עם חברת "מטרופולינט" ומועסק במשרה מלאה דרך חברה זו.

מאגרי המידע הקיימים בעירייה כגון: גביה, הנהלת חשבונות, רכש, חינוך, עיקולי בנקים, רווחה, שירות פסיכולוגי, שירותי וטרינריה, משאבי אנוש, פקוח עירוני וכו' הינם תחת ניהולה של המחלקה. תפקידה העיקרי של המחלקה הינו איתור וטיפול בתקלות וכן ניתוחן. הטיפול בשרתים ובמערכות הליבה והחנייה כולל השירות הטכני ניתנים ע"י החברה החיצונית "מטרופולינט".

1. **<u>מבנה ארגוני ופעילות המחלקה (פרקים 1,2)</u>**

1.1. מחלקת המחשוב ומערכות המידע מתנהלת תחת אגף הכספים בניהולו של גזבר העירייה.

1.2. בעיריית קריית ביאליק מחלקת המחשוב ומערכות המידע כוללת אדם אחד בלבד אשר אחראי על כל מערך המחשוב ואבטחתו בעירייה, תפקידו מוגדר כמנהל מערכות המידע. מנהל מערכות המידע הינו עובד Outsourcing אשר מועסק במשרה מלאה ע"י חברת "מטרופולינט" המספקת את שירותי המחשוב לעירייה. מנהל מערכות המידע מכהן 9 שנים בתפקידו.

1.3. פעילות המחלקה כוללת את התחומים הבאים: ניתוח מערכות מידע, תשתיות המחשוב ותחזוקתן, תקשורת וטלפוניה, תמיכה ואחזקת מערכות המחשוב של מוסדות החינוך ואבטחת מידע.

1.4. הביקורת מעירה כי מנהל מערכות המידע לא מונה באופן רשמי לתפקיד מנהל אבטחת מידע בעירייה.

1.5. בעקבות הערת הביקורת מסר גזבר העירייה כי הוא פועל להוצאת המינוי כנדרש.

1.6. הביקורת ממליצה לעגן בהסכם עם חברת "מטרופולינט", קבלת עובד בעת העברות מנהל מערכות המידע בגין חופשה, מחלה, מילואים או כל סיבה אחרת, על מנת שיוכל לשמש ממלא מקום מנהל מערכות המידע זאת מאחר ונמצא כי לא מונה עד כה ממלא מקום.

1.7. במקרה של היעדרות מנהל מערכות המידע ישנה חשיבות לקיומה של רוטציה בעיקר בשל הצורך לתת מענה למחלקות העוסקות בתחומי הליבה של העירייה בזמן אמת.

2. רישום מאגרי מידע (פרק 3)

2.1. בתקנות הגנת הפרטיות (אגרות), התשס"א-2000, ובנוהל "אבטחת מידע" קיימת חובת תשלום בגין אגרת הרישום וכן מפורטים ההליכים שינקטו במידה והאגרה לא תשלום במועדה או בכלל.

2.2. הביקורת מעירה כי לא בוצע חידוש רישום ותשלום אגרה בגין מאגרי המידע מזה 9 שנים, דבר העלול לגרור קנסות בגין אי תשלום ואף שלילת רישום המאגר בפנקס הרשם.

3. נהלים ומדיניות (פרק 4)

3.1. הביקורת מעירה כי קיימים בעירייה 2 נהלים: נוהל אבטחת מידע בעירייה ונוהל גיבויים אולם הם טרם אושרו ע"י היועמ"ש והנהלת העירייה והם מפרטים חלקית בלבד את הפעולות שנדרשות לביצוע בנושאי אבטחת המידע.

3.2. הביקורת ממליצה כי מנהל מערכות מידע יכין קובץ נהלים שיכלול את הנושאים הבאים:

3.2.1. נוהל מפורט בנוגע לכניסת עובדים למערכות המידע.

3.2.2. נוהל מפורט לגבי מתן סיסמאות ו/או חסימתן נוהל מפורט לביצוע ניתוח סיכונים.

3.2.3. נוהל אזהרה בגין הפרת סודיות.

3.2.4. נוהל מפורט של אבטחת מידע לגבי כניסת קבלנים ועובדי חוץ למערכות המידע.

3.2.5. נוהל התקנת תוכנות במחשבים ע"י המשתמשים.

3.2.6. נוהל מפורט בנוגע לשימוש בחומרה אשר הובאה מחוץ לארגון.

3.2.7. נוהל מפורט בנוגע להורדות מרשת האינטרנט.

3.2.8. נוהל מפורט בנוגע לשימוש בדואר אלקטרוני.

3.2.9. נוהל קבלת עובד הכולל הצהרת סודיות, הצהרה בדבר קבלת ציוד וכו', וכן נוהל זהה בנוגע לפרישה או עזיבת עובד. דבר המשפיע באופן ישיר על האבטחה הפיזית והלוגית.

3.3. יצוין כי בעקבות הערת הביקורת בתאריך 28 למאי 2014 הוצאו הנחיות וריענון נהלי אבטחת מידע לעובדים הנוגעים באופן ישיר לנושאים שהועלו בביקורת. למרות האמור לעיל, ההנחיות הנ"ל אינן מכסות את כל נושא אבטחת המידע ואינן מהוות תחליף למדיניות אבטחת מידע מפורטת יותר ונהלים נפרדים לכל נושא.

3.4. הביקורת ממליצה לקיים הדרכה לעובדים חדשים בתחום אבטחת מידע.

4. <u>קיום מיפוי של מערך המחשוב (פרק 5)</u>

4.1. מנתונים שהתקבלו ממחלקת המחשוב עולה כי קיים מיפוי חלקי בלבד של מערך המחשוב בעירייה לשנת 2013 ולא קיימים מיפויים לשנים 2010-2012.

4.2. הביקורת ממליצה כי מנהל מערכות המידע יערוך מיפוי מלא של מערך המחשוב וינהלו עפ"י המפורט בטיוטת תקנות הגנת הפרטיות (אבטחת מידע), התשע"ב-2012, תקנה מס' 5(א). זאת על מנת להשיג האפשרות לשליטה על כמויות המחשבים, שרתים, החומרות, התוכנות ומיקומן ביחידות/מחלקות השונות בעירייה שכן המערכות הללו הן בתחום אחריותו של מנהל מערכות המידע.

5. **ביצוע סקר סיכונים בנושא מערכות מידע ממוחשבות (פרק 6)**

5.1. מתפקידו של הממונה על אבטחת מידע (באישור ההנהלה) לדאוג לעריכת סקר סיכונים בנושא אבטחת מידע ולבצע שינויים משמעותיים בהתאם לממצאי הסקר.

5.2. הביקורת מצאה כי בשנים 2010-2012 לא בוצע כל סקר סיכונים בעיריית קריית ביאליק. לפיכך, לדעת הביקורת יש לערוך סקר סיכונים בנושא אבטחת מידע ובכך להתעדכן בסיכונים הפוטנציאליים ולמגן את מערכות המידע מפני אותם הסיכונים. לשם עריכת הסקר מומלץ להיעזר בגורם חיצוני המוסמך לכך.

6. **פיקוח ובקרה על מחלקת המחשוב ומערכות מידע (פרק 7)**

6.1 הבקרות משמשות ככלי לפיקוח על התקנה ועדכון של רכיבי חומרה ותוכנה על מנת להבטיח כי המערכת תפעל כמצופה ממנה ולא תגרם לה פגיעה עקב עדכונים.

6.2 תקנה מס׳ 16, בטיוטת תקנות הגנת הפרטיות (אבטחת מידע), התשע״ב-2012, מחייבת ביקורות תקופתיות ומפרטת את התהליך. הביקורת ממליצה לאמץ התקנה המופיעה לעיל כבר עתה ולפעול בהתאם למפורט בה.

6.3 הביקורת ממליצה לנהל מנגנון תיעוד אוטומטי שיאפשר בקרה וביקורת הגישה למערכות המאגר (ראה נושא זה בהרחבה בפרק 12).

7. **תקציב (פרק 8)**

7.1. מהנתונים שהתקבלו מאגף הכספים עולה כי תקציב מחלקת המחשוב ואבטחת המידע הינו נגזרת מתקציב הגזברות.

7.2. הביקורת מעירה כי מניתוח נתוני התקציב מול הביצוע לאורך השנים הנסקרות ניתן לראות שישנה חריגה מיעדי התקציב ואף מגמת עלייה בחריגה לאורך אותן השנים.

7.3. מגזברות העירייה נמסר כי החריגות נבעו מתקלות לא צפויות, רכישת ציוד בלתי צפויה, תחזוקה מונעת.

7.4. יש לציין כי רכישת מחשבים וציוד נלווה מתבצעת ע״י המחלקות השונות מתקציביהן.

7.5. מכרטסת הספקים עולה כי קיימת התקשרות עם חברת ״אוטומציה״ לשם אספקת תוכנה וסך ההתקשרות לשנה עולה על

142,000 ₪ + מע"מ. מבדיקתנו עולה כי לא נערך מכרז בגין התקשרות זו.

7.6. בתגובתו לדו"ח מסר גזבר העירייה כי מדובר בחוזה ישן שמתחדש מעת לעת. חברת "אוטומציה" הוחלפה כספק תוכנה וכעת נותנת השירות בתחום הינה חברת "מטרופולינט". כלל יחידות העירייה מקבלות שירות מחברת "מטרופולינט" למעט מחלקת השכר כך שההתקשרות של מחלקה זו עם חברת "אוטומציה" מתבצעת ללא מכרז וכך גם התשלום.

7.7. הביקורת ממליצה כי נושא אבטחת המידע בעיריית קריית ביאליק יהיה מתוקצב באופן נפרד מתקציב מחלקת המחשוב , מאחר ולצורך ביצוע עבודתו של הממונה על אבטחת המידע בצורה נאותה ומספקת, עליו לקבל המשאבים הנדרשים לכך . תקציב נפרד יאפשר לממונה על אבטחת מידע להקצות משאבים להגנת המערכת שלא על חשבון החומרה.

8. <u>שרידות ומערך גיבוי מערכות המידע (פרק 9)</u>

8.1. בעיריית קריית ביאליק ישנו נוהל בנוגע לגיבויים. הנוהל חל על מנהל מערכות המידע ועל נציגו במידה שימונה ע"י מנכ"ל העירייה או הגזבר.

8.2. בעירייה ישנן 7 קלטות ברובוט גיבוי שבחדר המחשב. אחת לשבוע נשמרת קלטת אחת במקום אחר מוגן מאש ופריצה בכספת (שבמחלקת הגזברות הנמצאת בבניין אחר). מתבצעים גיבויים שוטפים יומיים שבועיים וחודשיים. חלק מהמערכות נמצאות בענן ביניהן מערכת הגביה, הנהלת חשבונות, רווחה ומוקד והן מגובות ע"י נוהל מסודר ולפי הסכם בחברה חיצונית.

8.3. הביקורת מעירה כי חדר המחשב בו נמצא רובוט הגיבוי אינו מוגן מפני אש.

8.4. הביקורת מציינת בנוסף, כי בעירייה קיימת תכנית מגירה לגיבוי שטרם מומשה, שרידות והתאוששות לאחר אירוע DRP. לדברי מנהל מערכות המידע עלות מימוש משוערת של התוכנית הינה 500 אלף ₪.

8.5. הביקורת ממליצה למפות את המידע עפ"י מידת רגישותו ולגבותו בהתאם לכך.

8.6. הביקורת ממליצה לקבוע נהלי התאוששות, בנוסף לתכנית המגירה DRP שקיימת בארגון, בהתאם למצוין בטיוטת תקנות הגנת הפרטיות (אבטחת מידע), התשע"ב-2012. מומלץ לתרגל נהלים אלו ולעדכנם מעת לעת. זאת כדי להבטיח את היכולת לשחזר מידע בכל עת למצבו המקורי, ובכך להבטיח את שלמות המידע במקרה של אובדן או הרס.

9. <u>אבטחת מידע לוגית (פרק 10)</u>

9.1. אבטחה לוגית, פירושה-האמצעים והנהלים הדרושים להגנה על מאגרי המידע ועל משאבי המידע, כגון: זיהוי המשתמשים באמצעות סיסמאות, מעקב ותיעוד הפעולות שמבוצעות במערכת, הטמעת מערכת תכנה וחומרה לגילוי ומניעת חדירת וירוס, בקרות על שלמות המידע ואמינותו וטיפול באירועים חריגים ועוד.

9.2. קיים בעירייה נוהל אבטחת מידע אשר טרם אושר סופית ע"י הנהלת העירייה והיועמ"ש ובו סעיפים הנוגעים לנושא אבטחת המידע הלוגית. כמו כן מובהרים המעשים שיחשבו לעבירות משמעת (בתחום אבטחת המידע הלוגית) ביניהם מודגש נושא העברת הסיסמא האישית לידי אדם אחר.

9.3. הביקורת מציינת כי קיימת בארגון תכנת אנטי וירוס מגרסה ESET NODE 32 4.2.76.0 לכל המחשבים, כמו כן קיימות מערכות הגנה "SPAM", "FIREWAL" מאובטחות ומעת לעת משודרגות גרסאותיהן.

9.4. הביקורת מעירה כי לא מתבצעות בדיקות יזומות של יומני האירועים במטרה לאתר אירועים חריגים ברשת.

9.5. הביקורת מצאה כי במחלקת משאבי אנוש (עפ"י דיווח העובדת) כאשר עובדת נעדרת מעבודתה, משתמשת העובדת שמחליפה אותה בסיסמה של העובדת שנעדרה ומעדכנת נתונים.

9.6. הביקורת ממליצה לחדד את הנהלים וההנחיות בנוגע לשימוש בסיסמאות האישיות ואיסור מוחלט על העברתן לידי אדם אחר.

9.7. הביקורת מציינת כי ביום 28/5/2014 הועבר ריענון לעובדי עיריית קריית ביאליק ע"י מנהל מערכות המידע, המדגיש בפרק השני את כל נושאים שצוינו לעיל, ביניהם איסור גלישה באינטרנט באתרים שלא לצרכי עבודה, איסור הורדת תוכנות "חינם" מהאינטרנט או

התקנת תוכנות/חומרות באופן עצמאי, כמוכן מודגש נושא הסיסמאות ואיסור העברתן מאדם לאדם, מודגש גם עניין נעילת תחנות העבודה ועוד נושאים נוספים שעלו בזמן הביקורת .

9.8. במרבית עמדות העבודה מתבצעת נעילה אוטומטית לאחר זמן קצוב של אי שימוש. הביקורת ממליצה שתבוצע הרחבה שתכלול את כלל עמדות העבודה בעירייה, דבר שימנע חשיפת מידע העלולה לאפשר פעילות בלתי מורשית באמצעות העמדות שלא ננעלות וכן לעגן זאת בנוהל.

9.9. הביקורת ממליצה להנהלת העירייה לבחון חסימה מלאה של משתמשים מרחבי הארגון לאתרי אינטרנט שונים ולהורדות.

9.10. הביקורת ממליצה לדאוג לעדכון תוכנת האנטי וירוס, מאחר וישנם איומים חדשים בכל יום ווירוסים המופצים ע"י רשת האינטרנט שהינה חלק בלתי נפרד מהארגון. נציין כי במהלך הביקורת בוצע עדכון לתוכנה.

9.11. יש לציין כי בטיוטת תקנות הגנת הפרטיות (אבטחת מידע), התשע"ב-2012, מפורטות מספר הפעולות שיש לנקוט בהן בנוסף לפעולות הננקטות כיום בארגון על מנת לאבטח את מאגרי המידע מבחינה לוגית. הביקורת ממליצה לאמץ כבר עתה את התקנות ולעגן הנושאים בנהלים מתאימים.

10. אבטחת מידע פיזית (פרק 11)

10.1. גישה פיזית למחשב (או לנתב) בדרך כלל נותנת למשתמש שליטה מלאה על אותו מחשב. האבטחה הפיזית כוללת: מניעת גישה פיזית למערכות המידע ע"י שימוש במנעולים, בקרות גישה, סורגים ועוד; מניעת פגיעה לא מכוונת בציוד רגיש של העירייה, כגון שריפות, הצפות וכדומה, העלולות לגרום לנזק בלתי הפיך למערכות הארגון וכתוצאה מכך איבוד מידע יקר לעירייה; הגנה על המערכות הניידות של העירייה כגון מחשבים ניידים, מדיה ניידת מפני גניבות ושימוש לא מורשה; וכן ההגנה על ציוד וניירת המכילים מידע רגיש.

10.2. קיים בעירייה נוהל אבטחת מידע אשר טרם אושר סופית ע"י הנהלת העירייה והיועמ"ש. בין היתר גם נושא אבטחת המידע הפיזית מופיע בנוהל.

10.3. השרתים של העירייה נמצאים בחדר השרתים הממוקם בקומת הכניסה בבניין הראשי של העירייה. החדר מסורג ונעול בדלת פלדלת.

10.4. בעיריית קריית ביאליק קיים אחסון גיבויים בכספת נעולה חסינת אש.

10.5. הביקורת מעירה כי ארונות התקשורת אינם סגורים.

10.6. הביקורת מעירה כי יש מערכת אזעקה במבני העירייה אך לא כל החלונות מסורגים. רק חדר השרתים וחדר משאבי אנוש בקומת הכניסה נמצאו מסורגים.

10.7. הביקורת מעירה כי חדר המחשב אינו מוגן מפני אש, דבר שמהווה בעיה מהותית במידה ותפרוץ שריפה בחדר המחשב.

10.8. הביקורת מעירה כי בחדר משאבי אנוש בו ביקרנו מדגמית לא נמצאו מערכות לגילוי וכיבוי אש, וכן נמצאה דלת הזזה מעץ הניתנת בקלות לפריצה, וניצתת במהירות במקרה בו פורצת שריפה.

10.9. הביקורת מעירה כי במסגרת ביקור במחלקת הגבייה נמצא כי הקלסרים המכילים מידע רגיש לגבי אזרחים (בקשות להנחות, חובות וכיו') נמצאים במדפים חשופים ובארונות לא נעולים. עניין זה חזר גם במחלקת משאבי אנוש שם נמצא כי התיקים האישיים של העובדים נמצאים בארונות לא נעולים או מדפים חשופים.

10.10. הביקורת מעירה כי עובדת במחלקת משאבי אנוש מחזיקה את הסיסמאות לכניסה למחשב ולתוכנות רגישות מתחת למקלדת שלה. יש לציין כי בעת השיחה עמה העובדת הבינה את חומרת העניין והוציאה את הפתק ממקומו.

10.11. הביקורת מעירה כי מתשאול עובדים במחלקות הנ"ל ומצפייה בהם נמצא כי העובדים מותירים על שולחנם מידע רגיש בעת עזיבת העמדה במהלך שעות העבודה.

10.12. הביקורת מעירה כי בעת עזיבת העמדה אין העובדות סוגרות את המחשב או התוכנות – באם אזרח יושב וממתין להן הוא יכול לצפות בנתונים המופיעים על המסך.

10.13. הביקורת מצאה כי אין הגבלה בשימוש בהתקנים חיצוניים כגון: USB,CD , ישנה חשיבות בהגבלת השימוש מאחר וקיימת סכנת חשיפת הרשת לווירוסים שונים שהשלכותיהם בין היתר הן פגיעות

שונות בשלמות וזמינות המידע, כמו כן ישנה סכנה מפני העתקה לא מורשית של מידע מסווג.

10.14. הביקורת ממליצה למפות את כל משרדי העירייה ולבצע תכנית למיגון מפני אש, וכן להתקין דלתות פלדלת בכל מקום בו אינן בנמצא.

10.15. הביקורת ממליצה להתקין סורגים בכל החלונות הקיימים במבני העירייה כהגנה נוספת לאזעקה מפני פריצות. זאת מאחר ומדובר במבנים בעלי 2 קומות לכל היותר דבר שמאפשר פריצה לתוך המבנים ולחדרים אסטרטגיים במבנים בקלות.

10.16. הביקורת מציינת כי ריענון ותקציר נהלי אבטחת מידע, מדגיש את העלאת המודעות של המשתמשים בתחום אבטחת מידע ועמידה בנהלים. בין היתר ריענון זה כלל את הדגשת הנושאים שעלו בפרק זה, כגון: איסור השארת מסמכים על שולחן העבודה או המדפסת/מכונת צילום, חובת השארת מסמכים רגישים נעולים במגירות/ארונות, איסור רשימת סיסמאות בסמוך למקלדת או במקום חשוף, הקפדה על נעילת עמדת העבודה כשהמחשב אינו בשימוש וכו'.

11. __מערך ההרשאות (פרק 12)__

11.1. בעיריית קריית ביאליק כדי לקבל הרשאה מועברים מיילים למנהל מערכות המידע וכל הרשאה או פתיחת הרשאה חדשה מלווה באישור הגזבר ומתויקת בקלסר אבטחת מידע.

11.2. הביקורת מעירה כי נושא ניהול המשתמשים (פתיחה, גריעה, הקצאה ושינוי הרשאות) מטופל לפי נוהג עבודה בלתי פורמאלי ואינו מעוגן באופן מפורט וברור דיו בנהלי העירייה. יישום הרשאות גישה מתבצע באופן סלקטיבי לפי צרכי העובד והגדרות של מנהל המחלקה שלו. בנוסף, הודעות על עובד שעזב או הועבר לתפקיד אחר ובקשות לביטולי ההרשאות לא מועברות אל מנהל מערכות המידע בזמן אמת, אלא רק לאחר שהעובד כבר עזב או מכהן בתפקיד אחר זמן מה.

11.3. הביקורת מעירה כי אין ברשות מנהל מערכות המידע את רשימת ההרשאות כמתחייב בתקנות הגנת הפרטיות כאמור לעיל.

11.4. הביקורת ממליצה לעגן במסגרת נוהל בנושא ההרשאות נושאים כגון: סדר הפעולות שיש לבצע בתהליך הרשאה, קיום פרטים מספקים אודות תפקידי המשתמשים, גורם מאשר, גורם מבצע וזאת בהתאם לפירוט המופיע בטיוטה לתקנות הגנת פרטיות (אבטחת מידע) התשע״ב -2012.

11.5. הביקורת מציינת כי לספקים החיצוניים, הנותנים שירות למאגרי המידע, ישנן הרשאות מלאות לכל הקבצים והמידע בעירייה, עד כה הם לא היו חתומים על טפסי התחייבות על סודיות, אך במהלך הביקורת הוחתמו הספקים של חברת ״מטרופולינט״ על טפסים אלו.

11.6. בטיוטת תקנות הגנת הפרטיות 2012, תקנה מס׳ 10 מפורט כי מנהל מערכות המידע ינהל מנגנון תיעוד אוטומטי לשם בקרה וביקורת על הגישה למערכות המידע הביקורת ממליצה לאמץ את התקנה כבר עתה ולפעול בהתאם לכתוב בה.

11.7. הביקורת ממליצה לבצע בחינה תקופתית וריענון של הרשאות משתמשים ברשת הפנימית. דבר שנועד לוודא כי מערך ההרשאות הינו מתאים לנדרש בפועל. כדאי לכלול בסקירה זו את בדיקת אופן היישום של הפרדת תפקידים נאותה בארגון, באמצעות הרשאות גישה למערכות מחשב.

11.8. הביקורת ממליצה להחתים את אנשי המחשוב (טכנאים בעיקר) שהינם ספקים חיצוניים על טפסי התחייבות על שמירת סודיות (זאת בהתאם לטיוטת תקנות הגנת הפרטיות(אבטחת מידע) התשע״ב-2012 תקנה מס׳ 15 (ו)).

12. <u>חברות חיצוניות (פרק 13)</u>

12.1. רוב המערכות המוניציפאליות (מערכות הגביה, גזברות, רווחה, חינוך, שכר, הנדסה, חנייה ופיקוח, ניהול נתוני אוכלוסין, פורטל שירותים לתושב, ארכיב ממוחשב, BI , גישה לאינטרנט ולמייל) מסופקות, מוטמעות בעירייה ומנוהלות על-ידי ספקית שירותי מחשוב חיצונית ״חברת מטרופולינט בע״מ״ שבנוסף מספקת שירותים טכניים למערך המחשוב , ומתחזקת את ה-FIREWALL.

12.2. חברה חיצונית נוספת המספקת שרותי מחשוב לעירייה הינה חברת ״אוטומציה״.

12.3. יש לוודא קיום אבטחת מידע כאשר האחריות על עיבוד המידע נמסרת לגורם חיצוני. יש להתייחס לסיכונים, לבקרות האבטחה ולנהלי האבטחה עבור הסביבות השונות.

12.4. הביקורת מעירה כי ישנו חוזה בין חברת "אוטומציה" לעירייה בגין העסקת עובד של ה"אוטומציה" במחלקת משאבי אנוש, אולם העירייה משלמת סכום כספי נוסף מעבר לתשלום בגין העסקת העובד. תגובת גזבר העירייה בנוגע לנושא הנ"ל הייתה כי ישנו חוזה ישן עם חברת "אוטומציה" בגין אספקת שירותי מחשוב. החוזה מתחדש מעת לעת אך ע"י ספחים בלבד ולא ע"י מכרז וחידוש חוזה, זאת מאחר ורק מחלקת השכר מקבלת את שירותי "החברה לאוטומציה" יתר המחלקות מתקשרות החוזה נפרד עם חברת "מטרופולינט". עפ"י נהלי מחלקת התקציבים והחשבות כל התקשרות עם חברה חיצונית שהיקפה בין 142,000 ₪ ועד 347,000 ₪ מחייבת מכרז זוטא (כלומר קבלת הצעות מחיר מ-4 ספקים) כשבסופו של דבר הזוכה יחתום על הסכם מול עיריית קריית ביאליק. היקף ההתקשרות של "חברת אוטומציה" הינו בין 259,000 ₪ ועד 349,999 ₪ אולם לא נחתם עימה הסכם עדכני למעט חתימה על ספחים.

12.5. העירייה חתמה על חוזה מפורט עם חברת "מטרופולינט" שנכנס לתוקף בתאריך 02/12/09. בסעיף 3.4 לחוזה מצוין כי ימונה מטעם העירייה עובד עירייה שינהל את ההתקשרות עם החברה הן בנוגע לאי הסכמות ו/או הבנות לגבי ההסכם עצמו והן בנוגע לטיב השירות.

12.6. הביקורת מעירה כי לא מונה עובד עירייה כמתחייב עפ"י סעיף 3.4 לחוזה עם חברת "מטרופולינט".

12.7. מנהל מערכות המידע הינו עובד של חברת "מטרופולינט" ואיננו עובד עירייה. נושא העסקתו מעוגן באותו החוזה שנחתם ביום 02/12/2009 ולא נחתם עמו חוזה העסקה נפרד.

12.8. הביקורת מציינת כי מנהל מערכות המידע הינו העובד היחיד במחלקה ואין לו כל מחליף. במידה והעובד נעדר מעבודתו הנושאים נשארים לא מטופלים עד חזרתו.

12.9. הביקורת מעירה כי לא הוחתמו עובדי חברת "מטרופולינט" לא הוחתמו על התחייבויות לשמירת סודיות כמפורט בסעיף 1.71 להסכם שנחתם עימם.

12.10. הביקורת מציינת כי במהלך הביקורת עובדי חברת "מטרופולינט" הוחתמו על התחייבויות לשמירת סודיות.

12.11. העירייה מחייבת את החברה, בסעיף 81 לחוזה, לעמוד בדרישות אבטחת המידע במערכות הנ"ל.

12.12. הביקורת מציינת כי לא נמצא כל סעיף המאפשר לעירייה לבצע ביקורת על פעילות ספקית השירות בתחום אבטחת המידע ולבדוק האם באמת עומדת החברה בדרישות אבטחת המידע.
לפיכך, אין לעירייה אינפורמציה כלשהי על רמת הבקרות ואבטחת מידע במערכות המידע המתוחזקות על ידי חברת "מטרופולינט".

12.13. הביקורת ממליצה לבצע בחינה של רמת אבטחת המידע והבקרה במערכות המנוהלות על יד חברת "מטרופולינט". בנוסף, מומלץ במועד חידוש החוזה לכלול בו סעיף המאפשר לעירייה לקיים ביקורת מערכות מידע ואבטחת מידע בכל הנוגע לתחומים הרלוונטיים למערכות התוכנה שבשימוש העירייה.

12.14. יש לציין כי בטיוטת תקנות הגנת הפרטיות(אבטחת מידע) התשע"ב-2012, תקנה מס' 15(א)(2) ו-(4) מפורט נושא ההתקשרות עם חברות חיצוניות שלהן גישה למאגרי המידע וכן נושא הבקרה על אותן חברות ועל עבודתן. הביקורת ממליצה כי יש לאמץ כבר עתה את התקנות ולהגדיר בפני החברה החיצונית, "מטרופולינט", את חובותיה בתחום אבטחת המידע של המאגרים אותם מספקת לעירייה ומתחזקת ולנקוט באמצעי בקרה ופיקוח על מנת לוודא כי החברה מאבטחת את המידע כנדרש ובהתאם לסיכונים הרלוונטיים.