אגף מחשוב ומערכות מידע

1. מבוא

1.1. כללי

א. בעיריית כפר סבא (להלן: "**העירייה**") קיימות מערכות מידע ומחשוב עירוניות המשמשות את יחידות העירייה השונות וחיוניות לפעילותן השוטפת. מערך המחשוב העירוני תומך במגוון רחב של תחומים, כגון: גבייה, חינוך, טיפול בפניות תושבים, הנדסה ועוד.

ב. על מתן שירותי המחשוב לכל אגפי העירייה אחראי אגף מחשוב ומערכות מידע (להלן: "**האגף**").

ג. בין היתר, אמון האגף על אבטחת המידע בעירייה, מתן תמיכה, אחזקה ושרות בתחום התוכנה, חומרה ותשתיות וכן עבודה מול ספקי מערכות צד ג' המבצעים פיתוחים עבור האגף. האגף מבצע עבודות אפיון עיצוב, הכנת מכרזים, בדיקות קבלה ומעקב אחר ההתקשרות עם הספקים. השרות ניתן עבור כלל יחידות העירייה השונות, תוך ראייה עתידית והקפדה על אינטגרציה מלאה בין המערכות.

ד. בשנת 2014 ביצע האגף פעילות מקיפה במגוון רב של תחומים, אשר כללה בין היתר את הפרוייקטים הבאים: הקמת ארכיון עירוני לתכניות בניין, הטמעת מערכת ממוחשבת לאישור לטאבו, המשך פרויקט עירוני לשדרוג כיתות אם לכיתות "חכמות" מתוקשבות בכל בתי הספר, שדרוג המוקד העירוני והפיכתו למערכת מידע אינטרנטית כלל עירונית, הטמעת מערכת לניהול תורים באגף הכנסות, הטמעת ושדרוג הרשאות למשתמשי קצה ועוד.

ה. המחלקה הבכירה לביקורת המדינה במשרד ראש הממשלה פרסמה בחודש ספטמבר 2005 - "**נוהל מסגרת לאבטחת מידע**" הכולל 38 נהלים לאבטחת מידע במשרדי הממשלה. נהלים אלה עוסקים בנושאים כגון: קביעת מדיניות ומיפוי מידע; הגורם האנושי ואבטחת המידע; אבטחה לוגית; אבטחה פיזית; גיבוי, שחזור והתאוששות; אבטחת תקשורת ושימושי אינטרנט; אבטחת

מידע במחשבים המנותקים מרשתות המשרד ועוד (להלן: "**חוברת נהלי המסגרת**").

ו. **<u>תגובת האגף</u>:** *"לא ברור כלל כי נוהל זה **מחייב** רשויות מקומיות. התייחסות בהמשך דוח זה רואה בו קווים מנחים ומתייחסים בהמשך מסמך זה להוראות הנוהל ברוח זו".*

הביקורת מציינת בהתייחס לתגובת האגף את הערת מבקר המדינה בדוח ביקורת משנת 2014 בנושא: "**ניהול רשומות אלקטרוניות ורשומות נייר ברשויות מקומיות**" כי: *"הנהלים המובאים באתר מחייבים את מוסדות המדינה, ומכאן שהם חלים גם על הרשויות המקומיות".*

1.2. מערכות המידע המרכזיות

להלן טבלה המציגה את מערכות המידע והמחשוב העירוניות ומיקום שרתי בסיס הנתונים:

שם המערכת	נושאים מרכזיים	מיקום שרתי המערכת	גורם אחראי לעדכוני ואבטחת השרתים
אוטומציה	מערכת גבייה ואוכלוסין, חינוך, רישוי עסקים, מערכות לניהול הגזברות, הנה"ח, תקציב, תב"ר[1]	החברה לאוטומציה - פתח תקווה	החברה לאוטומציה
מלם	ניהול עובדים	חברת מלם - ירושלים	חברת מלם
מלם	ניהול דיווחי נוכחות העובדים	חברת מלם - ירושלים	חברת מלם
מלם	שכר	חברת מלם - ירושלים	חברת מלם
office light	שמירת מסמכים	במבנה של העירייה	אגף מחשוב ומערכות מידע

כפי שעולה מן הטבלה, העירייה בחרה להיעזר במיקור חוץ מלא לניהול מערכות המידע העיקריות. האגף מנהל באופן עצמאי את תשתיות המחשוב ביניהם: ניהול רשת המשתמשים באמצעות מערכת ה-Active Directory, 4 שרתים וירטואליים, מערך DRP, מספר שרתים פיזיים נוספים, מערך גיבוי, פלטפורמות שונות לרבות

[1] תקציב בלתי רגיל

Exchange, SQL ועוד. ניהול זה מטיל את האחריות לאחסון מערכות המידע, שדרוגי תוכנה, אבטחת פיסית ואבטחה לוגית של המשתמשים על ספקי התוכנה (החברה לאוטומציה וחברת מלם). אחד החסרונות במדיניות זו הינה הסתמכות על ספק השירותים בכל הקשור לזמינות הנתונים, קרי, במקרה של תקלה בשרתי הספק נמנעת גישה למערכות המידע הקריטיות.

יצויין כי קיימות חלופות אחרות כמו ברשויות רא. ורע.[2], אשר בחרו לאחסן את בסיס הנתונים של מערכות המידע במסגרת פעילות אגף המחשוב במקביל לאחסון הנתונים אצל ספק השירותים, זאת על מנת שלא להסתמך על שרותי הספק במקרה של קריסת מערכות המידע אצל הספק.

1.3. מטרת הביקורת

הביקורת ביקשה לבחון כיצד מערכות המידע של העירייה תומכות במדיניות העירייה בכל הקשור לרכישת מערכות מידע למשתמשים, ומערכות תומכות למשתמשים בתחומים שונים, כגון:

שיפור תהליכי עבודה בעירייה, שיפור תשתיות (טלפוניה, אחסון וגיבוי הנתונים), פיתוח מערכות שונות לעבודות מחלקות העירייה.

בנוסף, בחנה הביקורת את מערך הבקרה והניהול של האגף בכל הקשור לתחום אבטחת המידע בעירייה והעמידה בהוראות החוק והנהלים המתאימים.

1.4. מתודולוגיה

לצורך הכנת הדוח, בוצעו הפעולות הבאות:

- פגישות עם מנהל האגף;
- פגישות עם סגן מנהל האגף ועם מזכירת האגף והאחראית על החשבות;
- שיחות עם עובדים ויועצים המעניקים שרותים באגף;

כמו כן, נסמכה הביקורת, בין היתר, על המסמכים הבאים:

- תכניות העבודה לשנים 2015- 2014;
- כרטיסי הנהלת חשבונות;
- חוזי עבודה עם יועצים;

[2] שמות הרשויות בניירות העבודה של הביקורת

- צילומי מסך ממערכת ה- Active Directory ;
- קבצים ממערכות ניטור ובקרה ;
- תיקי העובדים מאגף משאבי אנוש ;
- נהלי עבודה של האגף.

1.5. חקיקה ונהלים

להלן רשימת המקורות המשפטיים והמנהליים המחייבים את העירייה בתחום מערכות המידע:

- נוהל מסגרת לאבטחת מידע ;
- חוק הגנת הפרטיות, התשמ"א-1981 ;
- חוק המחשבים, התשנ"ה-1995.

2. <u>עיקרי הממצאים וההמלצות</u>

2.1. בכרטסות התב"ר של האגף בשנים 2013-2014, נמצאו תשלומים שוטפים ליועצים ולצרכי תחזוקה שוטפים שאינם עולים בקנה אחד עם הגדרת התב"ר המיועד לשדרוג מערכות מחשוב. סעיף 213 (ב) לפקודת העיריות קובע בין היתר, כי: *"...לא ייעשה כל שימוש בכספים של תקציב בלתי רגיל שלא למטרה שלשמה נועד, ובכלל זה לא ייעשו כל פעולות קיזוז בין כספים של תקציב בלתי רגיל לכספים של תקציב שאינו בלתי רגיל,... "*.

<u>תגובת האגף</u>: *"לקבלת תגובת הגזברות באשר למקורות ההוצאות השונות. ניהול התב"ר והתקציב וחלוקת הקצאת הכסף ביניהם היא באחריות הגזברות."*

<u>המלצה</u>

על גזברות העירייה בשיתוף מנהל האגף לפעול למניעת הפקת הזמנות המחייבות את כרטיסי התב"ר ממערכת הרכש, כאשר נושאי ההזמנה מתייחס לתחזוקה/ייעוץ שוטף הניתן למחלקות העירייה/האגף. לחילופין, יש לשקול כי הפקת ההזמנות תבוצע על ידי מחלקת הרכש בעירייה אשר תבחין בין רכישת שרות/טובין שוטף, לבין רכישות שאינן שוטפות אשר שייכות לתב"רים.

2.2. לא נמצאה תכנית עבודה רב שנתית לפעילות האגף למרות שהאגף תוקצב בסך של 7,890 אלפי ₪ לפעילויות שדרוג מערכות המידע לחמש שנים (2015-2019) באמצעות שני תב"רים. תקצוב זה, הנפרס כאמור, על פני 5 שנים, אינו בא לידי ביטוי בתכנית עבודה רב שנתית מוסדרת שמנוהלת עלי ידי מנהל האגף.
בידי מנהל האגף לא קיימת רשימה מפורטת בה מפורטים מהם התחומים והפרוייקטים אשר יבוצעו על ידי האגף, תוך פירוט של העלויות וכיצד יבוצע ניצול תקציב זה על פני 5 השנים.

<u>תגובת האגף</u>: *"קיימת תוכנית עבודה מפורטת אשר הוצגה לביקורת, עבור שנת 2106. אגף המחשוב עובד על פי תקציב שנתי עבור כל שנת תקציב. בפרויקטים רב-שנתיים (כגון CRM, סריקת תיקי בניין וכדומה), בהן יש הוצאה תקציבית ידועה ומתוכננת, נעשו שירויונים תקציביים בהתאם."*

<u>הערת הביקורת</u>

התוכנית הקיימת באגף אינה מותאמת לתקציב האגף לשנים 2015-2019. מומלץ כי הנהלת העירייה תערוך בחינה כוללת/תסדיר עבור כלל אגפי העירייה את כל הקשור לתשומות הנדרשות עבור כל אגף על מנת לעמוד ביעדים אשר הוצבו עבורם במהלך השנים הקרובות, תוך התייחסות לכלל המרכיבים: רגולציה, כמות התושבים להם ניתן השרות, התפתחויות טכנולוגיות צפויות, עלויות כספיות נדרשות ועוד. בהסתמך על תכנית זו תעודכן תכנית האב למספר שנים עבור אגף מחשוב ומערכות מידע.

2.3. נמצא כי לא אוייש תפקיד מנהל אגף מחשוב ומערכות מידע במשך 11 חודשים. מנהל אגף מחשוב ומערכות מידע הקודם, עזב בתאריך 30.4.2013 ותחילת העסקת מנהל אגף מחשוב ומערכות מידע הייתה בתאריך 1.4.2014.
הביקורת מציינת כי בזמן זה הסמכויות המקצועיות של האגף הואצלו למנהל מחלקת System והיועץ החיצוני (להלן: "**היועץ**"), והסמכויות הניהוליות הועברו למנהלת משאבי אנוש דאז.

<u>תגובת האגף</u>: *"לתגובת מש"א. להבנתי, מנהל האגף היוצא היה חולה תקופה ארוכה אך עדיין מועסק ורק לאחר שעזב ניתן היה לגייס עובד אחר במקומו."*

<u>המלצה</u>

מומלץ להנהלת העירייה לבצע תהליך הפקת לקחים בנוגע לאיוש משרות מרכזיות בעירייה בעתיד, זאת למרות הפתרון שנמצא בהעברת האחריות הניהולית למנהלת אגף משאבי אנוש, בתקופה הנדונה.

2.4 נמצא כי מסמך המדיניות, הקיים באגף, חסר ואינו מושלם.
נוהל מס' 1 במסמך מדיניות זה, קובע כי מסמך מדיניות אבטחת המידע בעירייה מתייחס לכלל היבטי אבטחת המידע בעירייה.
למסמך מדיניות זה דרושה השלמה במספר היבטים, כלהלן:

- אופן פעילות ותדירות התכנסות וועדת ההיגוי העירונית בתחום ניהול מערכות המידע, זהות המשתתפים והתפקידים של חברי הוועדה ועוד;
- הרשאות צפייה באתרי אינטרנט ייחודיים, כגון: Facebook, YouTube, תחנות רדיו. יש לציין, כי שימוש באתרי אינטרנט מעין אלה יוצר עומס רב על רשת התקשורת ומאט את פעילותה, ומאפשר גישה חופשית לאתרים כגון אלה לעובדים בעירייה;
- התחברות משתמשים חיצוניים למשרדי העירייה לצורך מתן שירותי מיקור חוץ, כולל התייחסות לגורמים המורשים להתחבר;
- אופן שימוש במחשבים ניידים;
- אופן שימוש בטלפון נייד המחובר למאגרי העירייה;

<u>המלצה</u>

יש לקיים דיון לבחינה ולהשלמת תכולת הסוגיות המרכיבות את מסמך מדיניות האגף ולאשרו במסגרת פעילות וועדת ההיגוי.

<u>תגובת האגף</u>: *"הנוהל אושר על ידי הנהלת העירייה, בסמכות מנכ"לית העירייה למנות וועדת היגוי באם נדרשת!.*

2.5 נמצא כי לא קיים נוהל עבודה חוצה ארגון המעגן את ממשק העבודה בין אגף משאבי אנוש לבין אגף מחשוב ומערכות מידע, בכל הקשור לקליטה ועזיבת עובדים.

<u>המלצה</u>

מומלץ להשלים ולהסדיר את הממשק בין אגף משאבי אנוש ואגף מחשוב ומערכות מידע בנוגע לקליטת/עזיבת עובדים ולגבותו בנוהל עבודה חוצה ארגון.

כמו כן, יש צורך שבטפסים היעודיים יצוינו ההרשאות והמערכות הנדרשות שיש להוסיף/להסיר לעובד עם גיוסו או עזיבתו את התפקיד.

<u>תגובת האגף</u>: *"ההמלצה מקובלת".*

2.6. נמצא כי לא נערכות הדרכות תקופתיות לעובדים פעילים וכן לעובדים חדשים עם קליטתם בעירייה.

<u>המלצה</u>

יש להכין תכנית הדרכה שנתית להדרכת עובדים פעילים ולשלב בתוכה את העובדים החדשים.

<u>תגובת האגף</u>: *"לתגובה יחד עם משא - רעיון טוב אפשרי לשלב הדרכה קצרה גם בנושא אבטחת מידע ונהלים.*

<u>סיכום</u>:

מומלץ כי אגף מחשוב ומערכות מידע, בשיתוף גזברות העירייה, יכין תכנית מפורטת עבור השנים הבאות, המתבססת על התקציב שאושר עבור האגף. בנוסף, יעגן האגף בנהלי עבודה את כלל פעולותיו וכן הממשקים הקיימים בינו לבין יחידות העירייה השונות, וזאת לשם הסדרת כלל תהליכי העבודה הקיימים, נהלי עבודה אלו יאושרו על ידי ועדת היגוי אשר תהיה אחראית על ניהול התוויה ומדיניות של מערכות המידע בעירייה.

3. <u>פירוט הממצאים</u>

3.1. נתונים כספיים

3.1.1. סעיף 213א לפקודת העיריות מגדיר מהו תקציב בלתי רגיל:

*"**תקציב בלתי רגיל** - תקציב של עירייה המיועד לפעולה חד-פעמית או לתחום פעילות מסוים, הכולל אומדן תקבולים ותשלומים לאותה פעולה או לאותו תחום פעילות, וכספים שיועדו על פי דין למטרות שאינן תקציב רגיל."*.

3.1.2. סעיף 213 (ב): *"<u>כספים של תקציב בלתי רגיל ינוהלו בנאמנות בידי ראש העיריה והגזבר, בנפרד מכספי חשבון התקציב שאינו בלתי רגיל; לא ייעשה כל שימוש בכספים של תקציב בלתי רגיל שלא למטרה שלשמה נועד, ובכלל זה לא ייעשו כל פעולות קיזוז בין כספים של תקציב בלתי רגיל לכספים של תקציב שאינו בלתי רגיל</u>[3], זולת בתום כל פעולה שלה יועד התקציב הבלתי רגיל; כספים של התקציב הבלתי רגיל אינם ניתנים לשעבוד שלא לטובת הפעולה שלה מיועד התקציב הבלתי רגיל'.*.

3.1.3. אגף מחשוב ומערכות מידע מנהל תקציב שוטף הכולל הוצאות שכר, הוצאות לקבלן שרותי מיקור החוץ - חברת "נ."[4] ותשלומים בגין תחזוקת מחשבים ועוד. בשנים 2013-2014 עמד תקציב האגף על 3,802 אלפי ₪ ועל 3,924 אלפי ₪, בהתאמה, וכן נעשו הוצאות של פרוייקטים שאושרו בתוכנית העבודה השנתית של האגף במסגרת כרטיסי התב"ר, וזאת כמפורט להלן:

	תקציב שנת 2013 ₪	**תקציב שנת 2014 ₪**	**שימוש עיקרי בסעיף התקציבי**
תקציב שוטף	3,802,436	3,924,000	שכר עובדי עירייה ועובדי חברת "נ."
תב"ר 2740012750	180,982	1,206,084	רכישת רישיונות, רכישת תשתיות תקשורת, תשלומים לחברות ייעוץ בגין פרויקטים
תב"ר 2730022751	1,325,047	624,532	רכישת ציוד מחשוב
<u>סה"כ תקציב</u>	**<u>5,308,465</u>**	**<u>5,754,616</u>**	

[3] הדגשת הביקורת

[4] שם החברה בניירות העבודה של הביקורת

ממצאים:

סעיף 213 (ב) לפקודת העיריות הקובע כאמור, כי לא ייעשה כל שימוש בכספים של תקציב בלתי רגיל שלא למטרה שלשמה נועד, ובכלל זה לא ייעשו כל פעולות קיזוז בין כספים של תקציב בלתי רגיל לכספים של תקציב שאינו בלתי רגיל. הביקורת מצאה בכרטסות התב"ר של האגף בשנים 2013-2014, תשלומים שוטפים ליועצים ולצרכי תחזוקה שוטפים שאינם עולים בקנה אחד עם הגדרת התב"ר המיועד לשדרוג מערכות מחשוב. (כמפורט בנספח א).

המלצה

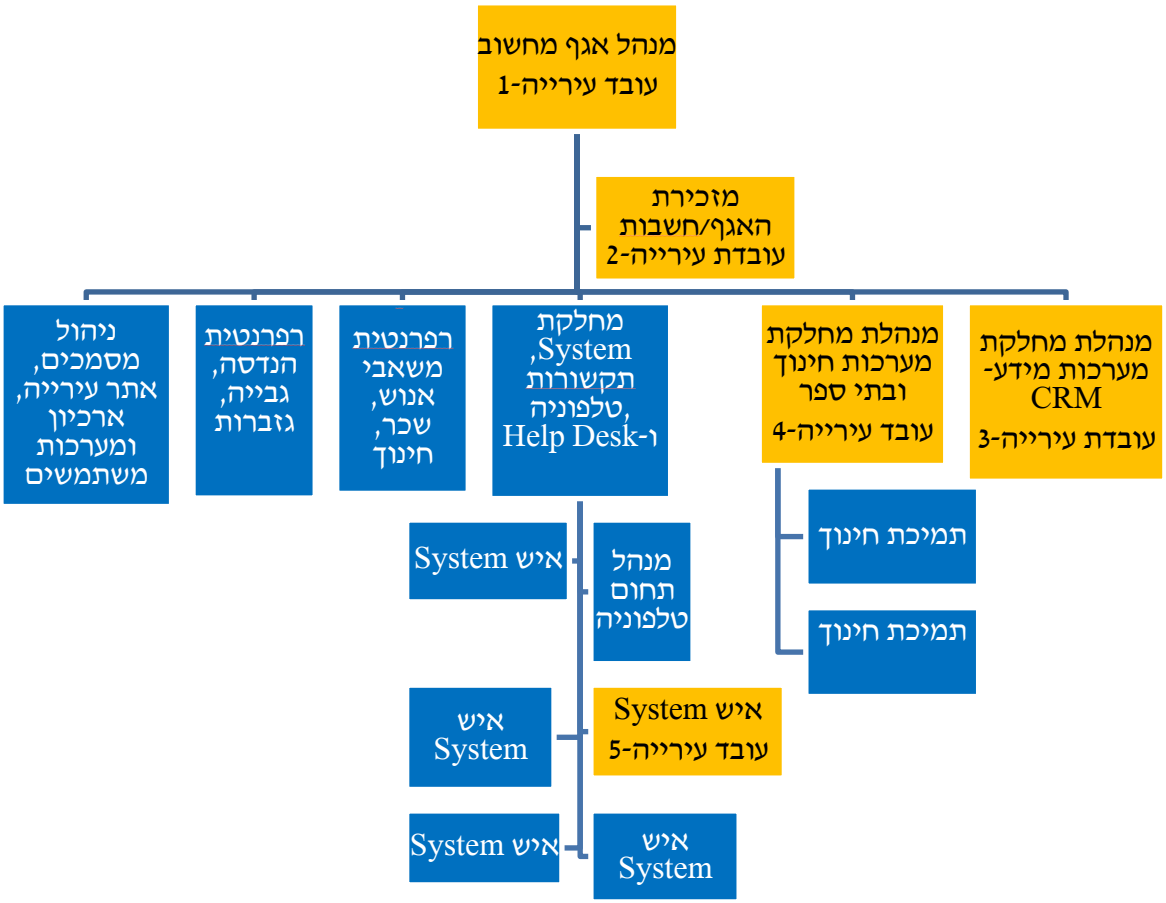
מומלץ כי גזברות העירייה בשיתוף מנהל האגף יימנעו הפקת הזמנות המחייבות את כרטיסי התב"ר ממערכת הרכש, כאשר נושאי ההזמנה מתייחס לתחזוקה/ייעוץ שוטף הניתן למחלקות העירייה/האגף. לחילופין, יש לשקול כי הפקת ההזמנות תבוצע על ידי מחלקת הרכש בעירייה אשר תבחין בין רכישת שרות/טובין שוטף לבין רכישות שאינן שוטפות אשר שייכות לתב"רים.

תגובת האגף: *"האגף נעזר בחשבים שהוקצו ע"י הגזברות והתקציב וחלוקתו (שוטף, תב"ר) נעשה על פי הנחיותיהם!.*

3.2. מבנה האגף

האגף מורכב מ-17 עובדים, בהם מנהל האגף, מנהלי מחלקות, מזכירת האגף, רפרנטים ואנשי תשתית. 5 מן העובדים הם עובדי עירייה ו-12 עובדי חברת "נ.".

להלן תרשים המבנה הארגוני של האגף:



לתיאור והגדרות התפקיד של עובדי האגף ראה פירוט בנספח ב'

<u>מקרא</u>:

- עובדי העירייה
- עובדי חברת "נ."

3.3. ניהול תכנית העבודה של האגף

תכנית העבודה של האגף מפורסמת במסגרת פרסום תכניות העבודה של העירייה.
בעת אישור התכנית מציג מנהל האגף לגזברות העירייה את הפרוייקטים הנדרשים ואת התקציב הנדרש ליישומם.
לאגף מחשוב ומערכות מידע תקציב תב"ר מאושר לשנים 2015-2019, בסך של 7,890 אלפי ₪ שנועד עבור שדרוג מערכות המידע.

3.3.1 בשנת 2014 ביצע האגף פעילות מקיפה במגוון רב של תחומים, אשר כללה בין היתר את הפרוייקטים הבאים: הקמת ארכיון עירוני לתכניות בניין, הטמעת מערכת ממוחשבת לאישור לטאבו, המשך פרוייקט עירוני לשדרוג כיתות אם לכיתות "חכמות" מתוקשבות בכל בתי הספר, שדרוג המוקד העירוני והפיכתו למערכת מידע אינטרנטית כלל עירונית, הטמעת מערכת לניהול תורים באגף הכנסות ועוד.

<u>האגף תוקצב בסך של 7,890 אלפי ₪ לפעילויות שדרוג מערכות המידע בחמש השנים (2015-2019). פעילויות אלו מתוקצבות על ידי גזברות העירייה באמצעות שני תב"רים. תקצוב זה, הנפרס על פני 5 שנים, דורש תכנית עבודה רב שנתית אשר תנוהל על ידי מנהל אגף מחשוב ומערכות מידע. מפניות שערכה הביקורת למנהל האגף, נמצא כי בידי מנהל האגף לא קיימת רשימה מפורטת מהם התחומים, פרוייקטים והעלויות אשר יבוצעו על ידי האגף תוך פירוט כיצד יבוצע ניצול תקציב זה על פני 5 השנים (2015-2019).</u>

<u>תגובת האגף</u>: *"קיימת תוכנית עבודה מפורטת אשר הוצגה לביקורת, עבור שנת 2106. בפרויקטים רב-שנתיים (כגון CRM, סריקת תיקי בניין וכדומה), בהן יש הוצאה תקציבית ידועה ומתוכננת, נעשו שירונים תקציביים בהתאם."*

<u>התייחסות הביקורת לתגובת האגף</u>: התוכנית הקיימת באגף, אינה מותאמת לתקציב האגף לשנים 2015-2019. מומלץ כי הנהלת העירייה תערוך בחינה כוללת/תסדיר עבור כלל אגפי העירייה את כל הקשור לתשומות הנדרשות עבור כל אגף, על מנת לעמוד ביעדים אשר הוצבו עבורם במהלך השנים הקרובות, תוך התייחסות לכלל המרכיבים: רגולציה, כמות התושבים להם ניתן השרות, התפתחויות טכנולוגיות צפויות, עלויות כספיות נדרשות ועוד.

בהסתמך על תכנית זו תעודכן תכנית האב למספר שנים עבור אגף מחשוב ומערכות מידע.

3.3.2 נמצא כי העירייה אינה נעזרת במערכת לניהול תכניות עבודה שמאפשרת מעקב יעיל אחר יישום התוכנית ויצירת תכנית ארוכת טווח כפי שמקובל ברשויות אחרות (כגון: עיריית א., עיריית ר.).

<u>המלצה</u>

מוצע לשקול שימוש במערכת לניהול משימות/פרוייקטים כפי שקיימת ברשויות אחרות, לשם פיקוח ובקרה יעילה אחר התקדמות הפרוייקטים, וזאת במסגרת תיעדוף הפרוייקטים אשר יבוצעו על ידי אגף מחשוב ומערכות מידע.

<u>תגובת האגף</u>: *"מערכת כזו נשקלה בעבר (מערכת לניהול משימות) הוחלט שלא לתקצבה במסגרת תקציב 2016 אלא להמתין להשקת ה CRM החדש תוך מקסום היכולות שלו עבור מעקב אחר משימות. יודגש, כי גם כיום מבוצעת בקרות על התקדמות תוכניות עבודה ומשימות ע"י מהנדסת התהליכים של העירייה. המערכות שנבדקו בעבר ונבדקות מדי פעם, אינם נותנות מענה מלא לנושא ומייקרות את התקורות והתשומות!*

3.3.3 נמצא כי לא הוטמעה במחלקת הביטוחים בגזברות העירייה, מערכת ממוחשבת לניהול תביעות, וזאת למרות הודעתו של גזבר העירייה לדוח ביטוחי העירייה אשר פורסם בדוח מבקר העירייה מס' 38 לשנת 2014, כי *"במהלך שנת 2015, תוטמע מערכת ממוחשבת לניהול תביעות, אשר עתידה להחליף את ניהול התביעות באמצעות הגיליון האלקטרוני ומערכת האופיס-לייט".*

גזבר העירייה מסר בתגובה, כי מנהלת הביטוחים התפטרה מתפקידה, וכי תפעול ושילוב הטמעת מערכת ממוחשבת לניהול תביעות מחייב גיוס של חצי תקן כוח אדם נוסף, דבר שיחייב הגדלה והקצאה תקציבית.

<u>המלצה</u>

במסגרת תיעדוף הפרוייקטים אשר יבוצעו על ידי אגף מחשוב ומערכות מידע מוצע לשקול אף הטמעת מערכת ממוחשבת לניהול תביעות אשר תיעל את עבודת המחלקה במתנהלת כיום באמצעות גיליונות אלקטרוניים.

<u>תגובת האגף</u>: *"מערכת כזו טרם הוטמעה לאור שיקולים תקציביים".*

3.4. מבנה ארגוני, קביעת מדיניות ומיפוי מידע

3.4.1 נמצא כי לא אוייש תפקיד מנהל אגף מחשוב ומערכות מידע במשך 11 חודשים. מנהל אגף מחשוב ומערכות מידע הקודם עזב בתאריך 30.4.2013 ותחילת העסקת מנהל אגף מחשוב ומערכות מידע שהיה בעת עריכת הביקורת, הייתה בתאריך 1.4.2014. הביקורת מציינת כי בזמן זה סמכויות האגף הואצלו למנהל מחלקת System וליועץ החיצוני (להלן: "היועץ"). והאחריות המנהלית הכללית הועברה למנהלת אגף משאבי אנוש, דאז.

<u>תגובת האגף</u>: *"לתגובת משא. להבנתי, מנהל האגף היוצא היה חולה תקופה ארוכה אך עדיין מועסק ורק לאחר שעזב ניתן היה לגייס עובד אחר במקומו."*

<u>המלצה</u>

מומלץ להנהלת העירייה לבצע תהליך הפקת לקחים בנוגע לאיוש משרות מרכזיות בעירייה בעתיד, זאת למרות הפתרון שנמצא בהעברת האחריות הניהולית למנהלת אגף משאבי אנוש, דאז.

<u>תגובת האגף</u>: *"ראה התייחסות מפורטת מעלה בנושא זה. הערה כללית: בתקופה שבה האגף נוהל ע"י מנהלת משא של העירייה הצליח האגף להגיע להישגים ניכרים והמשיך בתפקודו ואפ' ביצע מס' פרויקטים מרכזיים בהצלחה!*

<u>המלצה</u>

מומלץ להנהלת העירייה לבצע תהליך הפקת לקחים בנוגע לאיוש משרות מרכזיות בעירייה בעתיד, זאת למרות הפתרון שנמצא בהעברת האחריות הניהולית למנהלת אגף משאבי אנוש, דאז.

3.4.2 נוהל המסגרת לאבטחת המידע שנקבעו על ידי משרד ראש הממשלה,[5] קובע כי קיים צורך ב-"גורם מכוון" - ועדת היגוי לאבטחת מידע, שתפקידה בין היתר, להמליץ בדבר קווים מנחים, אישור נהלים מוצעים, הכוונה בקביעת מדיניות בדבר הרשאות גישה למידע וקביעת האירועים והפעילויות החריגות, שמהווים סיכון בכוח או בפועל, לניהולו התקין של המשרד. **<u>נמצא כי בעירייה לא פועלת ועדת היגוי וזאת בניגוד לנוהל המסגרת לאבטחת המידע ולמקובל ברשויות אחרות (כגון בערים: ר., א. ועוד)</u>.**

[5] כמוזכר בסעיף 1.1 ה-ו לדוח

<u>המלצה</u>

מומלץ כי מנהל האגף יפנה להנהלת העירייה לשם הקמת וועדת היגוי אשר תהיה אחראית על התווית מדיניות בכל הקשור לתחום אבטחת המידע בעירייה, כפי שמקובל ברשויות אחרות. וועדה זו תאשרר את מדיניות העירייה ותעגן את מדיניות זו בנהלי עבודה מתאימה אשר יישומו על ידי עובדי האגף.

<u>תגובת האגף</u>: *"לא משוכנעים כי הוראות מסמך ראש הממשלה בנושא זה, תקפים ומחייבים גם את העיירה. בכל מקרה, הנושא ייבדק ובהתאם יוחלט על הקמת וועדת היגוי כאמור."*

<u>התייחסות הביקורת לתגובת האגף</u>: הביקורת מציינת בהתייחס לתגובת האגף את הערת מבקר המדינה בדוח ביקורת משנת 2014 בנושא "ניהול רשומות אלקטרוניות ורשומות נייר ברשויות מקומיות", בה קבע: ***"הנהלים המובאים באתר מחייבים את מוסדות המדינה, ומכאן שהם חלים גם על הרשויות המקומיות."***

3.4.3 נמצא כי לא נערך תיעוד לישיבות הצוות השבועיות של האגף, דבר שעלול לגרום לאי סדרים בקביעת סדרי העבודה ואופן חלוקת העבודה בין העובדים השונים, וכן לחוסר תיאום וחוסר ביצוע של חלק מהמשימות המוטלות על האגף.

<u>המלצה</u>

מומלץ כי בסיום ישיבות האגף יופק פרוטוקול המציג את ההחלטות שהתקבלו, לוחות זמנים והגורם המבצע, וזאת לשם מעקב ותיאום בין עובדי האגף.

<u>תגובת האגף</u>: *"בצד מחלקת התשתיות קיימת רשימת מעקב מסודרת המתעדכנת לפחות אחת לשבוע עבור כלל משימות המחלקה. זאת בנוסף למערכת מעקב הפניות לקבלת שרותי תמיכה."*

3.4.4 נוהל מס' 1 סעיף ט' במסמך המדיניות הקיים באגף, קובע כי מנהל האגף יערוך פעולות ביקורת ובקרה וזאת כחלק מהגדרת תפקידו. הביקורת מעירה כי לא נמצא כי אכן מנהל האגף עורך בקרה אחר פעילויות הרפרנטים באגפי העירייה וזאת, לאור חשיבות תפקידם כגורם האחראי על הממשק בין האגף ליתר מחלקות העירייה.

<u>המלצה</u>

מומלץ כי אחת לרבעון מנהל האגף יערוך סקר בקרה בו יבחן את פעילויות וביצועי הרפרנטים הפועלים באגפי העירייה, תוך קיום ישיבות עם משתמשי מפתח להם מעניקים עובדי האגף שרותים.

<u>תגובת האגף</u>: *"מנהל האגף מבצע פגישות תקופתיות אחת לשבוע-שבועיים עם כל אחד מהרפרנטים. במסגרת זו מבוצעת בקרה אחר משימות, קידומן, בעיות ופתרונן."*

3.4.5 נוהל מספר 10 בנהלי המסגרת, קובע כי יש לבצע בדיקה תקופתית של תשתיות התקשורת במשרד, באמצעות הרצת תוכנות חדירה אחת לתקופה כפי שייקבעו על ידי האגף, **<u>נמצא כי בשנים המבוקרות לא בוצעו על ידי האגף בדיקות חוסן שמטרתן בחינת רמת הפגיעה של השרתים ורמת החשיפה של מחשבי העירייה לפריצות מן החוץ, כפי שמקובל ברשויות אחרות</u>**.

<u>המלצה</u>

מומלץ כי במסגרת תיעדוף הפרוייקטים אשר יבוצעו על ידי אגף מחשוב ומערכות מידע ייבחן שוב הצורך בבדיקות חוסן וזאת עקב המידע הרגיש הקיים במאגרי העיריה (כגון: רשימת מטופלים באגף הרווחה, רשימת תלמידים באגף החינוך).

<u>תגובת האגף</u>: *"דרישה לבדיקות כנ"ל התבקשה אך לא אושרה במסגרת תקציב 2016."*

3.4.6 נוהל מס' 1 בנהלי המסגרת, קובע כי מסמך מדיניות אבטחת המידע בעירייה מתייחס לכלל היבטי אבטחת המידע בעירייה. נמצא כי מסמך המדיניות הקיים באגף חסר היבטים כגון:

- אופן פעילות והתדירות התכנסות ועדת ההיגוי העירונית בתחום ניהול מערכות המידע, זהות המשתתפים בוועדה זו, תדירות התכנסות, תפקדי חברי הוועדה ועוד.
- הרשאות צפייה באתרי אינטרנט ייחודיים, כגון: Facebook, YouTube, תחנות רדיו. יצויין כי שימוש באתרי אינטרנט מעין אלה יוצר עומס רב על רשת התקשורת ומאט את פעילותה, ומאפשר גישה חופשית לעובדים בעירייה לאתרים, כגון אלה.
- התחברות המשתמשים מחוץ למשרדי העירייה, הנותנים שירותי מיקור חוץ לעירייה, כולל התייחסות לגורמים המורשים להתחבר.
- אופן שימוש במחשבים ניידים;

- אופן שימוש בטלפון נייד המחובר למאגרי העירייה.

<u>המלצה</u>

מומלץ כי יתקיים דיון לבחינת ולהשלמת תכולת הסוגיות המרכיבות את מסמך מדיניות האגף, על מנת שיכיל את כלל מרכיבי אבטחת המידע. מסמך זה יידון ויאושר במסגרת פעילות ועדת ההיגוי.

<u>תגובת האגף</u>: *"הקמת וועדת היגוי לאור המלצת המבקר מקובלת בכפוף לאשור המנכ"לית.*

לאחר שאושרה מסגרת מדיניות אבטחת המידע - וועדת ההיגוי תאשרר כל נוהל ו/או בקרה שיופעל בעירייה כנגזרת ממסמך המדיניות."

3.4.7 הביקורת ביצעה סקר מדגמי של בחינת תפקידי העובדים באגף, ונמצא כי קיימת הגדרה ברורה עבור כל עובד ושיוך של המערכת עליה הוא אחראי והמשתמשים להם הוא מעניק תמיכה - לביקורת אין הערות בנושא זה.

3.5. סקרי סיכונים

3.5.1. נוהל מספר 3 בחוברת נהלי המסגרת[6], שעניינו "סקרי סיכונים - ניהול והערכה", קובע כי על האגף לערוך סקר סיכונים שמטרתו לאתר את הסיכונים לארגון ולהעריך את חומרתם. זאת, על מנת לאפשר קבלת החלטה מבוססת באיזה סיכונים לטפל, מהו סדר העדיפות לטיפול בסיכונים, מהי העלות ומהו לוח זמנים. הנוהל ממליץ להעריך סיכונים כשלב מקדים בתהליך עיצוב מדיניות אבטחת מידע כאשר תוצאות ההערכה יסייעו לקבוע מהן פעולות האבטחה שראוי לנקוט וישמשו כאמצעי לקביעת קדימויות להקצאת המשאבים.

3.5.2. סעיף 4.1.2 למסמך מדיניות אבטחת המידע בעירייה, קובע כי *"לאחר אישור מסמך המדיניות תתבצענה הפעילות הבאה על ידי מנהלת אבטחת המידע בארגון [...] ביצוע סקר סיכונים ומבדקי חדירה"*, אך אין התייחסות לתדירות ואופן עריכת הסקר.

<u>המלצה</u>

מומלץ כי ועדת ההיגוי תעגן את נושא סקרי הסיכונים במסגרת מסמך מדיניות האגף תוך התייחסות לתדירות הסקרים, ותכולתם.

---

[6] ראה סעיף 1.1 ה

<u>תגובת האגף</u>: *"לא משוכנעים כי הוראות מסמך ראש הממשלה בנושא זה, תקפים ומחייבים גם את העירייה. הנושא ייבדק ובהתאם יוחלט עם הקמת וועדת היגוי כאמור."*

<u>התייחסות הביקורת לתגובת האגף</u>: הביקורת מציינת בהתייחס לתגובת האגף את הערת מבקר המדינה בדוח ביקורת משנת 2014 בנושא "ניהול רשומות אלקטרוניות ורשומות נייר ברשויות מקומיות", בה קבע: ***"הנהלים המובאים באתר מחייבים את מוסדות המדינה, ומכאן שהם חלים גם על הרשויות המקומיות."***

3.5.3. בעירייה בוצע סקר סיכונים במהלך השנים 2013-2014 על ידי מבקר העירייה. הסקר מציין כי קיימים סיכונים ברמה גבוהה עבור התהליכים הבאים:

- מידע רגיש נחשף לעובדים בלתי מורשים ועלול גם לזלוג מחוץ לרשות;
- במערכות המידע ימצא מידע שגוי אשר יביא לקבלת החלטות שגויות או לתהליכים תפעוליים שגויים;
- אובדן מידע ונתונים וכתוצאה מכך פגיעה בפעילות העירייה, כאשר בחלק מהרשתות קיימות תלונות על איטיות הרשת;
- היעדר אמצעים לבקרת גישה פיזית לרשת (NAC);

<u>לא נמצאה התייחסות כוללת בתוכניות העבודה של האגף לממצאי הסקר</u>, שתפקידם לשמש את האגף כאמצעי לקביעת קדימויות להקצאת המשאבים.

<u>תגובת האגף</u>: *"בוצעו מספר פעולות כלקח ממצאי הסקר - הוגדלו קצבי התקשורת, הותקנה מערכת PRTG, הוקם מערכת שרתים ו - DR ועוד, לא בא לידי ביטוי בממצאי הבקרות. תוכנית העבודה 2016 לקחו בחשבון והתייחסו לממצאים הנ"ל. בין השאר התבקש תקציב עבור מבחני חדירה, מערכת NAC ועוד. הבקשות אושרו חלקית בלבד".*

<u>המלצה</u>

מומלץ כי תכנית העבודה השנתית והרב שנתית של האגף תתבסס בכל הקשור לסדרי קדימויות הפרויקטים על סקרי הסיכונים המבוצעים באגף.

3.6. רישום מצאי המחשבים

3.6.1. נמצא כי מערכת ה - A.D. מאפשרת הצגת כללי מצאי המחשבים הקיים בעירייה, רשימה זו אינה מועברת למחלקת הרכש והמצאי בעירייה לשם עדכון מערכת המצאי.

<u>המלצה</u>

מומלץ כי אגף מחשוב ומערכות מידע יעדכן את מחלקת הרכש בכל תנועות המלאי, וכי אחת לתקופה תיעשה השוואה בין רישומי מצאי המחשבים הקיימים באגף לבין רישומי המצאי הקיימים במחלקת הרכש.

<u>התייחסות האגף</u>: *"ההמלצה הזו מקובלת ומבוצעת בפועל."*

3.6.2. מדוח מצאי המחשבים שנתקבל ממנהל האגף נמצאו עשרות מחשבים המופעלים באמצעות מערכת הפעלה WINDOWS XP על אף, שהיא אינה מאובטחת על ידי חברת MICROSOFT החל מחודש 3/2014. משמעות הדבר היא כי משתמשים בעלי תחנות העובדות במערכת הפעלה WINDOWS XP, חשופים לפגיעה של וירוסים לעומת משתמשים בעלי מערכות הפעלה אשר מאובטחות על ידי חברת MICROSOFT, היות ומערכות אלו מעודכנות בתוכנות אשר מונעות כניסות וירוסים (קרוי גם: "Patch").

<u>המלצה</u>

מומלץ כי במסגרת תעדוף הפרוייקטים אשר יבוצעו על ידי אגף מחשוב ומערכות מידע ייבחן הצורך בעדכון כלל תחנות העבודה של המשתמשים למערכת הפעלה מתקדמת אשר נתמכת על ידי חברת MICROSOFT.

<u>תגובת האגף:</u> *"פעילות זו מבוצעת ומוגדרת כחלק מתוכניות העבודה של האגף לשנת 2016. בין השאר הוקצה משאב לצורך ביצוע השדרוגים הנל. כבר קיים נותרו כ-30 מחשבי XP בשימוש העירייה."*

3.7. גיוס עובדים והדרכות

על מנת להפחית טעויות אנוש או שימוש לרעה במידע שנאגר במשרד יש להציג את נושא אבטחת מידע ונושא שמירת הסודיות בשלב גיוס העובדים ועל נושאים אלה להיכלל בחוזי ההעסקה של העובדים. יתרה מכך, עם תחילת

עבודתו של העובד ועד סיום העסקתו יש לנטר פעילותו בנושאים אלה באופן תקופתי.

נוהל מס' 6 בחוברת נהלי המסגרת, שעניינו *"בדיקת מהימנות העובדים, התחייבות לשמירת סודיות"* (להלן: *"נוהל מס' 6"*), קובע כי *"תנאי ההעסקה יציינו את אחריותו של העובד לאבטחת מידע. אם אפשר, האחריות תהיה תקפה למשך תקופה מוגדרת לאחר גמר העסקתו במשרד. יפורט גם איזו פעולה יש לנקוט במקרה שהעובד אינו מציית לדרישות האבטחה. הזכויות והחובות של העובד בנושא אבטחה, כגון על פי שמירת דיני זכויות יוצרים והחקיקה בנושא הגנת נתונים, יובהרו ויכללו בין תנאי העסקתו [...] אם אפשר, תנאי ההעסקה יכללו גם הצהרה שאחריות חלה על העובד גם מחוץ לכותלי המשרד וגם מעבר לשעות העבודה הרגילות, כגון במקרה של עבודה בבית."*

עוד נקבע בנוהל מס' 6 כי *"כל מועמד פוטנציאלי לעבודה יתוחקר כראוי, במיוחד עבור תפקידים רגישים."*

מנתוני אגף משאבי אנוש, בשנת 2014 נקלטו בעירייה 449 עובדים חדשים ועזבו את העירייה 232 עובדים.

3.7.1 נמצא כי לא קיים נוהל עבודה חוצה ארגון המעגן את ממשק העבודה בין אגף משאבי אנוש לבין אגף מחשוב ומערכות מידע בכל הקשור לקליטה ועזיבת עובדים.

<u>המלצה</u>

מומלץ להשלים ולהסדיר את הממשק בין אגף משאבי אנוש ואגף מחשוב ומערכות מידע בנוגע לקליטת/עזיבת עובדים ולגבותו בנוהל עבודה חוצה ארגון. כמו כן, יש צורך שבטפסים היעודיים יצויינו ההרשאות והמערכות הנדרשות שיש להוסיף/להסיר לעובד עם גיוסו או עזיבתו את התפקיד.

<u>תגובת האגף</u>: *"ההמלצה מקובלת."*

3.7.2 הביקורת ביקשה לבחון האם מבוצעת חתימה על טפסי סודיות של עובדים הנקלטים באגף משאבי אנוש. הביקורת ערכה מדגם של 6 עובדים חדשים אשר

נקלטו בעירייה ומצאה כי אכן העובדים חתמו על טופס התחייבות והצהרת סודיות.[7]

3.7.3 נמצא כי לא נערכות הדרכות לעובדים חדשים בנושא אבטחת מידע וכי המשתמשים אינם מודעים לדרישות העירוניות בנושא אבטחת המידע, זאת בניגוד לנוהל מס׳ 8 בחוברת נהלי המסגרת שעניינו *"מודעות, הדרכה, הטמעה והסברה."* וכי העלאת מודעות עובדי העירייה לנושא אבטחת המידע נעשית באמצעות הפצת חומרי אבטחת מידע בדואר הפנימי. בין החודשים ינואר-אוגוסט 2015 נשלחו 17 התראות במגוון נושאים שונים, כגון מתקפת וירוס, טלפוניה, עבודת שרתים, קבצים תקולים ועוד.

3.7.4 הביקורת מצאה כי ברשימת משתמשי ה-A.D מופיעים גורמים שאינם עובדי עירייה. להלן תיאור החריגים:[8]

- ספקים המעניקים שירותים לעירייה - נמצאו 4 ספקים המעניקים שירותי תמיכה ליישומים אך בעלי גישה לרשת המשתמשים. מצב זה מייצר סיכון כי גורם שאינו עירוני יהיה חשוף לנתונים רגישים ברשת המשתמשים, כגון: נתוני מטופלי רווחה, או רשימות תלמידים שעניינם נדון בוועדות השמה.
- משתמשים בעל שם משתמש כללי ולא ייחודי - נמצאו משתמשים כלליים אשר ניתנים לשימוש של 2 עובדים או יותר. מתן שם משתמש כללי למספר עובדים אינו מאפשר זיהוי הגורם שביצע את הפעולה באופן חד ערכי. כך, נוצר סיכון כי משתמשים אלו יבצעו עבירות אבטחת מידע ולא יתאפשר זיהוי וודאי של הגורם שביצע את הפעולה.

<u>תגובת האגף</u>: *"חלק מן המשתמשים משמשים לכתיבת דואר אלקטרוני בלבד ואינם בעלי הרשאות."*

<u>המלצה</u>

מומלץ כי מנהל האגף/סגנו יפעלו לבחינת כלל המשתמשים הגנריים, וכן המשתמשים המשוייכים לספקים, אחת לרבעון. בנוסף, מומלץ כי תבוצע בחינה על ידי מנהל אגף מחשוב ומערכות מידע, לגבי הצורך בהקמת משתמשים, עבור ספקים חיצוניים והבקרות הקיימות על פעילותם.

[7] טבלה מרכזת של המדגם נמצאת בניירות העבודה של הביקורת
[8] טבלה מרכזת של רשימת המשתמשים החריגים נמצאת בניירות העבודה של הביקורת

3.7.5 אחת הדרכים לאיתור משתמשים שעזבו אך לא דווחו לאגף היא סריקה רבעונית של משתמשים אשר לא ביצעו כל כניסה לרשת במהלך הרבעון. הדבר אף נדרש, בהתאם לנוהל מס׳ 13 בנהלי המסגרת. לדברי מנהל מחלקת System, בשנת 2015 אגף מחשוב ומערכות מידע לא ביצע כלל ביטול או הקפאה של משתמשים שלא עשו שימוש במשאבי המחשוב. אי ביצוע ביטול או הקפאה של משתמשים שלא עשו שימוש במשאבי המחשוב, מייצר סיכון כי משתמשים לא מורשים עלולים לבצע פעולות בשם משתמש שעזב את העירייה.

<u>המלצה</u>

מומלץ כי מנהל האגף/סגנו ייבצעו סקירה רבעונית של משתמשים שלא עשו שימוש במשאבי המחשוב, לשם בחינה האם המדובר במשתמשים שעזבו את העירייה ולא דווחו לאגף מחשוב ומערכות מידע.

3.7.6 משתמשים בעלי הרשאת Admin הם, בין היתר, משתמשים בעלי הרשאה להקים/להסיר משתמשים וכן בעלי אפשרות עריכה בכלל תיקיות הרשת. כל משתמשי ה-Admin ברשימת ה-ADMIN USERS הם עובדי האגף - **נמצא תקין**.

3.8. טיפול בתקלות

לצורך טיפול בתקלות, עובדי אגף מחשוב ומערכות מידע, נעזרים במערכת אינטרנטית חינמית SPICE WORKS. עבור כל פנייה נרשמת קריאה במערכת, כאשר סגן מנהל האגף מסווג את הקריאות ומקצה אותן לעובד המתאים להמשך טיפול. כל עובד, סוגר את התקלות ששוייכו אליו. תיקון התקלות נבדק על ידי סגן מנהל אגף מחשוב ומערכות מידע.

ממצאים:

3.8.1 נמצא כי המערכת אינה כוללת פרמטר המגדיר מהו התקן/משך הזמן הרצוי לפתרון כל תקלה. היות ולא קיים במערכת, פרמטר/תקן המגדיר את פרק הזמן לטיפול בכל תקלה. אי קיום פרמטר זה הקרוי : SLA-(Service Level Agreement) אינו מאפשר בקרה וניהול של מנהל אגף מחשוב ומערכות מידע אחר זמני הטיפול בתקלות של העובדים.

<u>המלצה</u>

מומלץ לבחון מערכת ייעודית לטיפול בתקלות אשר תכיל בין היתר אפשרות להזנת מדדי זמן טיפול בתקלות, לחילופין, יבחן האגף שימוש במערכת מוקד השרות הקיימת בשימוש העירייה.

<u>תגובת האגף</u>: *"המערכת הנל הינה מערכת ייעודית לטיפול בפניות Help Desk אשר נעשה בה שימוש במספר רב של ארגונים. מקובלת דרישת הביקורת להוסיף מעקב SLA אחר פניות במערכת!*

3.8.2 בתאריך 3.8.2015 הפיקה הביקורת דוח המציג את כלל הקריאות הפתוחות. מדוח זה נשלפו באופן אקראי תקלות שזמן הטיפול בהן ארך מעבר ל-50 יום. נמצא תקין כי התקלות שהוצגו בדוח זה הינן תקלות מורכבות אשר הזמן לתיקונן אורך מעבר ל-50 יום.

לביקורת אין הערות.

3.9. התחברות ספקים מרחוק והשתלטות מרחוק

3.9.1 סעיף 6.5 למסמך מדיניות אבטחת המידע בעירייה קובע כי: *"גישה למידע מארגון ומבחוץ תהיה מותנית בהרשאות מתאימות הנגזרות מהתפקיד לסקור/לצפות/לנהל/לערוך/לעבד את המידע. שימוש במערכות המידע של העירייה מותנה בהזדהות אישית חד משמעית של המשתמש ובאמצעים טכנולוגיים העומדים לרשות העירייה."*

3.9.2 נמצא כי, בניגוד לרשויות אחרות, לא קיימים בעירייה כלי ניטור - כלי NAC- (Network Access Control) המציגים בפני מנהל אגף מחשוב ומערכות מידע את הגורמים אשר התחברו למערכות המידע, את הפעולות שביצעו, את שעת הכניסה, שעת היציאה ועוד. על כן, האגף אינו מודע למהות השינויים/צפייה בנתונים רגישים המבוצעת על ידי הספקים. לטענת האגף, הניטור כיום מבוצע באמצעות ה-EVENT LOG המנטר כניסות ברמת מערכת ההפעלה. הביקורת סבורה כי מצב זה יוצר סיכון שמבוצעת התחברות ספקים באופן שאינו מבוקר על ידי האגף. קרי, אין מידע מיהו הגורם אצל הספק המבצע את ההתחברות, מהו המאגר אליו הוא מתחבר, מהם הנתונים שנצפו על ידו, ומהו השינוי המבוצע על ידו.

<u>המלצה</u>

מומלץ כי במסגרת תעדוף הפרוייקטים אשר יבוצעו על ידי אגף מחשוב ומערכות מידע ייבחן הצורך ברכישת כלי NAC אשר יאפשרו ביצוע ניטורים אחר כניסות משתמשים למערכות המידע. כמו כן, נושא התחברות הספקים והגורמים הרשאים לאשר לספקים התחברות זו יעוגנו בנהלי האגף.

<u>תגובת האגף</u>: *"הבקשה לתקצוב כלי NAC עלתה כחלק מדרישות תקציב 2016 ואושרה חלקית בלבד, במסגרת תיעדוף התקציב לשנת 2016."*

3.10. מדיניות סיסמאות ברשת המשתמשים

לפי נוהל מס' 13 בנהלי המסגרת, *"לא יתאפשר לעבור מיישום ליישום... אלא דרך התפריט הראשי ומערכת הסיסמאות."* נוהל זה מכתיב מדיניות סיסמאות רצויה.

ממצאים:

3.10.1 להלן הוראות נוהל מסגרת מול מדיניות הסיסמאות כפי שהיא מוגדרת באגף:

נושא הבדיקה	נהלי מסגרת	מדיניות סיסמאות ברשת באגף מחשוב ומערכות מידע
מס' דורות סיסמאות	4	6
כמות תווים	6	6
אילוץ להחלפה כל מס' ימים	90 ימים	90
מורכבות סיסמה תווים רצופים אותיות ומספרים	כן	אין
הגבלת מס' ניסיונות כניסה	3	אין

3.10.2 לא קיים נוהל המגדיר מהי מדיניות הסיסמאות אשר העירייה מעוניינת ליישם ברשת המשתמשים. נדרש כי, נושא המדיניות יעוגן בנוהל עבודה וזאת בנוסף לסעיף 6.5.1 לנוהל העבודה הקיים באגף הקובע כי: *"שימוש במערכות המידע של העירייה מותנה בהזדהות אישית חד משמעית של המשתמש."*

3.10.3 נמצא כי קיימת אי התאמה בין קביעת נהלי המסגרת לבין יישום מדיניות הסיסמאות ברשת המשתמשים. דבר זה מייצר סיכון כי משתמשים המעוניינים להתחקות אחר סיסמתם של משתמשים אחרים יוכלו לעשות זאת בקלות.

להלן אי ההתאמות שנמצאו:

- בניגוד לנוהל המסגרת הקובע צורך בהרכבת סיסמא שתהיה מורכבת מתווים, אותיות ומספרים. באגף, אין הגדרה של מורכבות הסיסמא (הפונקציה מושבתת - disabled).
- בניגוד לנוהל המסגרת המגדיר הגבלה ל-3 ניסיונות כניסה למערכת, באגף אין הגבלה על מספר ניסיונות הכניסה לחשבון משתמש (הפונקציה מושבתת - disabled). לכן גם במידה והמשתמש שגה מספר רב של פעמים, לא תתבצע כלל, נעילה של החשבון.

<u>המלצה</u>

מומלץ כי ועדת ההיגוי תגדיר את מדיניות הסיסמאות ברשת המשתמשים, במסגרת מסמך מדיניות האגף, כפוף לנהלי אבטחת המידע של משרד ראש הממשלה.

<u>תגובת האגף</u>: *"קיימת אכיפת סיסמאות מוגבלת ע"י שימוש בכלי Microsoft. במהלך שנת 2015 הוקשחו דרישות הסיסמאות. מקובלת דרישת הביקורת להקשחה נוספת של מדיניות הסיסמאות והפעלת תכונות הקשחה נוספות כאמור."*

3.11. בקרה ופיקוח לוגי על פעולות ברשת

3.11.1 נוהל מס' 15 בחוברת נהלי המסגרת, שעניינו *"בקרה ופיקוח לוגי"* (להלן: "נוהל מס' 15"), מגדיר "בקרה לוגית" כ-*"ניטור שוטף ממוחשב אחר הפעילות במערכת הממוחשבת, תוך התמקדות באירועים חריגים או רגישים." "פיקוח לוגי" מוגדר כ-"מעקב אחר פעילויות במחשב גם לאחר ביצוע הפעילות ובהשהיית זמן כלשהו."*

3.11.2 נוהל מס' 15 ממליץ כי-*"יוגדרו במערכת פעולות חריגות או רגישות...ההגדרה תכלול ניסיונות סרק לכניסה למערכת וכן ניסיונות לבצע פעולות בלתי מורשות אחרות...הגדרת הפעילויות החריגות תיבדק ותתעדכן לפחות אחת לשנה."*

3.11.3 כמו כן, נוהל מס' 15 ממליץ כי במערכת יישמר יומן (LOG) של כל הפעילויות באמצעות תוכנה ייעודית, וכי ה-"לוגים" ינותחו אחת לשבוע באמצעות כלים ממוכנים וממצאים חריגים יועברו באופן מיידי לממונה לאבטחת מידע, שיערוך בירור דחוף לגביהם.

ממצאים:

3.11.4 נמצא כי לא קיימת הגדרה לאירועי אבטחה/פעילויות חריגות (כגון: טעויות חוזרות בכניסה למערכת, פעילות בשעות הלילה וכו'). לפיכך, כלל לא נבחנים אירועים חריגים על ידי אגף מחשוב ומערכות מידע. יתר על כן, נמצא כי נכון לתקופת עריכת הביקורת, כלל לא נשמרים לוגים בעירייה. לדברי מנהל התשתיות של אגף מחשוב ומערכות מידע, לא מתבצע תחקור של יומן ההתראות של המערכות השונות במחלקת תשתיות של האגף.

<u>המלצה</u>

מומלץ כי במסגרת תעדוף הפרוייקטים אשר יבוצעו על ידי אגף מחשוב ומערכות מידע ייבחן הצורך ברכישת כלי NAC אשר יאפשרו ביצוע ניטורים, ואיסוף לוגים אחר פעולת המשתמשים. בנוסף, מערכת זו תאפשר ניתוח ובקרה אחר אירועי אבטחת מידע חריגים אשר יוגדרו במסגרת נהלי אגף מחשוב ומערכות מידע.

<u>תגובת האגף</u>: *"הבקשה לתקצוב כלי NAC עלתה כחלק מדרישות תקציב ואושרה חלקית בלבד במסגרת תעדופי התקציב לשנת 2016. על מנת לביצוע ניטור ותיחקור מומלץ להטמיע מערכות SIM SOC/IPS /IDS - אשר תקציב נדרש עבורן אושר חלקית בלבד."*

3.12. השמדת מסמכים ואמצעים מגנטים

נוהל מס' 20 לחוברת נהלי המסגרת, קובע כי *"ההשמדה תתבצע באופנים הבאים: מחיקה, גריסה ע"י מכונת גריסה מיוחדת למדיה מגנטית/אופטית, שריפה."*

ממצאים:

3.12.1 לדברי סגן מנהל אגף מחשוב ומערכות מידע במקרים של דיסקים/קלטות גיבוי תקולים לא מבוצעת השמדה באמצעות מגנוט של הדיסק כפי שמקובל.

<u>המלצה</u>

מומלץ כי השמדת דיסקים תבוצע באמצעות מגנוט וכי השמדת אמצעים מגנטיים אחרים תבוצע באמצעות מכונת גריסה ייעודית/שריפה תוך ביצוע רישום מתאים.

<u>תגובת האגף</u>: *"תבחן הצעת הביקורת ויישומה."*

3.13. גיבוי, שחזור והתאוששות

3.13.1 נוהל מס' 29 בחוברת נהלי המסגרת, בנושא "*תכניות התאוששות מאסון*" (להלן: "נוהל מס' 29") דן בהגנה על תהליכים קריטיים מהשפעת כשלים רציניים או מקרי אסון. המטרה היא להקטין נזקים במקרה אסון, להקטין הוצאות ביטוח ולהגביר מודעות להגנת המערכות. נוהל מס' 29 ממליץ על הדברים הבאים: הכנת תכניות התאוששות, שיפותחו על ידי צוות היגוי, הגדרת אתר חלופי כתשובה לתרחיש של אסון מלא שלא יאפשר כלל להשתמש באתר הקבוע וכן, עריכת תרגיל מקיף של כלל היבטי ותחומי התכנית אחת לשנה.

3.13.2 בשנת 2014 הוקם מערך DR מלא המאפשר כתיבה בו זמנית של המשתמשים לסביבת העבודה ובמקביל לאתר ה-DR.

3.13.3 נמצא כי באגף לא נכתב נוהל DRP, הקובע כיצד על מערך המחשוב והתקשורת להיערך להמשכיות תפעולית במקרה של כשל, כגון: שריפה, שיטפון, רעידת אדמה או כל אירוע סביבתי אחר, כמו כן, נמצא כי לא קיימת באגף רשימת שרתים וציוד מעודכנת אליה פונים במצב חירום.

3.13.4 בשנים 2014-2015 לא בוצע תרגיל התאוששות מאסון הבוחן את האפשרות של המשתמשים לעבוד ישירות מול אתר ה-DR, בעת קריסת חדר המחשבים המרכזי.

<u>המלצה</u>

מומלץ כי האגף יכתוב תוכנית התאוששות מאסון אשר תובא לאישור ועדת היגוי. תוכנית זו, תכיל, בין היתר, רשימה של שרתים וציוד אליה פונים במצב חירום, כמו כן, תדירות בחינת התוכנית תעוגן אף היא במסגרת נהלי העבודה של האגף.

<u>תגובת האגף</u>: "*מקובלת המלצת הביקורת. במסגרת תוכנית העבודה יכתב נוהל DR מסודר שכבר החלה כתיבתו.*"

3.14. אבטחת מידע והגנת הפרטיות

המחוקק נתן דעתו להיבטים שונים של אבטחת מידע, והדבר בא לידי ביטוי בחוק הגנת הפרטיות, התשמ"א-1981 (להלן: "**חוק הגנת הפרטיות**") ובחוק המחשבים, התשנ"ה-1995.

א. להלן הגדרות לפי סעיף 7 לחוק הגנת הפרטיות:

*"'**אבטחת מידע**'- הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין;*

*"**מאגר מידע**'- אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט*

(1) אוסף לשימוש אישי שאינו למטרות עסק; או

(2) אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר אפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף;

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

*"**מידע רגיש**'-*

(1) נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו;

(2) מידע ששר המשפטים קבע בצו, באישור ועדת החוקה חוק ומשפט של הכנסת, שהוא מידע רגיש;

*"**מנהל מאגר**'- מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לענין זה;*

*"**רשם**'- מי שמתקיימים בו תנאי הכשירות למינוי שופט של בית משפט השלום, והממשלה מינתה אותו, בהודעה ברשומות, לנהל את פנקס מאגרי מידע (להלן - הפנקס) כאמור בסעיף 12;*

*"**שלמות מידע**'- זהות הנתונים במאגר מידע למקור שממנו נשאבו, בלא ששונו, נמסרו או הושמדו ללא רשות כדין."*

ב. דוח מספר 62 לשנת 2011 של מבקר המדינה, שעניינו *"אבטחת מידע והגנת הפרטיות ברשויות מקומיות,"* קובע כדלקמן: *"במשך שנים לא קבע משרד הפנים מדיניות לאבטחת המידע ולהגנת הפרטיות ברשויות המקומיות; לא הניח את התשתית לטיפול בנושא; ולא פעל לקביעת הנחיות בתחום זה, אף שכבר בשנת 1996 תוקן חוק הגנת הפרטיות ונוספו לו סעיפים הנוגעים להגנה על הפרטיות במאגרי מידע. [...] הרשות למשפט, טכנולוגיה ומידע שבמשרד המשפטים לא קיימה מאז הקמתה פעולות פיקוח ואכיפה על רישום מאגרי מידע. כמו כן היא לא קבעה נהלים והנחיות ולא הטילה קנסות על רשויות מקומיות שלא קיימו את חובתן זו."*

ג. סעיף 8(ג) לחוק הגנת הפרטיות מחייב את העירייה ברישום של מאגרי מידע בפנקס מאגרי המידע במשרד המשפטים (להלן: "**פנקס**").

ד. הממונה על אבטחת מידע אחראי לאבטחת המידע במאגרים המוחזקים ברשות העירייה.

ממצאים:

3.14.1 נמצא **<u>כי לא קיים באגף מסמך מדיניות הגנת הפרטיות</u>**, הדן, בין היתר, ביעדי ההגנה על הפרטיות, סמכויות, אחריות וניהול הגנת הפרטיות וסיווג מאגרי המידע וכן, מסמך מדיניות אבטחת המידע בעירייה אינו דן בנושא של מיפוי מאגרי מידע לאיתור מאגרים התואמים להגדרות בחוק הגנת הפרטיות.

<u>המלצה</u>

מומלץ כי נושא יעדי ההגנה על הפרטיות, סמכויות, אחריות, ניהול הגנת הפרטיות, סיווג מאגרי המידע ומיפוי מאגרי מידע יעוגנו במסגרת מסמך מדיניות האגף המתייחס לחוק הגנת הפרטיות.

<u>תגובת האגף</u>: *"קיים מיפוי של מאגרי המידע העירוניים אל מול רשם מאגרי המידע. בשנים 2014-2015 נעשו עדכונים רלוונטיים במאגרים הנל אל מול רשם מאגרי המידע. יתר המלצות הביקורת בעניין זה ייבדקו ויגובשו המלצות בהתאם."*

3.14.2 עבור כל מאגר מידע חדש, נשלחת בקשה חתומה על ידי היועץ המשפטי לעירייה לרמו"ט (הרשות למשפט, טכנולוגיה ומידע), הכוללת: בקשה לרישום מאגר מידע בפנקס מאגרי מידע בהתאם לסעיף 9 לחוק הגנת הפרטיות, אישור מנהל פעיל של גוף שבבעלותו/החזקתו מאגר מידע בהתאם לסעיף 7 לחוק הגנת הפרטיות, וכן הצהרת מנהל המאגר - **נמצא תקין**.

3.14.3 נמצא כי מאגרי המידע המתייחסים לנתונים הכספיים, לוגיסטיים ונתוני כוח אדם נמצאים בחברה לאוטומציה ובחברת מלם ואינם מוחזקים על ידי העירייה.

3.14.4 מהשוואה בין המערכות הממוחשבות הקיימות בעירייה למאגרים שנרשמו בפנקס משרד המשפטים נמצא כי המערכות המוגדרות כמאגר, אכן נרשמו בהתאם לחוק הגנת הפרטיות במאגר משרד המשפטים - **נמצא תקין**.


הפטרות

נספח א':

כרטסת	סעיף תקציבי	פקודה	תיאור[9]	סכום ב-₪
2014	2740022750	650804	תחזוקה 1.7.2014-1.7.2015	8,496
2013	2730022750	600696	תחזוקה עבור מילון וינקדן טקס	561
2013	2730022750	618279	נס אי טי- 7/13 שעות נוספות	8,911
2013	2730022751	603553	נס א.ט- 1/13	8,835
2013	2730022751	603555	נס א.ט- 1/13 י. ב.	11,934
2013	2730022751	603556	נס א.ט- 2/13 י. ב.	11,934
2013	2730022751	603559	נס א.ט- ר. ה. צ. 2/13	15,444
2013	2730022751	604048	סי.אר.אם-תחזוקה מוקד-13-2/14	11,877
2013	2740012753	608260	וויספין- מ. טלפון	53,100
2013	2740012753	613874	איתוראן-ד. מנוי	2,889

[9] פרטי התיאורים המלאים נמצאים בניירות העבודה של הביקורת

נספח ב' - תיאור תפקידי עובדי המחלקה

	שם העובד/ת[10]	תפקיד	תאריך תחילת עבודה	אחוז משרה
1	נ. ב. ל.	מנהל אגף מחשוב ומערכות מידע	1.4.2014	100%
2	א. ק.	ס. מנהל אגף מחשוב ומערכות מידע	21.12.1998	100%
3	א. ה.	מנהלת מערכות מידע ורכזת נושא CRM/	1.2.2004	100%
4	מ. ה.	מזכירת אגף מחשוב ומערכות מידע	1.3.1995	100%
5	א. ר.	מנהל רשת ומנהל מרכז תמיכה ואבטחת מידע	1.12.2000	100%
6	א. פ.	טכנאי מרכז תמיכה/ עובד תמיכה	1.9.2008	100%
7	א. ט.	טכנאי מרכז תמיכה	2008	100%
8	ב. י.	טכנאי מרכז תמיכה	12.10.2008	100%
9	ה. י.	מנהלת מסמכים, אתר העירייה והארכיון	2006	100%
10	צ. ב.	טכנאי בית ספר	1.11.2002	100%
11	ר. ה.	מטמיע מערכות מידע	2009	100%
12	א. פר.	טכנאי מרכז תמיכה	2011	100%
13	א. ע.	מתאמת מיכון באגף הכספים		100%
14	ר. ה. צ.	הטמעת מערכת מידע		100%
15	א. ב. י.	טכנאי בית ספר		100%
16	א. מ.	מנהל תחום טלפוניה	2008	100%
17	ר. ח.	טכנאי בית הספר		50%

[10] שמות העובדים נמצאים בניירות העבודה של הביקורת