מעודכן ליום 22.07.19	**נוהל טיפול במאגרי מידע המחויבים ברישום בעירייה**	

מש-21 081 נוהל מאגרי מידע

1. כללי

1.1 חוק הגנת הפרטיות, התשמ"א-1981 (להלן: "**החוק**" או "**חוק הגנת הפרטיות**") קובע הוראות שונות וחובות המוטלים על בעל מאגר מידע, מחזיק במאגר מידע ומנהל מאגר מידע. אחת החובות המרכזיות היא חובת אבטחת המידע, הקבועה בסעיף 17 לחוק, אשר מטרתה צמצום החשש מפני שימוש לרעה או פגיעה בשלמות המידע.

1.2 תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "**תקנות אבטחת מידע**") קובעות עקרונות אבטחת מידע הקשורים בניהול ובשימוש מידע במאגרי המידע, בהתבסס על תקני אבטחת מידע מקובלים בעולם.

1.3 אבטחת מידע ברשת ובמערכות עיריית רמת השרון (להלן: "**העירייה**") הינה חיונית להגנת המידע של העירייה, תושביה ועובדיה.

1.4 לאור זאת, על העירייה להתקין ולהטמיע מערכות הגנה מפני איומים וחיצוניים ופנימיים וליישם בקרות נוהליות וטכנולוגיות לאכיפת רמת אבטחת מידע ואבטחה פיזית על תשתיות המידע.

2. מטרת הנוהל

2.1. הגדרת כללי אבטחת המידע המחייבים את העירייה, עובדיה וספקיה.

2.2. התאמת פעילות העירייה להוראות החוק, לתקנות שהותקנו מכוחו ובפרט לתקנות אבטחת המידע, ולהנחיות הרשות להגנת הפרטיות, כפי שיעודכנו מעת לעת.

2.3. מימוש תכליות החוק והגנה על זכויות נושאי המידע במאגרי המידע מפני שימוש לרעה במידע אודותיהם, הן ע"י גורמים מחוץ לעירייה והן ע"י העובדים.

2.4. הגדרת פעולות ובקרות הנדרשות לעמידה בדרישות החוק ותקנות אבטחת המידע.

3. הגדרות

3.1. אנטי-וירוס- תוכנה המגינה על מחשבים מפני תוכנות זדוניות, פריטי דוא"ל ואתרי אינטרנט המכילים תוכנות אלו.

3.2. FIREWALL– אמצעי להסדרה ואבטחה של התקשורת בין העירייה וגורמים חיצוניים.

3.3. ספק מיקור החוץ – שם הספק

3.4. משתמש – אדם הפועל ברשת המחשוב של העירייה

3.5. בעל הרשאה – כהגדרתו בתקנה 1 לתקנות אבטחת מידע.

3.6. עדכון במערכת ההפעלה- חברת Microsoft מפרסמת מדי פעם עדכונים למערכת ההפעלה החדשה ביותר שלה. עדכונים אלה קרויים גם Service Packs או מהדורות מעודכנות המכילות שיפורים חשובים במערכות ההפעלה כמו למשל, תוכנות אבטחה מעודכנות, כלים עדכניים ושינויים במוצר על פי בקשת הלקוחות.

3.7. מאגר מידע - אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט אוסף לשימוש אישי שאינו למטרות עסק או 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.

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

3.9. מידע רגיש - נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו.

3.10. מנהל מאגר מידע- מנהל פעיל של גוף, שבבעלותו או בהחזקתו מאגר מידע, או מי שהעירייה הסמיכה לעניין זה. מנכ"ל העירייה יסמיך מנהל מאגר לכל אחד ממאגרי המידע. האחריות על מאגרי מידע שלא הוגדר להם מנהל, היא של המנכ"ל.

3.11. מחזיק מאגר מידע- ספק שמנהל/מחזיק מערכת למאגר מידע דרך קבע והוא רשאי לעשות בו שימוש.

3.12. ממונה אבטחת מידע – בעירייה הוחלט כי מנמ"ר העירייה (ובהעדרו מנכ"לית העירייה) מוגדר כממונה אבטחת המידע על המאגרים.

3.13. אירוע אבטחת מידע- כל אירוע או תקרית אשר עלולים לגרום לפגיעה באמינות, בסודיות, בשלמות ו/או בזמינות המידע ברשת המחשוב של העירייה, ו/או לפגוע, לשבש או לקטוע תהליכי עבודה תקינים בעירייה, כגון:

3.13.1. חשיפה מורשית או בלתי מורשית, מכוונת או בלתי מכוונת, של מידע רגיש ממערכות המידע של העירייה או אצל ספק המערכות.

3.13.2. התקפות מניעת שירות על מערכות העירייה (Denial Of Service).

3.13.3. פריצה למערכות המידע בעירייה (ע"י תוקף חיצוני או פנימי).

3.13.4. פגיעת וירוס בתשתיות המחשוב של העירייה.

3.13.5. שינוי פני אתרים ואפליקציות (Defacement).

3.13.6. מעילה, שימוש לא מורשה בהרשאות במערכת מידע.

3.13.7. השחתה או גניבת ציוד מחשבים במשרדי העירייה.

3.13.8. שימוש במערכות מידע לפעילות לא חוקית (גניבת תוצרת גמורה, מלאי בתהליך, וכו').

3.14. אירוע אבטחה חמור - אירוע שנעשה בו שימוש בחלק מהותי מן המאגר, בלא הרשאה או בחריגה מהרשאה או שנעשתה פגיעה בשלמות המידע לגבי חלק מהותי מן המאגר (עבור מאגר מידע שחלה עליו רמת האבטחה הבינונית – כהגדרת מונח זה בתקנות האבטחה)

או

אירוע אשר נעשה בו שימוש במידע מן המאגר, בלא הרשאה או בחריגה מהרשאה או שנעשתה פגיעה בשלמות המידע (עבור מאגר מידע שחלה עליו רמת האבטחה הגבוהה – כהגדרת מונח זה בתקנות האבטחה).

4. חלות הנוהל ואחריות

4.1. האחריות ליישום הנוהל והבאתו לידיעת כלל המשתמשים בעירייה חלה על מנהל יחידת המחשוב.

4.2. בקרת יישום הנוהל ועדכונו חלה על מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך.

5. שיטה

5.1. **<u>אזורים מאובטחים</u>**

5.1.1. מנהל יחידת המחשוב יגדיר אזורים אשר יוגדרו כ"אזורים רגישים מבחינה טכנולוגית".

5.1.2. מערכות המאגרים של העירייה יישמרו במקום מוגן, המונע חדירה וכניסה אליו בלא הרשאה, והתואם את אופי פעילות המאגר ורגישות המידע המצוי בו וכמפורט בנוהל זה.

5.1.3. העירייה תגדיר מיהם בעלי תפקידים המורשים להיכנס לשם ותנהל רשימת מורשי גישה, אשר כל שינוי בה יחייב את אישורו של מנהל המאגר. אחת לשנה יש לאשרר מול מנכ"ל העירייה את הרשימה כאמור.

5.1.4. מנהל יחידת המחשוב בשיתוף עם מנהל אגף בטחון ופיקוח יישמו אמצעי אבטחה פיזיים על מתחמים אלו.

5.1.5. מנהל אגף ביטחון ופיקוח יישם אמצעי מיגון פיזיים להגנה על ארונות התקשורת תוך הקפדה על הצבתם באזורים מאובטחים בבניין.

5.1.6. חדרי שרתים וארונות תקשורת יינעלו ע"י מורשה הגישה לאזורים אלה, כך שיהיו מחוץ להישג ידם של גורמים שאינם מורשים. כמו כן לא תתאפשר גישת מבקרים לאזורים אלה, למעט לצורך תפעול טכני בליווי גורם רלוונטי בעירייה ובאישור מנהל המאגר. מבקר שנכנס למבני העירייה עם אמצעי מחשוב נייד, יחתום על טופס מבקר עם לפטופ. הטופס כאמור יישמר לצורך תיעוד ובקרה.

5.1.7. אין לאפשר חיבור מחשבים ניידים של מבקרים למחשבי העירייה, אלא במקרים חריגים ובאישור מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך.

5.1.8. אין לאפשר חיבור אמצעי זיכרון ניידים (התקנים ניידים) של מבקרים למחשבי העירייה, אלא במקרים חריגים ובאישור מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך. ככל שנעשה שימוש בהתקנים ניידים כאמור במתקני העירייה, יחולו ההוראות הבאות:

* אין לחבר לרשת העירייה ו/או לשמור מידע בהתקנים ניידים אשר לא הוקצו לעובד מטעם העירייה ונסרקו לאיתור תוכנות זדוניות וכיו"ב.
* אין לבצע כל שימוש בהתקנים הניידים של העירייה באופן החורג ממסגרת התפקיד, הסמכות וההרשאות אשר ניתנו למשתמש.
* התקנים ניידים יסומנו כשייכים לעירייה, לרבות פרטי התקשרות במקרה של אובדן או גניבה.
* על העירייה להגביל או למנוע, ככל הניתן, את אפשרות החיבור של התקנים ניידים למערכותיה במתכונת ההולמת את רמת אבטחת המידע שחלה על המאגר, רגישות המידע, סיכונים מיוחדים למערכות המאגר ו/או למידע הנובעים מחיבור ההתקן הנייד ואת קיומם של אמצעי הגנה מתאימים מפני סיכונים אלה.
* ככל שהשימוש בהתקן הנייד מאפשר למשתמש גישה למאגר המידע ו/או להעתקת תוכנו, אזי שעל העירייה לנקוט באמצעי ההגנה הסבירים הנדרשים, בשים לב לסיכונים המיוחדים הקשורים לכך.

* במקרה בו משתמש ו/או כל עובד של העירייה נתקל באירוע חריג, אשר העלה אצלו חשש לפגיעה בשלמות המידע במאגר או זליגתו אל מחוץ למערכות המאגר בלא הרשאה, עליו לדווח על כך מידית ל מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך בעירייה, והאחרון יפעל בהקדם לתחקור הסוגיה ומציאת פתרון, בנוסף לדיווח שיעביר למנכ"ל העירייה.

5.1.9. אין לאפשר למבקרים גישה למערכות המידע של העירייה, למעט קבלני תמיכה אשר אושרו מראש על-ידי מנהל המאגר ו/או מנהל התחום ובפיקוח של מלווה בעל ידע מקצועי מתאים לצורך בקרה אודות הפעולות המבוצעות.

5.1.10. מבקרים קבועים

5.1.11. אישור מבקרים קבועים יתבצע על-ידי הגורם מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך בעירייה בלבד.

5.1.12. מבקר קבוע יחתום על הצהרת סודיות, באחריות מנהל התחום הרלוונטי.

5.1.13. מבקר קבוע לא יחויב בליווי בעת שהותו במתחמי העירייה.

5.1.14. גישת מבקרים קבועים למערכות המידע תתאפשר על פי צורך מקצועי ובאישור מנהל המאגר ו/או מנהל התחום בלבד.

5.1.15. עם סיום תפקידו של המבקר הקבוע, באחריותו של מנהל התחום לעדכן מידית את מנהל יחידת המחשוב ו/או מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך בעירייה שיש לבטל את הרשאת השהייה שניתנה למבקר הקבוע במתחמי העירייה.

5.1.16. מנהל יחידת המחשוב ינקוט אמצעים לבקרה ולתיעוד של הכניסה והיציאה מאתרים בהן מצויות מערכות המאגר, וכן יקיים תיעוד של הכנסה והוצאת ציוד אל מערכות מאגרי המידע ומהן. מנהל יחידת המחשוב ישמור נתונים אלה באופן מאובטח למשך 24 חודשים, לכל הפחות.

5.1.17. גריסת מסמכים מתבצעת אחת לשבוע באמצעות ספק חיצוני.

5.1.18. הספקים אחראים להגנה על המערכות המצויות ברשותם, לבקרה ולתיעוד של הכניסה והיציאה מאתרים בהן מצויות מערכות המאגר, וכן לתיעוד של הכנסה והוצאת ציוד אל מערכות מאגרי המידע ומהן.

5.2. <u>אבטחת סביבת העבודה והמחשבים</u>

5.2.1. בעת עזיבת סביבת העבודה, עובדי העירייה יעבדו בשיטת מדיניות "שולחן נקי" **Clear Desk Policy**) כמפורט להלן:

5.2.2. מידע רגיש יאוחסן באופן מאובטח, במתקן נעול (מגירה, ארון או כספת, בהתאם למידת הרגישות והאמצעים הזמינים). במידה ואין, יש לנעול את החדר.

5.2.3. בתום יום העבודה או בעת עזיבת מקום העבודה לזמן ארוך על המשתמש להותיר את סביבת העבודה כשמסמכי העירייה מתויקים או מסודרים במקומם הראוי ואינם חשופים לעיני כל. מובהר, כי מידע כאמור ישמר לפרק זמן מינימאלי נדרש, וזאת בהתאם להוראות ודרישות העירייה והוראות כל דין המגבילות את משך שמירת המידע כאמור.

5.2.4. מנהל יחידת המחשוב יישם נעילת מסך עם סיסמה לאחר 30 דקות ללא פעילות, בכל תחנות הקצה.

5.2.5. מנהל יחידת המחשוב יתקין בכל שרת ותחנת עבודה תוכנת אנטי-וירוס ויגדיר תהליך יומי לעדכונו.

5.2.6. מנהל יחידת המחשוב יגדיר בכל שרת ותחנת עבודה תהליך לעדכון מערכת ההפעלה בעדכוני אבטחת מידע והתקנת חבילת שירות של היצרן.

5.2.7. שימוש ברכיבי DOK או בכונן CD ייעשה באישור מנכ"ל בלבד.

5.2.8. מנהל יחידת המחשוב יגדיר ניתוק אוטומטי של משתמשים לאחר השעה 00:20

5.2.9. כל שינוי בתצורת המחשב האישי, ובכלל זה התקנת תוכנה, או חומרה, כמו כן שינוי להגדרות האבטחה של המחשב – הרשאות גישה, הגדרות תקשורת, הגדרות תוכנת האנטי וירוס, יתבצע ע"י מנהל יחידת המחשוב או מי שהוגדר מטעמו, או ע"י ספק מורשים באישורו ותוך תיעוד הפעילות.

5.2.10. התקשרות עם הספקים מתבצעת בתווך מוצפן.

5.2.11. הספקים אחראים לאבטחת סביבת העבודה והמחשבים שברשותם. מנהל יחידת מחשוב ו/או מנהל אגף ביטחון יוודאו קיום הוראה זו.

5.3. <u>ניהול הרשאות</u>

5.3.1. ניהול ההרשאות במחשבי העירייה ייעשה ע"י מנהל יחידת המחשוב באמצעות מנגנון ממוכן לניהול הרשאות (AD) (להלן: "**מנגנון הבקרה**").

5.3.2. מטרת מנגנון הבקרה הינה לספק מידע אמין ומלא בעת בדיקה או תחקור, על מנת ליצור תמונת מצב מפורטת אחר האירועים השונים שהתרחשו.

5.3.3. יש לתעד את כל הפעולות השונות המבוצעות על רכיבי הרשת הרגישים בסביבת מאגרי המידע והמידע האישי המצוי בהם, החל מכניסה וכלה בגישה לקובצי מערכת רגישים אלו.

5.3.4. יש ליידע את העובדים כי פעילותם מתועדת. מקום בו ניתנת גישה לגורם חיצוני למערכות העירייה מסיבה כלשהי, יש לעדכן אף אותו כי פעולותיו מתועדות.

5.3.5. אין לשמור במנגנון הבקרה מידע רגיש בצורה גלויה.

5.3.6. יש לוודא כי כל מנגנוני הבקרה פעילים עם עליית מערכות העירייה.

5.3.7. מנגנון הבקרה מנוהל על ידי מנהל יחידת המחשוב ומאפשר ביקורת על הגישה למערכות המאגר ובכלל זה נתונים אלה: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה.

5.3.8. ספקים אשר מחזיקים/מנהלים מאגרי מידע ומערכות מאגרי מידע, אחראים לקיום מנגנון בקרה במאגרים ובמערכות שברשותם.

5.3.9. מנהל יחידת המחשוב יגדיר כי רק לאנשי המחשוב אשר להם צורך בכך לשם ביצוע תפקידם תהיה גישה לניהול ההרשאות ולקבציי הלוגים של מנגנון הבקרה. כמו כן, מנגנון הבקרה <u>לא יאפשר, ככל יכולתו, ביטול או שינוי של הפעלתו</u> ויאתר שינויים או ביטולים בהפעלתו ויפיץ התראות למנכ"ל העירייה, למנהלי המאגרים, למנהל יחידת המחשוב, לממונה אבטחת המידע וסייבר.

5.3.10. מנהל יחידת המחשוב יקבע נוהל בדיקה שגרתי לנתוני התיעוד של מנגנון הבקרה ויערוך דו"ח של הבעיות שהתגלו והצעדים שננקטו.

5.3.11. מנהל יחידת המחשוב ישמור את נתוני התיעוד של מנגנון הבקרה באופן מאובטח למשך 24 חודשים, לכל הפחות.

5.3.12. מנהל יחידת המחשוב ו/או מנהל כל מאגר יידע את בעלי ההרשאות במאגר בדבר קיום מנגנון הבקרה למערכות המאגר.

5.3.13. מנהל יחידת המחשוב יוודא כי חשבון משתמש בגישה למחשבי העירייה ולמערכות העירייה ישויך לעובד מסוים ותוגדר אחריות של העובד על החשבון והפעולות המתבצעות בו.

5.3.14. מנהל יחידת המחשוב יגדיר הרשאות בגישה למחשבי העירייה ולקבצים ולמערכות ברשת העירייה בהתאם לתפקידם ולצורך ביצוע תפקידם בלבד. הוראה זו תחול על מנהל יחידת המחשוב גם ביחס לגישה המוענקת לספקים חיצוניים לעירייה.

5.3.15. במערכות המתופעלות על ידי ספקים, הספק ינהל ההרשאות בנפרד מלקוחות אחרים של אותו הספק.

5.3.16. ממונה אבטחת מידע ייבחן את הרשאות הניהול במערכות, אחת לשישה חודשים ואחת לשנה את שאר ההרשאות לכלל המערכות. **רשימת הרשאות תקפות מהווה נספח א' לנוהל זה – אינה מצורפת מפאת נימוקי אבטחת מידע (מסווג).**

5.3.17. בכל מקרה בו ידוע על הפסקת עבודה של משתמש המוגדר במערכת לתקופה העולה על 30 יום (עקב מילואים, חופשה, מחלה), מנהל יחידת המחשוב ינעל את חשבון המשתמש של אותו עובד אל מחשבי העירייה. במקרה של חופשת לידה החשבון יישאר זמין. בנוסף, מנהל יחידת המחשוב יעדכן את הספקים הרלוונטיים לנעול חשבונות למערכת.

5.3.18. מנהל יחידת המחשוב יוודא הקפאת הרשאות של משתמש עד ליום שובו לעבודה, בתיאום עם מחלקת משאבי אנוש.

5.4. <u>סגירת/ביטול הרשאות משתמש</u>

5.4.1. כאשר סיים עובד בעל הרשאה את עבודתו בעירייה, מנהל יחידת המחשוב יסגור את הרשאתו למחשבי העירייה לצמיתות, בתיאום עם מחלקת משאבי אנוש. בנוסף, מנהל יחידת המחשוב יוודא כי ספקי התוכנה או השירותים הרלוונטיים יסגרו את הרשאות העובד במערכות בהן יש לו חשבון משתמש.

5.4.2. לצורך שמירה על רצף שירותי מידע, מנהל יחידת המחשוב ייבחן את הצורך לשמור או להעביר ספריות מהרשאה המיועדת לסגירה אל הרשאותיו של משתמש אחר.

5.4.3. עובד המשנה את סטאטוס התפקיד שלו בעירייה – יש לשנות בהתאם גם את סיסמאותיו והרשאותיו.

5.5. <u>שימוש בשם משתמש וסיסמאות</u>

5.5.1. הסיסמה הינה המפתח לגישה למערכות המידע. על הסיסמה להישמר פרטית וסודית.

5.5.2. שם המשתמש (User ID/Username) מיועד לשימוש אישי בלבד וחל איסור על שימוש בסיסמה זהה עבור קבוצת משתמשים.

5.5.3. לא תתבצע הגדרת משתמשים גנריים לפעילות משתמשים אנושיים, אלא עבור שרתים ויישומים בלבד, תוך תיעוד בקבץ ייעודי.

5.5.4. אין לחשוף את הסיסמה האישית לאדם אחר, וחל איסור על משתמש לנסות לגלות את סיסמתו של משתמש אחר. בכל מקרה בו יש חשש לחשיפת הסיסמה, יש לדווח לממונה על אבטחת המידע, ולפעול להחלפת הסיסמה באופן מיידי.

5.5.5. אין לשמור את הסיסמה כתובה במקום בו היא עלולה להיחשף (למשל, מדבקה בסביבת המחשב, מתחת למקלדת, או בקובץ לא מוצפן על גבי המחשב).

5.5.6. סיסמה ראשונית למערכות המידע תינתן על-ידי הגורם המוסמך לכך בעירייה. הסיסמה תועבר אישית לעובד או באמצעות הטלפון יחד עם הסבר לגבי החלפת הסיסמה בכניסה הראשונית למערכת. מובהר כי הסיסמה הראשונית תהא ייחודית ושונה עבור כל משתמש.

5.5.7. מדיניות הסיסמאות ברשת (AD) , תחנות הקצה והשרתים תוגדר כדלהלן:

5.5.7.1. על הסיסמא להיות שונה מ"זיהוי המשתמש".

5.5.7.2. אורך הסיסמא יהיה 7 תווים לפחות.

5.5.7.3. סיסמא תכיל לפחות אות אחת, וסיפרה אחת.

5.5.7.4. אין לבחור סיסמאות כגון: סיסמא קלה לניחוש בדומה לשם המשתמש, תו אחד אשר חוזר על עצמו מספר פעמים וכיו"ב.

5.5.7.5. הסיסמה תוחלף אחת ל-90 יום. לא ניתן לחזור על אותה סיסמה.

5.5.7.6. סיסמאות לא תוצגנה על המסך בעת הקשתן.

5.5.7.7. תוגדר נעילת משתמש לאחר 7 ניסיונות זיהוי כושלים ושחרור ע"י מנהל יחידת המחשוב בלבד.

5.6. **<u>אבטחת מידע בניהול כוח אדם</u>**

5.6.1. כלל עובדי העירייה מחויבים לשמור על אבטחת המידע בהתאם להוראות נוהל זה והוראות כל דין.

5.6.2. הגשת מועמדות לעבודה בעירייה, קבלת עובד לעבודה בה, ועבודתו בפועל יתבצעו בהתאם לנוהל זה בכל הקשור לאבטחת המידע.

5.6.3. מנהל המאגר לא ייתן גישה למידע המצוי במאגר ולא ישנה היקף הרשאה שניתנה, אלא אם נקט אמצעים סבירים, המקובלים בהליכי מיון עובדים ושיבוצם, כדי לברר שאין חשש כי בעל ההרשאה אינו מתאים לקבלת גישה למידע המצוי במאגר. אמצעים כאמור יינקטו בשים לב לרגישות המידע שבמאגר ולהיקף הרשאות הגישה לתפקיד שמיועד לו הנוגע בדבר.

5.6.4. באשר לבעלי הרשאות הקיימים עוד בטרם נכנס לתוקפו נוהל זה, מנהל המאגר יבחן את מידת התאמתם לגישה למאגר המידע באמצעים סבירים המקובלים בהליכי מיון עובדים ושיבוצם, וכל זאת בשים לב לרגישות המידע לסוג הרשאת הגישה ויעדכן בהתאם לצורך את הרשאות הגישה.

5.6.5. מנהל המאגר ידאג לקיום הדרכות לבעלי הרשאות, בטרם יקבלו גישה למידע שבמאגר או לפני שינוי היקף הרשאותיהם, בנושא החובות לפי חוק הגנת הפרטיות ותקנות אבטחת המידע וימסור להם מידע אודות חובותיהם לפי חוק הגנת הפרטיות ונוהל זה.

5.6.6. במאגרים בעלי רמת אבטחה בינונית-גבוהה, מנהל מאגר ידאג לקיים, אחת לשנה, פעילות הדרכה תקופתית לבעלי ההרשאות, בדבר מסמך הגדרות המאגר, נוהל זה והוראות אבטחת מידע, בהתאם לחוק הגנת הפרטיות ולתקנות אבטחת המידע, בהיקף הנדרש לצורך ביצוע תפקידיהם ובדבר חובות בעלי ההרשאות לפיהם. הדרכה לבעל הרשאה לתפקיד חדש תיערך סמוך ככל האפשר למועד תחילת הסמכתו. מובהר כי מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך יוודא את קיום ההדרכות כאמור.

5.6.7. ספקים אשר מחזיקים/מנהלים מאגרי מידע ומערכות מאגרי מידע, אחראים למתן הרשאות גישה וקיום הדרכות לעובדיהם.

5.6.8. עם קבלת מועמד לעבודה, וטרם תחילת עבודתו, מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך יבחן את הרשאות הגישה שיש לאפשר לו בהתאם לנוהל זה. לאחר שקיבל את ההרשאות המתאימות לתפקידו, יקבל העובד החדש את פרטי ההזדהות למערכות העירייה הרלוונטיות לביצוע תפקידו, בהתאם להוראות נוהל זה.

5.6.9. טרם תחילת עבודתו של העובד החדש ומתן הסיסמאות והגישה למערכות המידע הרלוונטיות, תקיים העירייה הדרכה לעובד החדש, בה יובהרו הנהלים הקשורים בסיסמאות, הרשאות גישה, יידוע העובד אודות מנגנון הבקרה האוטומטי שלך העירייה, עמדות עבודה ויתר החובות הנדרשות בהתאם להוראות נוהל זה ותקנות האבטחה. הדרכה כאמור יכול שתועבר באופן פרונטלי או באמצעות לומדה וכיו"ב.

5.6.10. לעובדים חדשים הנדרשים לכך במסגרת תפקידם תוגדר תיבת דואר אלקטרוני ייעודית (להלן "**תיבת המייל**"). תיבת המייל היא אישית עבור כל עובד אך מוגדרת כמקצועית – כך שהן התיבה והן תוכנה שייכים באופן בלעדי לעירייה. לפיכך, עובדים (חדשים וקיימים כאחד) יחויבו להשתמש בתיבת המייל לצרכי עבודתם בעירייה בלבד. תיבת המייל ותוכנה יועברו על פי הצורך מעובד לעובד, בהתאם להרשאות הגישה ולהוראת הגורם מנהל יחידת המחשוב ו/או מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך בעירייה.

5.7. **<u>שמירת מידע</u>**

5.7.1. שמירת מידע במדיית אחסון נתיקה יתבצע ע"י מורשים לכך ע"י מנכ"ל העירייה, כאשר המידע יימחק עם הסיום בשימוש בו.

5.7.2. תיקיות "המסמכים שלי" של המשתמשים ימופו לכונן רשת, וכן שולחן העבודה, במידת האפשר.

5.7.3. על המשתמשים להימנע מאחסון מידע על גבי הכוננים הקשיחים המקומיים (C:,D:). מידע השמור מקומית על גבי מחשבים אישיים אינו מגובה, ומאובטח פחות מאשר כונני הרשת.

5.7.4. העירייה אינה ממליצה לעובדיה לשמור מידע אישי במחשביה, אם כי ניתן לעשות כן על כונן :D שאינו מגובה. להסרת ספק מובהר, כי העירייה אינה אחראית על אבטחת מידע זה ואינה אחראית לכל נזק מכל סוג שהוא אשר ייגרם למידע ו/או לבעל המידע ו/או לכל גורם שהוא.

5.8. **<u>גיבויים</u>**

5.8.1. מנהל יחידת המחשוב או ממונה מטעמו יבצע גיבויים לכל השרתים ברשת העירייה ברמה יומית לספק חיצוני.

5.8.2. מנהל יחידת המחשוב יוודא מול הספקים את נתוני מדיניות הגיבוי שלהם למערכות המשמשות את העירייה.

5.8.3. מנהל יחידת המחשוב או מי מטעמו ישמור את הגיבויים למשך 24 חודשים, לכל הפחות.

5.8.4. מנהל יחידת המחשב או ממונה מטעמו ישמור סט שנתי לפי המפרט הבא: 4 קלטות יומיות, 4 קלטות שבועיות (גיבוי של יום ו'), קלטת חודשיות.

5.8.5. כל בוקר יתעד מנהל המחשוב את תוצאות תהליך הגיבוי בקבץ ייעודי וינהל רישום מעודכן של מועדי ביצוע הגיבוי כאמור, יעבירו למנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך שיפקח אחר ביצוע הרישום כאמור ויוודא את ביצוע הגיבוי למערכות המידע של העירייה.

5.8.6. קלטות הגיבוי יועברו אחת ליום לאתר חיצוני מאובטח (ניתן במבנה אחר של העירייה).

5.8.7. דרישות הגיבוי יכללו את הפרמטרים הבאים:

5.8.7.1. תדירות גיבוי מלא / משתנה;

5.8.7.2. גיבוי מקוון / לא מקוון;

5.8.7.3. תקופת השמירה של עותקי גיבוי בהתאם לחשיבות ורגישות המידע;

5.8.7.4. תיעדוף גיבויים בהתאם לסוג המידע;

5.8.8. אמצעי אחסון הגיבוי יכללו את הפרמטרים הבאים:

5.8.8.1. אחסון הגיבויים ייעשה במיקום נפרד מן המידע עצמו על מנת למנוע נזק למידע ולגיבוי באירוע אחד כגון שריפה או פיצוץ;

5.8.8.2. יש לשמור את הגיבויים באזור חסין לאש;

5.8.8.3. יש להגביל את הגישה לגיבויים. יש לבצע בקרה על רמת האבטחה של אתר אחסון הגיבויים פעם בשנה לכל הפחות;

5.8.8.4. יש לנהל ולתחזק רשימה של פרטים ביחס לאמצעי הגיבוי:

* שם האדם אשר ביצע את הגיבוי;

* תאריך הגיבוי וסוג המידע שנשמר;

* הסיבה לביצוע גיבוי (ככל שרלוונטי - למשל גיבוי אשר נעשה לפני עדכון גרסאות);

5.8.9. שחזור מידע רגיש יבוצע באישור מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך בלבד.

5.8.10. יש לתעד כל אירוע במסגרתו התבצע שחזור מידע רגיש. התיעוד יכלול את הסיבה לאיבוד המידע, האדם שביקש את המידע והאדם שאישר את ביצוע השחזור. מידע זה יהיה זמין למנמ"ר / מנכ"ל העירייה.

5.8.11. עם קרות אירוע אבטחת מידע בעירייה, יודיע מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך על הצורך בשחזור של כלל המידע המגובה, לפי הגיבוי המאוחר המצוי ברשות העירייה.

5.9. **<u>מיקור חוץ</u>**

5.9.1. העזרות בשירותי מיקור חוץ מהווה מרכיב משמעותי בפעילותם של ארגונים רבים במשק המודרני, במטרה לקדם יעילות, להוזיל עלויות ולהתמקד בליבת העיסוק של אותו ארגון. כך, גם העירייה נעזרת לעתים בגופים חיצוניים המספקים עבורה שירותים המבוססים על מידע המצוי במאגרי המידע שלה. שימוש בשירותי מיקור חוץ חושף את העירייה לסיכונים נוספים מעבר לאלה הגלומים בפעילות העסקית הרגילה המנוהלת באמצעות המערכות הטכנולוגיות בעירייה. פעילות בהתאם לנוהל זה תבטיח את זיהוי הסיכונים הטמונים בעבודה במיקור חוץ, תמנע או לכל הפחות לצמצם סיכונים אלו, ככל הניתן, תוך עמידה בהוראות כל דין ובפרט בהתאם לחוק, לתקנות האבטחה, והרגולציה החלה על העירייה. האחריות לקיום ההוראות בנוגע לפעילות במיקור חוץ חלה על מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך.

5.9.2. על מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך לבחון האם העירייה רשאית להוציא את המידע שהיא מבקשת לעבד במיקור חוץ אל מחוץ לשליטתה. האמור נובע מכך שעשויות להיות מגבלות חוקיות ו/או אתיות שיש בהן כדי למנוע את ההעברה לשירותי מיקור חוץ כאמור. יצוין, כי אף אם לא קיימת הגבלה פורמלית, מומלץ לקיים הליך בחינה ראוי ומתועד בהתאם לאופי המידע המועבר.

5.9.3. בטרם ההתקשרות עם גורם חיצוני כלשהו במיקור חוץ, על מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך לאפיין את השירות הנדרש, לרבות הגדרת האיומים והסיכונים הנובעים מסוג המידע המועבר לגורם החיצוני, ובהתאם לכך להחליט מהו היקף המידע שיש למסור לידיו. אפיון ראשוני זה, נועד למנוע העברת מידע אישי שאינו נדרש במישרין לצורך מתן השירות. בהקשר לאמור, ישנן שלוש רמות שירות (מהמחמירה אל הקלה):

5.9.3.1. שירות הכולל איסוף ועיבוד המידע על-ידי הגורם החיצוני, לרבות הקמת מאגר מידע עבור העירייה;

5.9.3.2. שירות המחייב העברה או העתקה של כל מאגר המידע, או חלק מהותי ממנו, מהעירייה אל הגורם החיצוני;

5.9.3.3. שירות אשר במסגרתו ניתנות לגורם החיצוני הרשאות גישה למאגר המידע של העירייה לצורך מתן השירות, ללא העברת מאגר המידע או חלק מהותי ממנו.

האפשרות האחרונה (ס"ק 5.9.3.3 לעיל), הינה כמובן העדיפה, וזאת מאחר שהעברת עותק שלם של מאגר המידע או מתן גישה בלתי מוגבלת למערכות מציבים סיכון ממשי של העברת מידע עודף, אשר אינו דרוש במישרין לצורך מילוי תפקידו החוזי של הגורם החיצוני המספק את שירותי מיקור החוץ. ככל שאכן נבחרה האופציה האחרונה כאמור, ניתן יהיה להקל בדרישות הקשורות בהסדרת נושא התפעול והפיקוח, מאחר שהדבר יוביל לצמצום ניכר של הסיכונים הנובעים מעיבוד מידע. ככל שנבחרה חלופה אחרת, אזי שעל מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך לנמק את הבחירה בחלופה זו ולתעד אותה.

5.9.4. בעת בחינת המועמדים הראויים לשמש כגורמים חיצוניים בפעילות מיקור חוץ עבור העירייה, על מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך לשים דגש על שלוש נקודות עיקריות ביחס לגורם החיצוני:

5.9.4.1. ניסיון קודם בעיבוד מידע מהסוג שעתיד להיות מועבר לאותו גורם חיצוני;

5.9.4.2. רקע ומוניטין של הגורם החיצוני;

5.9.4.3. קיום חשש לניגוד עניינים או לשימוש פסול במידע שעתיד להימסר לגורם החיצוני.

5.9.5. ככל שהמידע המועבר לגורם החיצוני לצורך שירותי מיקור החוץ הינו רגיש יותר, אזי שיש לנקוט במשנה זהירות בבחירת אותו גורם חיצוני.

5.9.6. קודם ולאחר העברת הפעילות למיקור חוץ לידי הגורם החיצוני, על מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך לוודא כי הגורם החיצוני מקיים את רמת אבטחת המידע הדרושה, שכן כל פעולה המבוצעת מטעם העירייה על-ידי הגורם החיצוני הינה באחריותה של העירייה גם כן.

5.9.7. לאור האמור לעיל, על מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך להסדיר במסגרת משפטית וארגונית את השימוש בשירותי מיקור חוץ, לרבות הגדרת תחומי האחריות בכל הנוגע לאבטחת המידע במאגרים וביצוע הוראות החוק והתקנות על-ידי הגורם החיצוני. ההסדרה האמורה תיעשה הן באמצעות הסכם מיקור חוץ, אשר יכול שיהווה נספח/תוספת להסכם המקורי בין העירייה לבין הגורם החיצוני, ויעמוד בהוראות כל דין על כל סעיפיו, והן על-ידי נוהל פנים ארגוני מסוג זה.

5.9.8. הסכם מיקור החוץ יכלול, בין היתר, הוראות אשר יתייחסו לדברים הבאים :

5.9.8.1. המידע אותו הגורם החיצוני רשאי לעבד ומטרות השימוש המותרות בו לצורכי ההתקשרות;

5.9.8.2. מערכות המאגר אליהן הגורם החיצוני רשאי לגשת, אם בכלל, ו/או המידע אשר יעבור לידי הגורם החיצוני;

5.9.8.3. סוגי העיבוד או הפעולות אותם הגורם החיצוני רשאי לעשות;

5.9.8.4. במקרה בו הגורם החיצוני אוסף מידע ישירות ממושא המידע, לוודא כי הוא מקיים את חובת הודעה למושא המידע כאמור בסעיף 11 לחוק הגנת הפרטיות;

5.9.8.5. קיום בטוחות, לרבות עריכת ביטוח אחריות מקצועית;

5.9.8.6. קיום זכות עיון ותיקון בהתאם לחוק עבור מושא המידע והוראות המפרטות את הדרך למימוש זכות זו, לרבות זמני תגובה, עלויות וכיו"ב;

5.9.8.7. משך ההתקשרות, אופן השבת המידע לידי העירייה בסיום ההתקשרות, השמדת המידע המצוי ברשותו של הגורם החיצוני ודיווח על כך לעירייה;

5.9.8.8. אופן יישום החובות בתחום אבטחת המידע שהעירייה חייבת בהן, וכן הנחיות נוספות לעניין אמצעי אבטחת מידע, כפי שתקבע העירייה ובהתאם להוראות חוק הגנת הפרטיות ותקנות האבטחה;

5.9.8.9. חובתו של הגורם החיצוני לקיים הדרכות ביחס למטרות השימוש במידע המועבר לכל מורשי הגישה מטעמו ולתעד אותן, ובנוסף להחתים את בעלי ההרשאות שלו על התחייבות לשמירת סודיות המידע, שימוש במידע אך ורק בהתאם להוראות ההסכם, ויישום אמצעי האבטחה כאמור בנוהל זה;

5.9.8.10. מומלץ למנות ממונה / אחראי אבטחת מידע אצל הגורם החיצוני שיהווה גורם אחראי / איש קשר לצורך מתן השירותים וקיום הפעילות בין הצדדים, ולאפשר פיקוח מצד העירייה, בהתאם לרגישות המידע המועבר במסגרת ההתקשרות;

5.9.8.11. איסור העברת המידע לצד שלישי כלשהו ו/או שימוש במידע אליו נחשף הגורם החיצוני אגב ההתקשרות, לכל מטרה שאינה קשורה במישרין לביצוע ההתקשרות;

5.9.8.12. איסור מפורש על איסוף מידע בדרכים בלתי-חוקיות ו/או עשיית שימוש במאגרי מידע בלתי-חוקיים;

5.9.8.13. נספח הגדרות אבטחה שיהיה חלק בלתי נפרד מתנאי ההתקשרות עם הגורם החיצוני ויכלול, בין היתר, הוראות לגבי אבטחה פיסית ולוגית, הפרדת מאגרי מידע, מתן הרשאות, עריכת רישום מעודכן של מורשי הגישה למידע, הוראות תפעול, סודיות, בקרה, דרך קבלת עובדים וכיו"ב;

5.9.8.14. היה והעירייה תחליט להתיר לגורם החיצוני לספק את השירות באמצעות גורם נוסף – חובתו של הגורם החיצוני לכלול בהסכם עם אותו גורם נוסף את כלל הנושאים המפורטים בסעיף זה לעיל ולהלן;

5.9.8.15. חובתו של הגורם החיצוני לדווח לעירייה, אחת לשנה לפחות, אודות אופן ביצוע חובותיו בהתאם להוראות נוהל זה והסכם מיקור החוץ עמו, ולהודיע לעירייה במקרה של אירוע אבטחה;

5.9.9. כחלק מפעילות מיקור החוץ של העירייה עם הגורם החיצוני, יכול שיעלה לעתים הצורך ברישומו כמחזיק במאגר המידע הרלוונטי של העירייה.

5.9.9.1. מחזיק, על פי סעיף 3 לחוק הגנת הפרטיות, הוא "מי שברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש", בעבור בעל המאגר, על פי הוראותיו ולצרכיו. הרישום הינו רלוונטי לשם הטלת חובה על המחזיק, אף מהיבט זה, לשמור על אבטחת המידע המצוי במאגר המידע, גם כאשר פרטי המאגר הרלוונטיים היוצאים אל מחוץ לכותלי העירייה בפעילות מיקור חוץ מצויים בידיים זרות לבעל המאגר.

5.9.9.2. במקרה בו ניתנת זכות שימוש במאגר או במידע המצוי בו לגורם חיצוני לבעל מאגר המידע כדרך קבע, אותו גורם חיצוני הופך למחזיק במאגר המידע על-פי דין, ולמעשה כאשר נבחנת חוקיות השימוש במידע, החוק אינו מבחין בין בעליו של מאגר המידע לבין המחזיק בו.

לפי-כך, בעת פעילות מיקור החוץ, החובות והאחריות המוטלים מכוח החוק על בעל מאגר המידע, ממשיכים לחול גם על הגורם החיצוני שמבצע את השירות במיקור החוץ.

5.9.9.3. ההבחנה בין סוג פעילות מיקור חוץ אחד למשנהו, מושתתת על היקף הרשאות הגישה הניתנות לגורם החיצוני, העושה שימוש במידע המצוי אצל בעלת המאגר. בהתאם לכך, על העירייה לתחום את מידת האחריות שתוטל על הגורם החיצוני על פי המודלים כדלקמן:

א. הזמנת שירות המחייב טיפול במידע אישי, החל משלב האיסוף ממושאי המידע בשם העירייה ועיבוד המידע על-ידי הגורם החיצוני, לרבות הקמת מאגר המידע (כגון שימוש בחברת השמה המאבחנת וממיינת מועמדים לעבודה);

ב. הזמנת שירות המחייב העברה או העתקה של מאגר מידע שלם, או חלק מהותי ממנו, מהעירייה לגורם החיצוני (כגון שירותי אחסון וגיבוי מידע);

ג. הזמנת שירות המחייב טיפול במידע אישי בדרך של מתן הרשאות גישה או עדכון למידע במאגר המידע של העירייה, בהיקף מוגדר וקבוע מראש לצורך מתן אותו שירות בלבד, ללא העברת מאגר המידע במלואו אל הגורם החיצוני (כגון הסתייעות בחברה המתמחה בחישוב והדפסת תלושי שכר לעובדים).

חלופות א' ו- ב' שלעיל עונות לרוב על ההגדרה של 'מחזיק' על פי החוק. בחלופות אלו תיבחן ההרשאה שניתנה למחזיק במידע, האם היא מוגבלת יותר או פחות. בחלופות אלו על החברה לבחון את אופן ומשך הזמן בו יש לגורם החיצוני גישה למידע או יכולת לשמור עליו, כדי שיהא ניתן לקבוע את מעמדו במאגר, בשאלת הגדרתו כמחזיק.

לעומתן, חלופה ג' מגבילה מראש את מידת הרשאות הגישה למאגר המידע של החברה, וזאת בהתאם למטרות מוגדרות. לכן, לא מן הנמנע כי הגורם החיצוני על-פי חלופה ג' אינו מהווה מחזיק, מאחר שהוא אינו מחזיק במאגר דרך קבע, אלא אך ורק בהתאם להרשאות גישה למידע ספציפי ומוגדר מראש, לצורך שירות מסוים ובכפוף לתנאי התקשרותו בהסכם מיקור החוץ עם החברה.

5.9.10. על מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך לבחון את פעילות מיקור החוץ ובאם יש לרשום את הגורם החיצוני כמחזיק במאגר ולהעביר מסקנותיו לראש העירייה על מנת שיאשר את ביצוע הרישום.

5.9.11. על מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך ליישם כלי בקרה באמצעותם ניתן יהא לוודא כי פעילות מיקור החוץ המבוצעת על-ידי הגורם החיצוני תתבצע בהתאם להוראות הדין. בשל האמור, בעת מתן שירותי מיקור החוץ על-ידי הגורם החיצוני, על מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך ליישם, בין היתר, את הבקרות הבאות, ככל שרלוונטיות לעניין וכמפורט להלן.

5.9.11.1. על מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך לוודא כי הגורם החיצוני מקיים את עקרונות אבטחת המידע הנאותים על מנת להגן על נכסי המידע של העירייה מפני דליפה, שינוי ו/או מחיקה. לצורך כך, יבצעו מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך ביקורות שוטפות וביקורות פתע על פעילות הגורם החיצוני, בהתאם למוגדר בהסכם מיקור החוץ.

5.9.11.2. כך למשל – ניתן לקבוע ביקורת פיזית במשרדי הגורם החיצוני, לשלוח שאלון אבטחת מידע עליו הגורם החיצוני ישיב ובהתאם לכך יתוקנו ליקויים, ככל שקיימים, וניתן גם להסתפק בקבלת דיווחים שוטפים ודו"ח שנתי מסכם.

5.9.11.3. הפרטים שיועברו לגורם החיצוני יוגדרו באופן ברור בהסכם מיקור החוץ. כמו כן, בטרם החתימה על הסכם מיקור חוץ, על מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך לבחון האם קיימות אי-אלו הגבלות רגולטוריות או אחרות, בקשר עם הוצאת סוג מידע או סוג פעילות אל גוף חיצוני.

5.9.11.4. מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך יבדוק, מעת לעת, את כל העברות המידע המתבצעות על-ידי הגורם החיצוני במסגרת פעילות מיקור החוץ, וזאת כדי לבחון, בין היתר, האם הועברו/דלפו פרטי מידע שלא לצורך ביצוע פעילות מיקור החוץ כאמור.

5.9.11.5. מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך יוודא קבלת דיווחים שוטפים מהגורם החיצוני, וכן קבלת דיווח מידי בכל מקרה של חשש לדליפת מידע מהמאגר ו/או שימוש חורג מההרשאות שניתנו.

5.9.11.6. על מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך לוודא כי הגורם החיצוני שומר על עקרונות מיקור החוץ, כפי שנקבע בהסכם ההתקשרות עמו לעניין זה.

5.9.11.7. על מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך לוודא כי הגורם החיצוני יערוך לעובדיו הרלוונטיים בהתאם להסכם מיקור החוץ (ו/או לגורמים נוספים – ככל שרלוונטי), הדרכה תקופתית (אחת ל-6 חודשים, לכל הפחות) בדבר הגדרות המאגרים, נהלי האבטחה והחובות המוטלות עליו. באחריות מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך לדאוג כי הגורם החיצוני יעביר לעירייה דו"ח אודות ביצוע ההדרכה התקופתית כאמור.

5.9.11.8. מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך ימסור למנכ"ל העירייה, אחת לשנה, דו"ח אשר יסקור את כלל פעילות מיקור החוץ של העירייה בהתאם להוראות נוהל זה.

5.9.12. על מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך לוודא כי במסגרת פעילות מיקור החוץ, הגורם החיצוני יקבע כללי הפרדה ברורה וממודרת של המערכות, באופן בו תהא אבחנה והפרדה ברורה בין הפעילות המבוצעת עבור העירייה לבין פעילות המבוצעת עבור גופים אחרים ו/או עבור הגורם החיצוני עצמו.

5.10. **<u>שימוש באינטרנט ודואר אלקטרוני</u>**

5.10.1. משתמשים יונחו שלא לפתוח קבצים המקושרים להודעות דואל או קישורים מתוך הודעות, במידה ומתרחש אחד מן הבאים:

5.10.1.1. השולח אינו מוכר

5.10.1.2. רשימת התפוצה לא רלוונטית לפעילות

5.10.1.3. שם הקובץ אקראי ולא קשור לפעילות

5.10.1.4. תוכן ההודעה חשוד ומזמין לפתוח הקובץ או הקישור

5.10.1.5. הקישור מוביל לכתובת בחו"ל

5.10.2. לא ניתן יהיה לשלוח קבץ מעל 3MB.

5.11. **<u>חוקי FIREWALL</u>**

5.11.1. כל בקשה להוספה, שינוי או ביטול של חוק Firewall תגובה בבקשה כתובה ע"י מנהל מחלקה, תוך ציון הצורך לבקשה. אישור הבקשה יתבצע ע"י מנהל יחידת המחשוב ויועבר לביצוע של ספק מיקור החוץ.

5.11.2. חוקי ה-Firewall יגובו אחת לחודש.

5.11.3. חוקי ה- Firewall יתועדו במסמך ויסקרו אחת לרבעון.

5.12. **<u>הגדרת סיכונים</u>**

5.12.1. בסעיף זה מוגדרים הסיכונים להם חשוף המידע שבמאגר במסגרת הפעילות השוטפת של העירייה, לרבות אלה הנובעים ממבנה מערכות המאגר. **מבנה מאגרי המידע ורשימה מעודכנת של מערכות המאגר מהווה נספח ב' לנוהל זה. אינם מצורפים מפאת נימוקי אבטחת מידע (מסווג).**

5.12.2. <u>סיכונים טכנולוגיים</u>:

5.12.2.1. פגיעה בזמינות מאגרי המידע ובמערכות המשמשות למאגרי המידע כתוצאה מפגיעה מלאה או חלקית בהן.

5.12.2.2. פגיעה בשרידות מאגרי המידע והמערכות המשמשות למאגרי המידע בשל כשל טכני או נזק.

5.12.2.3. חדירה למאגרי המידע וחשיפת מידע.

5.12.2.4. פגיעה בפרטיות של נושאי המידע שפרטיהם מצויים במאגרי המידע של העירייה כתוצאה מדלף מידע לגורמים לא מורשים וכן מאי עמידה בחוק הגנת הפרטיות והתקנות הנלוות אליו.

5.12.2.5. אובדן מידע בשל העדר גיבוי.

5.12.2.6. עקיפת הרשאות בשל היעדר בקרות ברמה טכנולוגית.

5.12.2.7. ספקים חיצוניים בעלי יכולת גישה מרחוק למאגרי המידע של העירייה.

5.12.3. <u>סיכונים ארגוניים ואנושיים</u>

5.12.3.1. פעילות שגויה של משתמשים בשל חוסר מודעות לאבטחת מידע.

5.12.3.2. גישת גורמים לא מורשים ופגיעה במאגרי המידע ובמערכות הנלוות להם.

5.12.3.3. חוסר התאמה בין מצבת כוח האדם בפועל למצבת כוח האדם במאגרי המידע ובמערכות בעירייה.

5.12.3.4. העברת קבצים ומסמכים באופן לא מאובטח ו/או לגורמים לא מוסמכים.

5.12.3.5. נזקים פיזיים למאגרי המידע ולציוד חומרה ותקשורת בעירייה.

5.12.3.6. אובדן או גניבת ציוד מחשוב נייד ונייח ומסמכים המכילים מידע רגיש.

5.13. **<u>אירועי אבטחת מידע</u>**

5.13.1. מנהל יחידת המחשוב אחראי להגדרת איתור, מעקב, ניטור ובקרה, דיווח ותיעוד כל מקרה בו התגלה אירוע המעלה חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה ו/או הסכמים, במערכות שמתופעלות על ידי העירייה (להלן : "**אירועי אבטחה**").

5.13.2. ספקים אשר מחזיקים/מנהלים מאגרי מידע ומערכות מאגרי מידע, אחראים לאירועי אבטחת מידע במערכות המאגרים שברשותם, לגבי מידע ושירותים של העירייה ולתיעוד האירועים.

5.13.3. תיעוד זה יבוסס, ככל האפשר, על רישום אוטומטי. התיעוד יכלול, בין היתר, הליכי שחזור המידע ובכלל זה את זהותו של מי שביצע את הליכי השחזור ופרטי המידע ששוחזר.

5.13.4. ניתן לאבחן ולזהות אירועי אבטחה במספר דרכים:

5.13.4.1. ניצול לרעה של סמכויות עובדים לצורך עדכון / שיבוש / שינוי מידע ותהליכים;

5.13.4.2. משתמש המבחין באי סדרים ו/או תהליכים לא תקינים ו/או חריגה מנהלי העבודה ו/או אירועים חשודים בסביבת העבודה שלו (כך למשל – הפרה של נוהלי אבטחת מידע על ידי העובד או על ידי עובדים אחרים; קיום או חשד לפרצה / חשיפה / שינוי / מחיקה באבטחת המידע במערכות; נעילה פתאומית של החשבון; זמן כניסה אחרון לא סביר (ככל שהדבר אפשרי); סימנים לפעילות לא ידועה (לדוגמה: קבצים חדשים, שינויים בשולחן העבודה וכיו"ב); ניסיונות (מוצלחים או כושלים) להשגת גישה לא מאושרת למערכת או המידע האגור בה; חוסר זמינות בשרות וכיו"ב;

5.13.4.3. כלים / מנגנונים ייעודיים ואוטומטיים לאבחון והתראה, כגון קבצי לוג וכיו"ב;

5.13.4.4. הודעות / עדכונים מגופים חיצוניים דוגמת: תוכנות אנטי וירוס, מערכות וכיו"ב;

5.13.4.5. התראות המיוצרות על ידי מערכות המחשוב (אזהרות מערכת / הודאות שגיאה).

5.13.5. במאגרי מידע בעלי רמת אבטחת בינונית, יקיים מנהל יחידת המחשוב דיון לעניין אירועי האבטחה, אחת לשנה לפחות ויבחן את הצורך בעדכונו של נוהל זה.

5.13.6. במאגרי מידע בעלי רמת אבטחה גבוהה, יקיים מנהל יחידת המחשוב דיון לעניין אירועי האבטחה, אחת לרבעון לפחות ויבחן את הצורך בעדכונו של נוהל זה.

5.13.7. מנהל יחידת המחשוב ידווח, באופן מיידי, למנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך בקרות אירוע אבטחה <u>חמור (כהגדרתו בתקנה 1 לתקנות אבטחת מידע)</u> וכן ידווח להם על הצעדים שנקט בעקבות האירוע.

מנמ"ר ו/או מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך ידווח לרשם באופן מיידי בקרות אירוע אבטחת מידע חמור וכן ידווח לו על הצעדים שננקטו בעקבות האירוע.

5.13.8. מנהל יחידת המחשוב והספקים ישמרו תיעוד של אירועי האבטחה והנתונים שיצברו בהתאם לסעיף זה באופן מאובטח למשך 24 חודשים, לכל הפחות.

5.14. **<u>הוראות לגבי התמודדות עם אירועי אבטחת מידע</u>**

5.14.1. מנהל המאגר יכלול במסגרת הדרכות המודעות לעובדים, הנחיה לגבי חשיבות הזיהוי והדיווח על אירועים חשודים וחשיבות מהירות הדיווח למנהל יחידת המחשוב ולמנהל המאגר.

5.14.2. מנהל יחידת המחשוב יחייב בכתב מכל ספק, אשר קיימת לו נגישות למערכות המחשבים ולמידע רגיש של העירייה, התחייבות לפיה כל אירוע אבטחת מידע במערכות המחשוב שלהם, אשר נוגעות למערכות המחשוב של העירייה או למידע של העירייה, ידווח גם למנהל יחידת המחשוב של העירייה.

5.14.3. אירוע שזוהה ואושר כאירוע אבטחת מידע על ידי מנהל יחידת המחשוב, יעבור תהליך סיווג על ידו, אשר במסגרתו יגדיר את חומרתו. חומרת האירוע נקבעת לפי גודל והיקף הנזק הצפוי כתוצאה מהאירוע ו/או הנזק שכבר נגרם, ותקבע את דרך הטיפול באירוע והדרגים המיודעים והאחראים.

5.14.4. מנהל יחידת המחשוב יקבע את דרגת חומרת האירוע לפי גודל הנזק:

5.14.4.1. מקומית – אירוע הגורם לנזק מקומי כהפרעה מועטה של פעילות ואינו מסוגל להתפשט למערכות אחרות (הדבקות בווירוס של מחשב בודד, אירועים מסוג זה יטופלו מקומית ע"י מנהל יחידת המחשוב).

5.14.4.2. בינונית – אירוע הגורם לפגיעה מקומית, אך חמורה ומשמעותית בפעילות העירייה וביכולת ניהול הפעילות (השבתת הרשת המקומית כתוצאה ממתקפת CYBER).

5.14.4.3. גבוהה – אירוע חמור הגורם לפגיעה מערכתית מהותית העלולה להוביל לפגיעה חמורה ביותר בביצועי העירייה, יכולתה התחרותית או בתדמיתה, ולפגוע בצורה חמורה תפעולית, כלכלית או משפטית העירייה. (וירוס במערכות התפעול, גניבת נתונים של עובדי העירייה).

5.14.5. מנהל יחידת המחשוב ינתח ויטפל באירוע בהתאם לסוג האירוע כדלהלן:

5.14.5.1. חשיפת מידע רגיש (לרבות חשיפת סיסמאות משתמשים ואובדן מחשב נייד של העירייה) - ניתוח האירוע יכלול זיהוי כל המקומות בהם מאוחסן המידע והמורשים לקראו, תחקור העובדים שניגשו למידע, ניתוח רשימות הניטור וכל אפשרויות הגישה למידע שנחשף (פיזית, לוגית).

5.14.5.2. התקפות מניעת שירות (Denial Of Service) - ניתוח האירוע יכלול את זיהוי הגורם המותקף (נתב חיצוני/פנימי, תחנה, רכיב אחר) ומיפוי דרכי הגישה אליו, ניתוח רשימות הניטור של כל הרכיבים במסלולי הגישה השונים לרכיב המותקף, דוחות תעבורה ברשת (sniffer) והתחקות אחר כתובת המתקיף.

5.14.5.3. השתלטות על מערכות/יישומים - ניתוח האירוע יכלול סריקת המערכת הפגועה ומערכות משיקות כדי לזהות את סוג החדירה ולהעריך את הנזק שנגרם. בדיקות טלאים חסרים העלולים לשמש לחדירה, שינויים בקבצי מערכת ההפעלה ובקוד, קבצים ששונו לאחרונה, משתמשים שנוספו לאחרונה ועוד.

5.14.6. באירועים קריטיים או באירועים כמו פריצה או השתלטות על אפליקציות ומערכות תפעול בעירייה או אצל ספק חיצוני, מנהל יחידת המחשוב או הספק, לפני העניין, יהיה אחראי לבודד את האזור הנגוע. מטרת בידוד המערכות שנפגעו הינה למנוע התפשטות האירוע למערכות אחרות והרחבת הנזק, מניעת מחיקה של ראיות על ידי התוקף, ומניעת שימוש לרעה ברשת כבסיס תקיפה של חברות אחרות. בידוד יכול להיעשות ע"י ניתוק הרשת, סגירת המערכת הפגועה, סגירת שירותים בתוך המערכת הפגועה, סגירת חשבונות מסוימים או רק החלפת סיסמא.

5.14.7. מנהל יחידת המחשוב או הספק, לפי העניין, אחראי לסקור מערכות שכנות המתממשקות למערכת הפגועה (למשל גיבוי) על מנת לוודא כי אין צורך לבודד גם אותן.

5.14.8. מנהל יחידת המחשוב יודיע לממונה אבטחת המידע על המקרה ועל צעדי הבידוד שבוצעו. מנהל יחידת המחשוב יוציא הודעה בהתאם למשתמשים ולבעלי התפקידים הרלוונטיים.

5.14.9. עדכון גורמים עסקיים - במקרה של דליפת מידע רגיש או השתלטות על מערכות, ממונה אבטחת המידע ינקוט בצעדי מנע עסקיים ו/או יודיע לגורמים המתאימים, על מנת להקטין את נזק דליפת המידע או שינוי הנתונים.

5.14.10. לפני שנשקלת החזרת המערכות לתפקוד מלא, מנהל יחידת המחשוב יוודא מספר פעולות חשובות: זיהוי והכחדה של שורשי הבעיה. יש לחפש ולנקות את כל הדלתות האחוריות (back doors) או אמצעים אחרים שנועדו להתקפה עתידית ונשתלו במהלך האירוע.

5.14.11. במידה והאירוע חייב מחיקת מידע/ פרמוט שרתים וכו', מנהל יחידת המחשוב יוודא ביצוע התקנה מחדש של כל הקבצים המעורבים, תכנות האפליקציה, התשתית, המשתמשים והקונפיגורציה הקשורים לאירוע. התקנה מחדש של מערכת ההפעלה וכל הטלאים (patches) שפורסמו עבורה. הפעלה מרבית של אמצעי הניטור הקיימים בתחנה ובמערכת ובמידת הצורך שחזור נתונים מגיבוי, ולעיתים גם להשלים מידע שאבד.

5.14.12. בדיקות לפני חזרה לפעילות:

5.14.12.1. מנהל יחידת המחשוב או הספק, לפי העניין, יבצע בדיקה למערכות לאחר השחזור כדי לוודא כי אינן מכילות פרצות אבטחה ו/או פגיעות אחרות והאירוע אכן הסתיים.

5.14.12.2. מנהל יחידת המחשוב או הספק, לפי העניין, יבצע בדיקה למערכות מבחינה פונקציונלית.

5.14.12.3. במקרה והאירוע גרם לשינוי נהלים או תהליכים, ממונה אבטחת מידע יתדרך את כל הנוגעים בדבר, ויוודא שהתהליכים החדשים מוכנים ליישום.

5.14.12.4. ממונה אבטחת מידע יוודא בדיקת כל המערכות המתממשקות למערכת הפגועה כדי לוודא כי לא נפגעו.

5.14.13. העלאת המערכות, ממונה אבטחת מידע וסייבר יוודא :

5.14.13.1. העלאת המערכות השונות, פתיחת הגישה לאפליקציות שנחסמו וכו'.

5.14.13.2. העלאת השירותים אשר הורדו (מייל/ אינטרנט וכו') – בצורה הדרגתית ובניטור הפעילות.

5.14.13.3. הודעה לכל המשתמשים והמעורבים בנושא על חזרה לפעילות שוטפת.

5.14.13.4. המשך הניטור - ממונה אבטחת מידע וסייבר יוודא המשך הפעלת אמצעי הניטור בשרתים וברשת בסמוך לעליית המערכות, על מנת לוודא כי אירוע האבטחה לא חוזר.

5.14.14. בסיום אירוע אבטחת מידע, יתחקר ממונה אבטחת המידע את תהליך הטיפול באירוע ויחליט על הפעולות שיש לבצע במטרה למנוע אירוע נוסף. הנושאים לבחינה הם:

5.14.14.1. מימוש נוהל זה, בחינה אם נדרש שיפור בתהליך התגובה המוגדר למעלה.

5.14.14.2. האם נדרש שיפור במנגנוני הניטור ואיתור האירועים.

5.14.14.3. כלים שעשויים לעזור בתהליך התגובה לאירועים, כמו שדרוג תכנת נתבים, התקנת firewalls פנימיים, שינוי כתובות IP, גישה למידע רגיש בשימוש באפליקציה ייעודית, וכדומה.

5.14.14.4. שיפורים לעמידות העירייה לאירועים כאלה.

5.14.14.5. שיפורים לתהליך ההתאוששות מאירועים אלו.

5.14.14.6. תהליכי תקשורת בין הגורמים שטיפלו באירוע.

5.14.15. מוכנות של מנהל יחידת המחשוב והספקים השונים לאירועים אלו.

5.14.16. ממונה אבטחת מידע יוודא, אחת לשנה, כי הספקים מבצעים בחינה של חוקי הניטור שהוגדרו ותקינותם ואיכות האירועים שמתקבלים.

5.15. <u>ניהול מאובטח ומעודכן של מערכות המאגר</u>

5.15.1. מנהל יחידת המחשוב יקפיד על ניהול ותפעול תקין של מערכות המאגר, לפי המקובל בהפעלות מערכות אלה.

5.15.2. מנהל יחידת המחשוב יפריד, בהיקף ובמידה הסבירים האפשריים, בין מערכות המאגר אשר ניתן לגשת מהן למידע, לבין מערכות מחשוב אחרות המשמשות את העירייה.

5.15.3. מנהל יחידת המחשוב ידאג לכך שיערכו עדכונים שוטפים של מערכות המאגר, לרבות חומר המחשב הנדרש לפעולתן. לא יעשה שימוש במערכות שהיצרן לא תומך בהיבטי האבטחה שלהן, אלא אם ניתן מענה אבטחה הולם.

5.15.4. ספקים אשר מחזיקים/מנהלים מאגרי מידע ומערכות מאגרי מידע, אחראים לניהול מאובטח ומעודכן של מערכות המאגרים שברשותם.

5.16. **<u>אבטחת תקשורת</u>**

5.16.1. מנהל יחידת המחשוב לא יחבר את מערכות המאגר לרשת האינטרנט או לרשת ציבורית אחרת, בלא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב.

5.16.2. העברת מידע ממאגר מידע, ברשת ציבורית או באינטרנט, תיעשה תוך שימוש בשיטות הצפנה מקובלות.

5.16.3. במאגר מידע שניתן לגשת אליו מרחוק, באמצעות רשת האינטרנט או רשת ציבורית אחרת, מנהל יחידת המחשוב ייעשה שימוש באמצעים שמטרתם לזהות את המתקשר והמאמתים את הרשאתו לביצוע הפעילות מרחוק ואת היקפה, וזאת בנוסף לשימוש באמצעי אבטחה לעיל.

5.16.4. ספקים אשר מחזיקים/מנהלים מאגרי מידע ומערכות מאגרי מידע, אחראים לאבטחת התקשורת במערכות המאגרים שברשותם.

5.16.5. תווך תקשורת מול ספקים מוצפן.

5.17. **<u>ביקורות תקופתיות</u>**

5.17.1. <u>מטרת הביקורות התקופתיות הינה הבטחת התנהלות תקנית בעירייה ביחס למערכותיה ומאגרי המידע שלה, והכל בהתאם להוראות נוהל זה ותקנות האבטחה.</u>

5.17.2. מנכ"ל העירייה אחראי לכך שתיערך, אחת ל-24 חודשים לפחות, ביקורת פנימית או חיצונית, על ידי גורם בעל הכשרה מתאימה לביקורת בנושא אבטחת מידע, שאינו ממונה האבטחה של המאגר, בליווי מבקר העירייה במטרה לוודא עמידתה של העירייה בתקנות אבטחת מידע.

5.17.3. <u>במסגרת הביקורת התקופתית ייבחנו, בין היתר, הנושאים הבאים:</u>

<u>* עמידת העירייה בהוראות נוהל זה ותקנות האבטחה;</u>

<u>* קיום ביקורות תקופתיות נדרשות;</u>

<u>* התאמת אמצעי האבטחה של העירייה לנוהל זה ולתקנות האבטחה, וזיהוי ליקויים ככל שישנם.</u>

5.17.4. המבקר ידווח בדו"ח הביקורת על התאמת אמצעי האבטחה לנוהל זה ולתקנות אבטחת המידע, יזהה ליקויים ויציע אמצעים הדרושים לתיקון המצב.

5.17.5. מנכ"ל העירייה בשיתוף מבקר הפנים, ידון בדוחות הביקורת שיועברו לו ויבחן את הצורך בעדכון מסמך הגדרות המאגר או נוהל זה.

5.17.6. העירייה תהיה רשאית לקיים ביקורת אחת לעניין כל מאגרי המידע שברשותה, המצויים באותה רמת אבטחת מידע ולהסתמך על בקורת שיבצעו מחזיקי מאגרים.

5.17.7. מנכ"ל העירייה ישמור את דוחות הביקורת באופן מאובטח למשך 24 חודשים, לכל הפחות.

5.17.8. מנהל יחידת המחשוב בשיתוף עם מבקר הפנים, יקבע נוהל לביצוע גיבויים לדוחות הביקורת, באופן תקופתי שגרתי.

5.17.9. מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך יבחנו מעת לעת, ולכל הפחות אחת לשנה, את היקף המידע הקיים במאגרי העירייה. מצא כי קיים מידע שאינו נדרש לעירייה נוכח הגדרת מאגריה, יכין הצעת הסרת מידע .הצעת הסרת מידע כאמור תכיל תיאור תמציתי של המידע אשר לדעת מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך אינו נדרש ולפיכך יש להסירו. הצעת הסרת המידע תועבר לעיונו של ראש העירייה והוא יאשרה. לאחר האישור כאמור, יוסר המידע לצמיתות ממערכות המידע של העירייה ולא יהא נגיש לעובדי העירייה מלבד גורמים רלוונטיים במערכות המידע של העירייה.

5.17.10. מנהל יחידת מחשוב ו/או מי שהוסמך על ידו לצורך כך בעירייה ישמרו עותק של המידע שהוסר לצורכי גיבוי ושחזור למשך 24 חודשים, לכל הפחות, החל מיום אישור בקשת ההסרה. העותק ישמר בנפרד ממערכות המידע של העירייה, ובתום התקופה ייגנז לאלתר.

5.18. **בקרה**

5.18.1. מנהל יחידת המחשוב יבחן, אחת לשנה, את הצורך בעדכון הנוהל.

5.18.2. כמו כן, מנהל יחידת המחשוב יבחן את הצורך בעדכון הנוהל במקרים הבאים:

5.18.2.1. בעת שינויים מהותיים במערכות המאגרים או בתהליכי עיבוד מידע.

5.18.2.2. בעת סיכונים טכנולוגיים חדשים הנוגעים למערכות המאגר.

5.18.2.3. מנהל יחידת המחשוב יוודא כי הנוהל והוראותיו יבוצעו על ספקי העיריה, עובדיה וכל גורם שהוא אשר עשוי לבוא במגע עם המידע כאמור בנוהל זה.

5.18.2.4. נוהל זה מותנה באישור מליאת מועצת העירייה.

נספח א' – רשימת הרשאות תקפות (מסווג)

נספח ב' - מבנה מאגרי המידע ורשימה מעודכנת של מערכות המאגר (מסווג)

נספח ג' – נספח מיקור חוץ להסכם התקשרות עם ספקים

נספח ג' – נספח מיקור חוץ להסכם התקשרות עם ספקים

1. הצהרות והתחייבויות הספק

הספק מצהיר, מאשר ומתחייב כלפי עיריית רמת השרון (להלן "**העירייה**") כדלקמן:

1.1. יש לו את הכישורים, הידע, האמצעים והיכולת לספק את השירותים באופן המיטבי ביותר. כמו כן, ידועים לו כל החוקים, התקנות וכל הוראה אחרת הנוגעים לאספקת השירותים והוא מתחייב למלא אחר הוראות כל דין, לרבות, אך לא רק, חוק הגנת הפרטיות, התשמ"א-1981 והתקנות המותקנות מכוחו, לרבות תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 והנחיות רשם מאגרי המידע כפי שיעודכנו מעת לעת וכיו"ב.

1.2. ימסור לעירייה כל מידע שיידרש ממנו על-ידה בנוגע לאספקת השירותים, אשר מצוי בידו ואין מניעה לגלותו על-פי דין ו/או הסכם, במועד ובאופן שתקבע בסבירות העירייה, ובכלל זה דו"חות, נתונים או כל מידע אחר שיידרש על-ידה מעת לעת ובכלל זה גם בתום תקופת ההסכם.

1.3. עם סיום ההתקשרות לאחר גמר מתן השירותים, הספק מתחייב שלא לעשות כל שימוש במידע אשר הגיע לידיו בכל הקשור ו/או הנובע מהסכם זה. כן מתחייב הספק להשמיד כל מידע שנותר בידיו השייך לעירייה ו/או נאסף עבורה וכן להימנע מהשארת עותק של המידע ברשותו, בכל דרך שהיא, וזאת לאחר שווידא כי כלל המידע הועבר במלואו לעירייה ומסר לעירייה הצהרה מאומתת כדין אודות האמור.

1.4. כי השימוש במידע שיועבר לספק בהתאם להוראות הסכם זה ייעשה אך ורק במסגרת מתן השירותים בהסכם זה ויתבצע על-ידי מורשי גישה למידע המועסקים אצל הספק ולא באמצעות גופים חיצוניים ו/או קבלני משנה המעניקים לו שירותים. עוד מצהיר ומתחייב הספק לתדרך כל עובד ו/או מי מטעמו שהינו בעל גישה למידע באשר לשימוש המותר במידע, לרבות החתמתם על התחייבות לשמירת סודיות ביחס למידע השייך לעירייה.

1.5. הספק מתחייב, כי ככל שייאסף עבור העירייה מידע אישי אודות אנשים, אגב או לצורך ביצוע השירותים עבור העירייה, האיסוף יתבצע בהתאם להוראות הדין.

1.6. הספק מתחייב לאפשר לנושאי המידע שפרטיהם נמצאים אצלו לממש את זכויות העיון והתיקון המוקנות להם, והכל תוך זמן סביר ובהתאם להוראות כל דין. כמו כן, הספק מתחייב לעדכן את העירייה באופן מיידי על כל פרט אשר יבקש את הסרתו מרשימת הדיוור שתועבר לידיו. כל נזק אשר ייגרם לעירייה בעקבות חוסר עדכון כאמור יהא באחריותו המלאה של הספק.

1.7. הספק מתחייב שלא להעביר ו/או למכור ו/או להפיץ את המידע המתקבל מהעירייה, בין במישרין ובין בעקיפין, בין בתמורה ובין שלא בתמורה, וכי במסגרת קיום חובותיו תהא הפרדה ברורה בין הפעילות שתתבצע עבור העירייה לבין הפעילות המבוצעת עבור גופים אחרים ו/או עבור הספק עצמו.

2. סודיות ואבטחת מידע

2.1. לצרכי הסכם זה, "**מידע סודי**" הוא מידע וידע מכל סוג, שאינו נחלת הרבים ושאינו ניתן לגילוי כדין בנקל על ידי אחרים, שנמסר או שיימסר לספק ו/או יגיע לידיו מידי העירייה ו/או כל מי מטעמה, או יגיע לידי הספק בכל דרך אחרת במסגרת ההסכם או המשא ומתן שקדם לכריתתו או אגב מתן השירותים לעירייה ולצרכיה, במישרין או בעקיפין, ולמעט מידע שהיה מצוי בחזקתו החוקית של הספק עובר למסירתו כאמור או מידע שנמסר לספק על-ידי צד שלישי שלא תוך הפרה של חובת סודיות בין אותו צד שלישי לבין העירייה.

2.2. הספק מתחייב, התחייבות בלתי חוזרת ושאינה מוגבלת בזמן, לרבות לאחר תום תקופת ההתקשרות בין הצדדים, לשמור בסודיות מוחלטת ולא להעביר או לגלות, בין במישרין ובין בעקיפין, בין בתמורה ובין שלא בתמורה, את המידע הסודי שהועבר לידיו מהעירייה או מידע שהתקבל אגב, בעקבות או למען ביצוע הסכם זה, ללא הסכמת העירייה, מראש ובכתב, ולא לעשות כל שימוש במידע הסודי למטרה אשר אינה קשורה לאספקת השירותים.

2.3. הספק מתחייב ומצהיר, כי ידוע לו שכל מידע שיגיע לידיו במהלך אספקת השירותים ביצוע הינו רגיש ביותר, וכי הגעתו לידי צדדים שלישיים עלולה לגרום לעירייה ו/או כל מי מטעמה נזקים חמורים, שהספק יישא באחריות להם באופן מלא ובלעדי, ולעתים לא יהא די בפיצוי כספי בגינם. לפיכך, בכל מקרה של חשש לגילוי אסור של המידע הסודי, העירייה תהא רשאית, בין היתר, לבקש צווי מניעה ותפיסה נגד הספק.

2.4. הספק מתחייב לפעול כך שהמידע שיועבר אליו בהסכם זה יאובטח כך שלא תתאפשר אליו גישה, בין באופן אקטיבי ובין באופן פאסיבי, לאיש מלבד המורשים לכך. ולהודיע לעירייה מיד לכשייוודע לו על כל נזק שנגרם לנכסי המידע של העירייה לרבות כל דליפה, שינוי או מחיקה של מידע.

2.5. העירייה תהא רשאית לבצע מעקב וביקורות שוטפות, לרבות ביקורות פתע, לבדיקת פעילותו של הספק בכל הקשור לאספקת השירותים. לצורך כך, נציג מטעם העירייה יהא רשאי להיכנס למשרדי הספק בשעות העבודה המקובלות, בליווי נציג מטעם הספק, ולבדוק את תקינות נהלי האבטחה וכן את קיום הוראות הסכם זה בכללותו.

2.6. הספק מתחייב כי ישמור על כל מידע שיתקבל מהעירייה ו/או אגב מתן השירותים ו/או לצורך ביצוע הסכם זה, רק למשך פרק הזמן הנדרש במישרין לביצוע השירותים על פי הסכם זה. ככל שקיימת הוראה בדין המחייבת את שמירת המידע אצל הספק, הספק מתחייב בזאת לוודא כי אמצעי האבטחה והבקרה שהוגדרו בהסכם זה יישארו אפקטיביים לכל אורך תקופת שמירת המידע.

ולראיה בא הספק על החתום:

_____ _____

חתימת הספק תאריך