

## נוהל טיפול במאגרי מידע - עיריית עראבה

1. חוק הגנת הפרטות, התשמ"א-1981 (להלן: "החוק" או "חוק הגנת הפרטיות") קבע 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 החש מפני שימוש לרעה או פגיעה בשלמות המידע.
2. תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "תקנות אבטחת מידע") קובעות עקרונות בטחת מידע הקשורים בניהול ושימוש מידע במאגרי המידע, בהתבסס על תקני אבטחת מידע מקובלים בעולם.
3. אבטחת מידע ברשת ובמערכות עיריית רמת השרון (להלן: "העירייה") הינה חיונית להגנת המידע של העירייה, תושביה ועובדיה.
4. לאור זאת, על העירייה להתקין ולהטמיע מערכות הגנה מני איומים וחיצוניים ופנימיים וליישם בקרות נוהליות וטכנולוגיות לאכיפת רמת אבטחת מידע ואבטחה פיזית על תשתיות המידע.

### **מטרת הנוהל**

5. הגדרת כללי אבטחת המידע המחייבים את העירייה, עובדיה וספקיה.
6. התאמת פעילות העירייה להוראות החוק, לתקנות שהותקנו מכוחו ובפרט לתקנות אבטחת המידע, ולהנחיות הרשות להגנת הפרטיות, כפי שיעודכנו מעת לעת.
7. 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.
8. הגדרת פעולות ובקורות הנדרשות לעמידה בדרישות החוק ותקנות אבטחת המידע.

### אזורים מאובטחים

9. מנהל יחידת המחשוב יגדיר אשורי אשר יוגדרו כ"אזורים רגישים מבחינה טכנולוגית".
10. מעורכות מאגרים של העירייה יישמרו במקום מוגן, המונע חדירה וכניסה אליו בלא הרשאה, והתואם את אופי פעילות המאגר ורגישות המידע המצוי בו וכמפורט בנוהל זה.
11. 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 לאשרו מול מנכ"ל העירייה את הרשימה כאמור.

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

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

14. 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 תכני בליווי גורם רלוונטי בעירייה ובאישור מנהל המאגר מבקש שנכנס למבני העירייה עם אמצעי מחשוב נייד, יחתום על טופס מבקר עם לפטופ. הטופס כאמור יישמר לצורך תיעוד ובקור.

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

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

- אין לחבר לרשת העירייה ו/או לשמור מידע בתקנים 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 התקשורת במקרה של אובדן או גניבה.
- על העירייה להגביל או למנוע, ככל הניתן, את אפשרות החבור של התקנים ניידים למערכותיה במתכונת ההולמת את רמת אבטחת מידע שחלה על המאגר, רגישות ואת קיומם של אמצעי הגנה מתאימים מפני סיכונים אלה.
- ככל שהשימוש בהתקן הנייד מאפשר למשתמש גישה למאגר המידע ו/או להעתקת תוכנו, אז שעל העירייה לנקוט באמצעי ההגנה הסבירים הנדרשים, בשים לב לסיכונים המיוחדים הקושרים לכך.
- במקרה בו משתמש ו/או כל עובד של העירייה נתקבל באירוע חריג, אשר העלה אצלו חשש לפגיעה בשלמות המידע במאגר או זליגתו אל מחוץ למערכת המאגר בלא הרשאה, עליו לדווח על כך מיידית למנמ"ר/מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך בעירייה, והאחרון יפעל בהקדם לתחקור הסוגה ומציאת פתרון, בנוסף לדיווח שיעביר למנכ"ל העירייה.

17. אין לאפשר למבקרים גישה למערכות המידע של העירייה, למעט קבלני תמיכה אשר אושרו מאשר עלי-ידי מנהל המאגר ו/או מנהל התחום ובפיקוח של מלווה בעל יד מקצועי מתאים לצורך בקרה אודות הפעולות המבוצעות.
18. מברים קבועים.
19. אישור מבקרים קבועים יתבצע על-ידי הגורם מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך בעירייה בלבד.
20. מבקר קבוע יחתום על הצהרת סודיות, באחריות מנהל התחום הרלוונטי.
21. מבקר קבוע לא יחויב בליווי בעת שהותו במתחמי העירייה.
22. גישת מבקרים קבועים למערכות המידע תתאפשר על פי צורך מקצועי ובאישור מנהל המאגר ו/או מנהל התחום בלבד.
23. עם סיום תפקידו של המבקר הקבוע, באחריותו של מנהל התחום לעדכן מידיית את מנהל יחידת המחשוב ו/או מנמ"ר/מנכ"ל ו/או מי שהוסמך על-ידם לצורך כל בעירייה שיש לבטל את השאת השהייה שניתנה למבקר הקבוע במתחמי העירייה.
24. מנהל יחידת המחשוב ינקוט אמצעים לבקרה ולתיעוד של הכניסה והיציאה מתארים בהן מצויות מערכות המאגר, וכן יקיים תיעוד של הכנסה והוצאת ציוד אל מערכות מאגרי המידע ומהן. מנהל יחידת המחשב ישמור נתונים אל באופן מאובטח למשך 24 חודשים, לכל הפחות.
25. גריסת מסמכים מתבצעת אחת לשבוע.
26. הספקים אחראים להגנה על המערכות המצויות ברשתם, לבקרה ולתיעוד של הכניסה והיציאה מאתרים בהן מצויות מערכות המאגר, וכן לתיעוד של הכנסה והוצאת ציוד אל מערכות מאגרי המידע ומהן.

### **אבטחת סביבת העבודה והמחשבים**

27. בעת עזיבת סביבת העבודה, עובדי העירייה יעבדו בשיטת מדיניות "שולחן נקי (desk clear policy) כמפורט להלן :
28. מידע רגיש יאוחסן באופן מאובטח, במתקן נעול (מגירה, ארון או כספת, בהתאם למידת הרגישות והאמצעים הזמינים). במדיה ואן, יש לנעול את החדר.
29. בתום יום העבודה או בעת עזבת מקום העבודה לזמן ארוך על המשתמש להותיר את סביבת העבודה כשמסמכים 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 ישמר לפרק זמן מינימאלי נדרש, וזאת בהתאם להוראות ודרישות העירייה והוראות כל דין המגבילות את משך שמירת המידע כאמור.
30. מנהל יחידת המחשוב יישם נעילת מסך עם סיסמה לאחר 30 דקות ללא פעילות, בכל תחנות הקצה.
31. מנהל יחידת המחשוב יתקין בכל שרת ותחנות עבודה תוכנת אנטי-וירוס ויגדיר תהליך יומי לעדכון.
32. מנהל יחידת המחשוב יגדיר בכל שרת ותחנות עבודה תהליך לעדכן מערכת ההפעלה בעדכוני אבטחת מידע והתקנת חבית שירות של היצרן.
33. שימוש ברכיבי dok או בכונן CD ייעשה באישור מנכ"ל בלבד.
34. מנהל יחידת המחשוב יגדיר ניתוק אוטומטי של משתמשים לאחר השעה 20:00.
35. כל שינוי בתצורת המחשב האישי, ובכלל זה התקנת תוכנה, או חומרה, כמו כן שינוי האנטי וירוס, יתבצע ע"י מנהל יחידת המחשוב או מי שהוגדר מטעמו, או ע"י ספק מורשים באישורי ותוך תיעוד הפעילות.
36. התקשרות עם הספקים מתבצעת בתווך מוצפן.
37. הספקים אחראים לאבטחת סביבת העבודה והמחשבים שברשותם. מנהל יחידת מחשוב ו/או מנהל אגף ביטחון יוודאו קיום הוראה זו.

### ניהול הרשאות

38. ניהול ההרשאות במחשבי העירייה ייעשה ע"י מנהל יחידת המחשוב באמצעות מנגנון ממוכן לניהול הרשאות (AD) (להלן: "מנגנון הבקרה").
39. מטרת מנגנון הבקרה הינה לספק מידע אמין ומלא בעת בדיקה או תחקור, על מנת ליצור תמונת מצב מפורטת אחר האירועים השונים שהתרחשו
40. יש לתעד את כל הפעולות השונות המבוצעות על רכיבי הרשת הרגישים בסביבת מאגרי המידע האישי המצוי בהם, החל מכניסה וכלה בגישה לקובצי מערכת רגישים אלו.
41. יש ליידע את העובדים כי פעילותם מתועדת. מקום בו ניתנת גישה לגורם חיצוני למערכות העירייה מסיבה כלשהי, יש לעדכן אף אותו כי פעולותיו מתועדות.
42. אין לשמור במנגנון הבקרה מידע רגיש בצורה גלויה.
43. יש לוודא כי כל מנגנוני הבקרה פעילים עם עליית מערכות העירייה.

44. מנגנון הבקרה מנוהל על ידי מנהל יחידת המחשוב ומאפשר ביקורת על הגישה למערכות המאגר וכלל זה נתונים אלה: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה.
45. ספקים אשר מחזיקים/מנהלים מאגרי מידע ומערכות מאגרי מידע, אחראים לקיום מנגנון בקשה במאגרם ובמערכות שברשותם.
46. מנהל יחידת המחשוב יגדיר כי רק לאנשי המחשוב אשר להם צורך בכך לשם ביצוע תפקידם תהיה גישה לניהול ההרשאות ולקבצי הלוגים של מנגנון הבקרה. כמו כן, מנגנון הבקרה לא יאפשר, ככל יכולתו, ביטול או שינוי של הפעלתו ויאתר שינויים או ביטולים בהפעלתו ויפיץ התראות למנכ"ל העירייה, למנהלי המאגרים, למנהל יחידת המחשוב, לממונה אבטחת המידע וסייבר.
47. מנהל יחידת המחשוב יקבע נוהל בדיקה שגרתי לנתוני התיעוד של מנגנון הבקרה ויערוך דו"ח של הבעיות שהתגלו והצעדים שננקטו.
48. מנהל יחידת המחשוב ישמור את נתוני התיעוד של מנגנון הבקרה באופן מאובטח למך 24 חודשים, לכל הפחות.
49. מנהל יחידת המחשוב ו/או מנהל כל מאגר יידע את בעלי ההרשאות במאגר בדבר קיום מנגנון הבקרה למערכות המאגר.
50. מנהל יחידת המחשוב יודא כי חשבון משתמש בגישה למחשבי העירייה ולמערכות העירייה ישויך לעובד מסוים ותוגדר אחריות של העובד על החשבון והפעולות המתבצעות בו.
51. מנהל יחידת המחשוב יגדיר הרשאות בגישה למחשבי העירייה ולקבצים ולמערכות ברשת העירייה בהתאם לתפקידם ולצורך ביצוע תפקידם בלבד. הוראה זו תחול ע מנהל יחידת המחשוב גם ביחס לגישה המוענקת לספקים חיצוניים לעירייה.
52. במערכות המתופעלות על ידי ספקים, הספק ינהל ההרשאות בנפרד מלקוחות אחרים של אותו הספק.
53. 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).
54. בכל מקרה בו ידוע על הפסקת עבודה של משתמש המודר 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.

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

### סגירת / ביטול הרשאות משתמש

56. כאשר סיים עובד בעל הרשאה את עבודתו בעירייה, מנהל יחידת המחשוב יסגור את השאתו 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.
57. לצורך שמירה על רצף שירותי מידע, מנהל יחידת המחשוב ייבחן את הצורך לשמור או להעביר ספריות מהרשאה המיועדת לסגירה או הרשאותיו של משתמש אחר.
58. עובד המשנה את סטאטוס התפקיד שלו בעירייה- יש לשנות בהתאם גם את סיסמאותיו והרשאותיו.

### שימוש בשם משתמש וסיסמאות

59. הסיסמה הינה המפתח לגישה למערכות המידע. על הסיסמה להישמר פרטית וסודית.
60. שם המשתמש (user ID/Username) מיועד לשימוש אישי בלבד וחל איסור על שימוש ויישומים בלבד, תוך תיעוד בקבץ ייעודי.
61. לא תתבצע הגדרות משתמשים גנריים לפעילות משתמשים אנושיים, אלא עבור שרתים ויישומים בלבד, תוך תיעוד בקבץ ייעודי.
62. אין לשמור 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.
63. אין לשמור את הסיסמה כתובה במקום בו היא עלולה להיחשף (למשל, מדבקה בסביבת המחשב, מתחת למקלדת, או בקובץ לא מוצפן על גבי המחשב).
64. 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.
65. מדיניות הסיסמאות ברשת(AD), תחנות הקצה והשרתים תוגדר כדלהלן.

- על הסיסמא יהיה 7 תווים לפחות.
- אורך הסיסמא יהיה 7 תווים לפחות.
- סיסמא תכיל לפחות אות אחת, וסיפרה אחת,
- אין לבחור סיסמאות כגון : סיסמא קלה לניחוש בדומה לשם
- המשתמש, תו אחד אשר חוזר על עצמו מספר פעמים וכיו"ב.
- הסיסמא תוחלף אחת ל-90 יום. לא ניתן לחזור על אותה סיסמא.
- סיסמאות ללא תוצגנה על המסך בעת הקשטן.
- תוגדר נעילת משתמש לאחר 7 ניסיונות זיהוי כושלים ושחרור ע"י מנהל יחידה המחשוב בלבד.

#### **אבטחת מידע בניהול כוח אדם**

66. כלל עובדי העירייה מחויבים לשמור על אבטחת המידע בהתאם להוראות נוהל זה והראות כל דין.
67. הגשת מועמדות לעבודה בעירייה, קבלת עובד לעבודה ב, ועבודתו בפועל יתבצעו בהתאם לנוהל זה בכל הקשור לאבטחת המידע.
68. 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 לא הנוגע בדבר.
69. באשר לבעלי הרשאות הקיימים עוד בטרם נכנס לתוקפו נוהל זה, מנהל המאגר יבחן את מידת התאמתם לגישה למאגר מידע באמצעים סבירים המקובלים בהליכי מיון עובדים ושיבוצם, וכל זאת בשים לב לרגישות המידע לסוג הרשאת הגישה ויעדכן בהתאם לצורך את הרשאות הגישה.
70. מנהל המאגר ידאג לקיום הדרכות לבעלי הרשאות, בטרם יקבלו גישה למידע שבמאגר או לפי שינוי היקף הרשאותיהם, בנושא החובות לפי חוק הגנת הפרטיות ותקנות אבטחת המידע וימסור להם מידע אודות חובותיהם לפי חוק הגנת הפרטיות ונוהל זה.
71. 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 בטחת 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 יודא את קיום ההדרכות כאמור.

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

73. 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.

74. טרם תחילת עבודתו של העובד החדש ומתן הסיסמאות והגישה למערכות המידע הרלוונטיות, תקיים העירייה הדרכה לעובד החדש, בה יובהרו הנהלים הקשורים בסיסמאות, הראשות גישה, יידוע העובד אודות מנגנון הבקרה האוטומטי שלך העירייה, הדרכה כאמור יכול שתועבר באופן פרונטלי או באמצעות לומדה וכיו"ב.

75. לעובדים חדשים הנדרשים לכך במסגרת תפקידם תוגדר תיבת דואר אלקטרוני ייעודית (להלן: "תיבת המייל"). תיבת המייל היא אישית עבור כל עובר 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 ולהוראות הגורם מנהל יחידת המחשוב ו/או מנמ"ר / מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כל בעירייה.

### שמירת מידע

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

77. תיקיות "המסמכים שלי" של המשתמשים ימופו לכוון רשת, וכן שולחן העבודה, במידת האפשר.

78. 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.

79. 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.



## גיבויים

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

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

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

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

84. 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.

85. קלטות הגיבוי יועברו אחת ליום לאתר חיזוני מאובטח (ניתן במבנה אחר של העירייה).

86. דרישות הגיבוי יכללו את הפרמטרים הבאים:

- תדירות גיבוי מלא/ משתנה.
- גיבוי מקוון / לא מקוון.
- תקופת השמירה של עותקי גיבוי בהתאם לחשיבות ורגישות המידע.
- תיעדוף גיבויים בהתאם לסוג המידע;

87. אמצעי אחסון הגיבוי יכללו את הפרמטרים הבאים:

- אחסון הגיבויים ייעשה במיקום נפרד מן המידע עצמו על מנת למנוע נזק למידע ולגיבוי באירוע אחד כגון שריפה או פיצוץ;
- יש לשמור את הגיבויים באזור חסין לאש;
- יש להגביל את הגישה לגיבויים. יש לבצע בקרה על רמת האבטחה של אתר אחסון הגיבויים פעם בשנה לכל הפחות;
- 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);

88. שחזור מידע רגיש יבוצע באישור מנמ"ר/מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך בלבד.
89. יש לתעד כל אירוע במסגרתו התבצע שחזור מידע רגיש. התיעוד יכלול את הסיבה לאיבוד המידע, אדם שביקש את המידע והאד שאיר את ביצוע השחזור. מידע זה יהיה זמין למנמ"ר/מנכ"ל העירייה.
90. 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 רשות העירייה.

### מיקור חוץ

91. העזרות בשירותי מיקור חוץ מהווה מרכיב משמעותי בפעילותם של ארגונים רבים במשק המודרני, במטרה לקדם יעילות, להוזיל עלויות ולהתמקד בליבת העיסוק של אותו אגון. כן, גם העירייה נעזרת לעתים בגופים חיצוניים המספקים עבודה 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.
92. 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.
93. 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 לידי. אפיון ראשוני זה, נועד למנוע העברת מידע אישי שאינו נדרש במישרין לצורך מתן השירות. בהקשר לאמור, ישנן שלוש רמות שירות (מהמחמירה לא הקלה):
- שירות הכולל איסוף ועיבוד המידע על-ידי הגורם החיצוני, לרבות הקמת מאגר מידע עבור העירייה;
  - שירות המחייב העברה או העתקה של כל מאגר המידע, או חלק מהותי ממנו, מהעירייה אל הגורם החיצוני;

- 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), הינה כמובן העדיפה, וזאת מאחר שהעברת עותק שלם של מאגר המידע או מתן גישה בלתי מוגבלת למערכות מצביבים סיכון ממשי של העברת מידע עודף, אשר אינו דרוש במישרין לצורך מילוי תפקידו החוזי של הגורם החיצוני המספק את שירותי 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 זו ולתעד אותה.
  - בעת בחנת המועמדים הראויים לשמש כגורמים חיצוניים בפעילות מיקור חוץ עבור העירייה, על מנמ"ר/מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כל לשים דגש על שלוש נקודות עיקריות ביחס לגורם החיצוני;
    - ניסיון קודם בעיבוד מידע מהסוג שעתיד להיות מועבר לאותו גורם חיצוני;
    - רקע ומוניטין של הגורם החיצוני;
    - קיום חשש לניגוד עניינים או לשימוש פסול במידע שעתיד להימסר לגורם החיצוני.
94. ככל שהמידע המועבר לגורם החיצוני לצורך שירותי מיקור החוץ הינו רגיש יותר, אזי שיש לנקוט במשנה זהירות בבחירת אותו גורם חיצוני.
95. 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.
96. לאור האמור לעיל, על מנמ"ר/מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך להסדיר במסגרת משפטית וארוגנית 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.
97. הסכם מיקור החוץ יכלול, בין היתר, הוראות אשר יתייחסו לדברים הבאים:
- המידע אותו הגורם החיצוני רשאי לעבד ומטרות השימוש המותרות
  - בו לצורי ההתקשרות;

- מערכות המאגר אליהן הגורם החיצוני רשאי לגשת, אם בכלל, ו/או המידע אשר יעבור לידי הגורם החיצוני ;
  - סוגי העיבוד או הפעולות אותם הגורם החיצוני רשאי לעשת ;
  - במקרה בן הגורם החיצוני אוסף מידע ישירות ממושא המידע, לוודא כי הוא מקיים את חובת הודעה למושא מידע כאמור בסעיף 11 לחוק הגנת הפרטיות ;
  - קיום בטוחות, לרבות עריכת ביטוח אחריות מקצועית ;
  - קיום זכות עיון ותיקון בהתאם לחוק עבור מושא המידע והוראות המפורטת את הדרך למימוש זכות זו, לרבות זמני תגובה, עלויות וכיו"ב ;
  - משך ההתקשרות, אופן השבת המידע לידי העירייה בסיום ההתקשרות, השמדת המידע ברשותו של הגורם החיצוני ודיווח על כך לעירייה ;
  - 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 ;
  - חובתו של הגורם החיצוני לקיים הדרכת ביחס למטרות השימוש במידע המועבר לכל מורשי הגישה מטעמו ולתעד אותן, ובנוסף להחתיים את בעלי ההרשאות של על התחייבות לשמירת סודיות המידע, שימוש במידע אך ורק בהתאם להוראות ההסכם, ויישום אמצעי האבטחה כאמור בנוהל זה ;
98. מומלץ למנות ממונה/ אחראי אבטחת מדע אצל הגורם החיצוני שיהווה גורם אחראי/ אישר קשר לצורך מתן השירותים וקיום הפעילות בין הצדדים, ולאפשר פיקוח הצד העירייה, בהתאם לרגישות המידע המועבר במסגרת ההתקשרות ;
99. איסור העברת המידע לצד שלישי כלשהו ו/או שימוש במידע אליו נחשף הגורם החיצוני אגב ההתקשות, לכל מטרה שאינה קשורה במישרין לביצוע התקשרות ;
100. איסור מפורש על איסוף מידע בדרכים בלתי-חוקיות ו/או עשיית שימוש במאגרי מידע בלתי-חוקיים ;
101. נספח הגדרות אבטחה שיהיה חלק בלתי נפרד מתאני ההתקשרות עם הגורם החיצוני ויכלול, בין היתר, הוראות לגבי אבטחה פיסית ולוגית, ופרדת מאגרי מידע, מתן הראשות עריכת רישום מעורכן של מורשי הגישה למידע, הוראות תפעול, סודיות, בקרה, דרך קבלת עובדים וכיו"ב ;

102. 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 המופרטים בסעיף זה לעיל ולהלן;

103. 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;

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

105. 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, אם 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.

106. 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.

107. ההבחנה בין סוג פעילות מיקור חוץ אחד למשנהו, מושתתת על היקף הרשאות הגישה הניתנות לגרם 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 המאבחת 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 (כמוגן 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 החבר לבחון את אופן ומשך הזמן בו יש לגורם החיצוני גישה למידע או יכולת לשמור עליו, כדי שיהא ניתן לקבוע את מעמדו במאגר, בשאת 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 חלפה 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.

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

109. על מנמ"ר/מנכ"ל העירייה /או מי שהוסמך על-ידם לצורך כל 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 /או מי שהוסמך על-ידם לצורך כך ליישם, בין היתר, את הבקורות הבאות, ככל שרלוונטיות לעניין וכמפורט להלן.

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

111. 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.

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

113. 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, וזת כדי לבחון, בין היתר, האם הועברו דלפו פרטי מידע שלא לצורך ביצוע פעילות מיקור החוץ כאמור.

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

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

115. 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. 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.

116. 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.

117. 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 המערכת, באופן בו תהא אבחנה והפרדה ברורה בין הפעילות המבוצעת עבור העירייה לבין פעילות המבצעת עבור גופים אחרים ו/או עבור הגורם החיצוני עצמו.

### **שימוש באינטרנט ודואר אלקטרוני**

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

- השולח אינו מוכר
- רשימת התפוצה לא רלוונטית לפעילות
- שם הקובץ אקראי ולא קשור לפעילות
- תוכן ההודעה חשוד ומזמין לפתוח הקובץ או הקישור
- הקישור מוביל לכתובת בחו"ל

119. לא ניתן יהיה לשלוח קבץ מעל MB3.

## חוקי FIREWALL

120. כל בקשה להוספה, שינוי או ביטול של חוק FIREWALL תגובה בבקשה כתובתה ע"י מנהל מחלקה, תוך הצורך לבקשה. אישור הבקשה יתבצע ע"י יחידת המחשוב ויועבר לביצוע ספק מיקור החוץ.
121. חוקי ה-FIREWALL יגובו אחת לחודש.
122. חוקי ה-FIREWALL יתועדו במסמך ויסקרו אחת לרבעון.

## הגדרת סיכונים

123. 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 מדווח נפסח ב' לנוחל זה. אינם מצורפים מפאת נימוקי אבטחת מידע (מסווג).**

## סיכונים טכנולוגיים:

124. פגיעה בזמינות מאגרי המידע ובמערכות המשמשות למאגרי המידע כתוצאה מפגיעה מלאה או חלקית בהן.
125. פגיעה בשרידות מאגרי המידע והמערכות המשמשות למאגרי המידע בשל כשל טכני או נזק.
126. חדירה למאגרי המידע וחשיפות מידע.
127. פגיעה בפרטיות של נושאי המידע שפרטיהם מצויים במאגרי המידע של העירייה כתוצאה מדלף מידע לגורמים לא מורשם וכן מאי עמידה בחוק הגנת הפרטיות והתקנות הנלוות אליו.
128. אובדן מידע בשל העדר גיבוי.
129. עקיפת הרשאות בשל היעדר בקורות ברמה טכנולוגית.
130. ספקים חיצוניים בעלי יכולת גישה מרחוק למאגרי המידע של העירייה.

## סיכונים ארגוניים ואנושיים

131. פעילות שגויה של משתמשים בשל חוסר מודעות לאבטחת מידע.
132. גישת גורמים לא מורשם ופגיעה במאגרי המידע ובמערכות הנלוות להם.



133. חוסר התאמה בין מצבת כוח האדם בפועל למצבת כוח האדם במאגרי המידע ובמערכות בעירייה.
134. העברת קבצים ומסמכים באופן לא מאובטח ו/או לגורמים לא מוסמכים.
135. נזקים פיזיים למאגרי המידע ולציוד חומרה ותקשורת העירייה.
136. אובדן או גניבת ציוד מחשוב נייד ונייח ומסמכים המכילים מידע רגיש.

### אירוע אבטחת מידע

137. מנהל יחידת המחשוב אחרי להגדרת איתור, מעקב, ניטור ובקרה,
- מקרה בו התגלה אירוע המעלה חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לריגה מהרשאה ו/או הסכמים, במערכות שמתופעלות על ידי העירייה (להלן: "אירועי אבטחה").
138. ספקים אשר מחזיקים/מנהלים מאגרי מידע ומערכות מאגרי מידע, אחראים לאירועי אבטחת מידע במערכות המאגרים שרשותם, לגבי מידע ושירותים של העירייה ולתיעוד האירועים.
139. 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.
140. ניתן לאבחן ולזהות אירועי אבטחה במספר דרכים:
- ניצול לרעה של סמכויות עובדים לצורך עדכון/שיבוש מידע ותהליכים;
  - משתמש המבחין באי סגרים ו/או תהליכים לא תקינים ו/או חריגה מנהלי העבודה ו/או אירועים חשודים בסביבת העבודה שלו (כף למשל-הפרה של נוהלי אבטחת מידע על ידי העובד או על ידי עובדים אחרים; 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) להגשת גישה לא מאושרת למערכת או המידע האגור בה; חוסר זמינות בשרות וכיו"ב;
  - כלים/מנגנונים ייעודיים ואוטומטיים לאבחון והתראה, כגון קבצי לוג וכיו"ב;
  - הודעות/עדכונים מגופי חיצוניים דוגמה: תוכנות אנטי וירוס, מערכות וכיו"ב;
  - במאגרי מידע בעלי רמת אבטחת בינונית, יקיים מנהל יחידת המחשוב דיון לעניין אירועי האבטחה, אחת לשנה לפחות ויבחן את הצורך בעדכונו של נוהל זה.

- במאגרי מידע בעלי רמת אבטחת בינונית, יקיים מנהל יחידות המשוב דיון לעניין אירועי האבטחה, אחת לשנה לפחות ויבחן את הצורך בעדכונו של נוהל זה.
- 141. במאגרי מידע בעלי רמת אבטחה גבוהה, יקיים מנהל יחידות המשוב דיון לעניין אירועי האבטחה, אחת לרבעון לפחות ויבחן את הצורך בעדכונו של הנוהל זה.
- 142. מנהל יחידת המשוב ידווח, באופן מיידי, למנמ"ר/מנכ"ל העירייה ו/או מי שהוסמך על-ידם לצורך כך בקרות אירוע אבטחה חמור (כהגדרתו בתקנה 1 לתקנת אבטחת מידע) וכן ידווח להם על הצעדים שנקט בעקבות האירוע.
- 143. 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 שנקטו עקבות האירוע.
- 144. מנהל יחידת המשוב והספקים ישמרו תיעוד של אירועי האבטחה והנתונים שיצברו בהתאם לסעיף זה באופן מאובטח למשך 24 חודשים, לכל הפחות.

#### הוראות לגבי התמודדות על אירועי אבטחת מידע

- 145. מנהל המאגר יכלול במסגרת הדרכות והמודעות לעובדים, הנחיה לגבי חשיבות הזיהוי והדיווח על אירועים חשודים וחשיבות מהירות הדיווח למנהל יחידת המשוב ולמנהל המאגר.
- 146. מנהל יחידת המשוב יחייב בכתב מכל ספק, אשר קיימת לו נגישות למערכות המחשבים ולמידע רגיש של העירייה, התחייבות לפיה כל אירוע אבטחת מידע במערכות המשוב שלהם, אשר נוגעות למערכות המשוב של העירייה או למידע של העירייה, ידווח גם למנהל יחידת המשוב של העירייה.
- 147. אירוע שזוהה ואושר כאירוע אבטחת מידע על ידי מנהל יחידת המשוב, 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 והאחרים.
- 148. מנהל יחידות המשוב יקבע את דרגת חומרת האירוע לפי גודל הנזק :

- מקומית- אירוע הגורם לנזק מקומי כהפרה מועטה של פעילות ואינו מסוגל להתפשט למערכות אחרות (הדבקות בוירוס של מחשב בודד, אירועים מסוג זה יטופל מקומית ע"י מנהל יחידת המשוב).
- בינונית-אירוע הגורם לפגיעה מקומית, אך חמורה ומשמעותית בפעילות העירייה וביכולת ניהול הפעילות (השבתת הרשת המקומית כתוצאה ממתקפת CYBER).

148. 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).

149. מנהל יחידת המחשב ינתח ויטפל באירוע בהתאם לסוג האירוע כדלהלן:

- 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).
- התקפות מניעת שירות (Denial Service) – ניתוח האירוע יכלול את זיהוי הגורם המותקף (נתב חיצוני/פנימי, תחנה, רכיב אחר) ומיפוי דרכי הגישה אליו, ניתוח תעבורה ברשת (sniffer) והתחקות אחר כתובת המתקיף.
- השתלטות על מערכות אישומים – ניתוח האירוע יכלול סריקת המערכת הפגועה ומערכות משיקות כדי לזהות את סוג החדירה ולהעריך את המק שנגרם. בדיקות טלאים חסרים העלולים לשמש לחדירה, שינויים בקבצי מערכת ההפעלה ובקוד, קבצים ששוננו לאחרונה, משתמשים שנוספו לאחרונה ועוד.
- באירועים קריטיים או באירועים כמו פריצה או השתלטות על אפליקציות ומערכות תפעול בעירייה או אצל ספק חיצוני, מנהל יחידת המחשוב או ספק, לפני העניין, יהיה אחראי לבודד את האזור הנוגע. 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.
- מנהל יחידת המחשב או הספק, לפי העניין, אחראי לסקור מערכות שכנות המתמשקות למערכת הפגועה (למשל גיבוי) על מנת לוודא כי אין צורך לבודד גם אותן.
- מנהל יחידת המחשוב יודיע לממונה אבטחת המידע על המקרה ועל צעדי הבידוד שבוצעו. מנהל יחידת המחשוב יוציא הודעה בהתאם למשתמשים ולבעלי התפקידים הרלוונטיים.
- עדכון גורמים עסקיים – במקרה של דליפת מידע רגיש או השתלטות על מערכות, ממונה אבטחת המידע ינקוט בצעדי מניע עסקיים וואו יודיע לגורמים המתאימים, על מנת להקטין את נזק דליפת המידע או שינוי הנתונים.

- לפני שנשקלת החזרת המערכות לתפקוד מלא, מנהל יחידת המחשוב יודא 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.
- במדיה והאירוע חייב מחיקת מידע/פרמוט שרתים וכו', מנהל יחידת המחשוב יודא ביצוע התקנה מחדש של כל הקבצים המעורבים, תכנות האפליקציה, התשתית, המשתמשים והקונפיגורציה הקשורים לאירוע, התקנה מחדש של מערכת ההפעלה וכל הטלאים (patches) שפורסמו עברה. הפעלה מרבי של אמצעי הניטור הקיימים בתחנה ובמערכת ובמידת הצורך שחזור נתונים מגיבוי, ולעיתים גם להשלים מידע שאבד.

### **בדיקות לפני חזרה לפעילות:**

150. 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.
151. מנהל יחידת המחשוב או הספק, לפי העניין, יבצע בדיקה למערכות מבחינה פונקציונלית.
152. במקרה האירוע גרם לשינוי נהלים, ממונה אבטחת מידע יתדרך את כל הנוגעים בדבר, ויודא שהתהליכים החדשים מוכנים ליישום.

### **אבטחת תקשורת**

153. 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.
154. העברת מידע ממאגר מידע, ברשת ציבורית או באינטרנט, תעשה תוך שימוש בשיטות הצפנה מקובלות.
155. במאגר מידע שניתן לגשת אליו מרחוק, באמצעות רשת האינטרנט או רשת ציבורית אחרת, מנהל יחידת המחשוב ייעשה מימוש באמצעים שמטרתם לזהות את המתקשר והמאמתים או הרשאתו לביצוע הפעילות מרחוק ואת היקפה, וזאת בנוסף לשימוש באמצעי אבטחה לעיל.
156. ספקים אשר מחזיקים/ מנהלים מאגרי מידע ומערכות מאגרי מידע, אחראים לאבטחת התקשורת במערכות המאגרים שברשות

### ביקורות תקופתיות

158. מטרת הביקורות התקופתיות הינה הבטחת התנהלות ביחס למערכותיה ומאגרי המידע שלה, והכל בהתאם להוראות נוהל זה ותקנות האבטחה.

159. 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.

160. במסגרת הביקורת התקופתית ייבחנו, בין היתר, הנושאים הבאים:

- \*עמידת העירייה בהוראות נוהל זה ותקנות האבטחה
- \*קיום ביקורות תקופתיות נדרשות;
- \*התאמת אמצעי האבטחה של העירייה לנוהל זה ולתקנות האבטחה, וזיהוי ליקויים ככל שישנם.

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

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

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

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

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