‏ט"ו בטבת תש"פ

‏12 בינואר 2020

מחלקת מערכות מידע

נוהל אבטחת מידע בעירייה

נוהל אבטחת מידע בעירייה

1. **כללי**
   1. חוק הגנת הפרטיות, התשמ"א-1981 (להלן: "החוק" או "חוק הגנת הפרטיות")، קובע הוראות שונות וחובות המוטלות על בעל מאגר מידע, מחזיק במאגר מידע ומנהל מאגר מידע. אחת החובות המרכזיות היא חובת אבטחת המידע, שמטרתה צמצום החשש מפני שימוש לרעה או פגיעה בשלמות המידע.
   2. תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "תקנות אבטחת מידע"), קובעות עקרונות אבטחת מידע הקשורים בניהול ובשימוש במידע במאגרי המידע, בהתבסס על תקני אבטחת מידע המקובלים בכל העולם.
   3. אבטחת מידע ברשת ובמערכות העירייה, לרבות מערכות הנמצאות ברשת ספק מיקור חוץ, הינה חיונית להגנת המידע של העירייה, תושביה ועובדיה.
   4. לאור זאת, על העירייה להתקין ולהטמיע מערכות הגנה מפני איומים וחיצוניים ופנימיים וליישם בקרות ניהוליות וטכנולוגיות לאכיפת רמת אבטחת מידע ואבטחה פיזית על תשתיות המידע.
2. **מטרת הנוהל**
   1. הגדרת כללי אבטחת המידע המחייבים את העירייה עובדיה וספקיה.
   2. התאמת פעילות העירייה להוראות חוק הגנת הפרטיות, התשמ"א-1981, לתקנות שהותקנו מכוח החוק ובפרט לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.
   3. מימוש תכליות החוק והגנה על זכויות נושאי המידע במאגרי המידע, מפני שימוש לרעה במידע אודותיהם, הן ע"י גורמים מחוץ לארגון והן ע"י העובדים.
   4. הגדרת פעולות ובקרות הנדרשות לעמידה בדרישות החוק ותקנות אבטחת מידע.
3. **הגדרות**
   1. אנטי וירוס - תוכנה המגינה על מחשבים מפני תוכנות זדוניות ופריטי דוא"ל ואתרי אינטרנט המכילים תוכנות אלו.
   2. עדכון במערכת הפעלה -חברת Microsoft מפרסמת מדי פעם עדכונים למערכת ההפעלה החדשה ביותר שלה. עדכונים אלה קרויים גם Service Packsאו מהדורות מעודכנות המכילות שיפורים חשובים במערכות ההפעלה כמו למשל, תוכנות אבטחה מעודכנות, כלים עדכניים ושינויים במוצר על פי בקשת הלקוחות
   3. משתמש – אדם הפועל ברשת המחשוב של עיריית מעלות תרשיחא.
   4. בעל הרשאה – כהגדרתו בתקנה 1 לתקנות הגנת הפרטיות (אבטחת המידע), התשע"ז-2017.
   5. 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.
   6. מחזיק מאגר מידע- ספק שמנהל/מחזיק מערכת למאגר מידע דרך קבע והוא רשאי לעשות בו שימוש.
   7. ממונה אבטחת מידע - בעירייה הוחלט כי \_\_\_ מוגדר ממונה אבטחת מידע.
   8. אירוע אבטחת מידע- אירוע אבטחת מידע הינו אירוע מכל סוג, אשר פוגע, או עלול לפגוע בסודיות, שלמות וזמינות המידע ברשת המחשוב של העירייה, ו/או לפגוע, לשבש או לקטוע תהליכי עבודה תקינים בעירייה, כגון:
      1. חשיפה בלתי מורשית של מידע רגיש ממערכות המידע של העירייה.
      2. התקפות מניעת שירות על מערכות העירייה (Denial Of Service).
      3. פריצה למערכות המידע בעירייה (ע"י תוקף חיצוני או פנימי).
      4. פגיעת וירוס בתשתיות המחשוב של העירייה.
      5. שינוי פני אתרים ואפליקציות (Defacement).
      6. מעילה, שימוש לא מורשה בהרשאות במערכת מידע.
      7. השחתה או גניבת ציוד מחשבים במשרדי העירייה.
      8. שימוש במערכות מידע לפעילות לא חוקית (גניבת תוצרת גמורה, מלאי בתהליך, וכו').
4. **חלות הנוהל ואחריות**
   1. האחריות ליישום הנוהל חלה על המנמ"ר.
   2. בקרת יישום הנוהל ועדכונו חלה על היועץ המשפטי\מבקרת פנים.
5. **שיטה**
   1. אזורים מאובטחים
      1. המנמ"ר יגדיר אזורים אשר יוגדרו כ-"אזורים רגישים מבחינה טכנולוגית", יגדיר מיהם בעלי תפקידים המורשים להיכנס לשם, ויאשרר מול אחראי המחשוב בעירייה את הרשימה אחת לשנה.
      2. מנמ"ר וקב"ט העירייה יישמו אמצעי אבטחה פיזיים על מתחמים אלו.
      3. קב"ט העירייה יישם אמצעי מיגון פיזיים להגנה על ארונות התקשורת תוך הקפדה על הצבתם באזורים מאובטחים בבניין.
      4. חדרי שרתים וארונות תקשורת יינעלו על ידי מורשי הגישה לאזורים אלו, כך שיהיו מחוץ להישג ידם של גורמים שאינם מורשים.
      5. המנמ"ר ינקוט אמצעים לבקרה ולתיעוד של הכניסה והיציאה מאתרים בהן מצויות מערכות המאגר, וכן יקיים תיעוד של הכנסה והוצאת ציוד אל מערכות מאגרי המידע ומהן. המנמ"ר ישמור נתונים אלה באופן מאובטח למשך 24 חודשים, לכל הפחות.
      6. גריסת מסמכים מתבצעת אחת לשבוע, באמצעות ספק חיצוני.
      7. 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.
   2. אבטחת סביבת העבודה והמחשבים
      1. בעת עזיבת סביבת העבודה, עובדי העירייה יאחסנו מידע רגיש באופן מאובטח, במתקן נעול (מגירה, ארון או כספת, בהתאם למידת הרגישות והאמצעים הזמינים), במידה ואין, יש לנעול את החדר.
      2. בתום יום העבודה או בעת עזיבת מקום העבודה לזמן ארוך על המשתמשים להותיר את סביבת העבודה כשמסמכי החברה מתויקים או מסודרים במקומם הראוי.
      3. מנמ"ר העירייה יגדיר נעילת מסך עם סיסמה לאחר 30 דקות ללא פעילות בכל תחנות הקצה.
      4. בכל שרת ותחנת עבודה יתקין מנמ"ר העירייה תוכנת אנטי וירוס ויגדיר תהליך יומי לעדכונו.
      5. בכל שרת תחנת עבודה יגדיר מנמ"ר העירייה תהליך לעדכון מערכת ההפעלה בעדכוני אבטחת מידע והתקנת חבילת שירות של היצרן.
      6. עובדי העירייה יאשרו שימוש ברכיבי DOK או בכונן CD מול מנהלים ברמת מנהל מחלקה ומעלה-לבדוק ישימות.
      7. 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 המנמ"ר או מי שהוגדר מטעמו או על ידי ספקים מורשים באישורו ותוך תיעוד הפעילות.
      8. התקשורת עם ספקים מתבצעת בתווך מוצפן.
      9. הספקים אחראים לאבטחת סביבת העבודה והמחשבים שברשותם.
   3. מדיניות הרשאות
      1. ניהול ההרשאות במחשבי העירייה ייעשה ע"י מנמ"ר העירייה באמצעות מנגנון ממוכן לניהול הרשאות (AD למשל) (להלן: "מנגנון הבקרה").
      2. מנגנון הבקרה מנוהל על ידי המנמ"ר 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.
      3. המנמ"ר יגדיר כי רק לאנשי המחשוב תהיה גישה לניהול ההרשאות ולקבציי הלוגים של מנגנון הבקרה. כמו כן, מנגנון הבקרה יאתר שינויים או ביטולים בהפעלתו ויפיץ התראות למנכ"ל העירייה, למנהל המאגר, למנמ"ר, לממונה אבטחת המידע וליועץ אבטחת מידע וסייבר.
      4. המנמ"ר יקבע נוהל בדיקה שגרתי לנתוני התיעוד של מנגנון הבקרה ויערוך דו"ח של הבעיות שהתגלו והצעדים שננקטו.
      5. המנמ"ר ישמור את נתוני התיעוד של מנגנון הבקרה באופן מאובטח למשך 24 חודשים, לכל הפחות.
      6. המנמ"ר ו/או מנהל המאגר יידע את בעלי ההרשאות במאגר בדבר קיום מנגנון הבקרה למערכות המאגר.
      7. ספקים אשר מחזיקים/מנהלים מאגרי מידע ומערכות מאגרי מידע, אחראים לקיום מנגנון בקרה במאגרים ובמערכות שברשותם.
      8. המנמ"ר יוודא כי חשבון משתמש בגישה למחשבי העירייה ולמערכות העירייה ישויך לעובד מסוים ותוגדר אחריות של העובד על החשבון והפעולות המתבצעות בו.
      9. מנמ"ר העירייה יגדיר הרשאות בגישה למחשבי העירייה ולקבצים ומערכות ברשת העירייה בהתאם לתפקידם ולצורך ביצוע תפקידם בלבד.
      10. במערכות המתופעלות על ידי ספקים, מנמ"ר העירייה יעביר בקשות לספקים הרלוונטיים לפתיחה/מחיקה של הרשאות.
      11. במערכות המתופעלות על ידי ספקים, הספק ינהל ההרשאות בנפרד מלקוחות אחרים של אותו הספק.
      12. מנמ"ר העירייה ייבחן את הרשאות הניהול במערכות, אחת לשישה חודשים ואחת לשנה את שאר ההרשאות לכלל המערכות. **רשימת הרשאות תקפות מצורפת כנספח א' לנוהל זה.**
      13. מנמ"ר העירייה יגדיר את אופן נעילת חשבון במקרה של אי שימוש ואת תהליך שחרור הנעילה.
      14. הקפאת הרשאת משתמש:
          1. בכל מקרה בו ידוע על הפסקת העבודה של משתמש המוגדר במערכת לתקופה העולה על 30 יום (עקב מילואים, חופשה, מחלה), המנמ"ר ינעל את חשבון המשתמש של העובד אל מחשבי העירייה. במקרה של חופשת לידה החשבון יישאר זמין, בנוסף, המנמ"ר יעדכן את הספקים הרלוונטיים על מנת לנעול חשבונות למערכות.
          2. מנמ"ר העירייה יוודא הקפאת ההרשאות של המשתמש עד ליום שובו לעבודה.
          3. יש ליצור ממשק עבודה מחייב מול משאבי אנוש לסנכרון הוספת\הקפאת עובדים.
      15. סגירת/ביטול הרשאות משתמש
          1. כאשר סיים עובד בעל הרשאה את עבודתו בעירייה, המנמ"ר יסגור את הרשאתו למחשבי העירייה לצמיתות. בנוסף, המנמ"ר יוודא כי ספקי התוכנה הרלוונטיים סוגרים את הרשאות העובד במערכות שבהם יש לו חשבון משתמש.
          2. לצורך שמירה על רצף שירותי מידע, ייבחן הצורך לשמור או להעביר ספריות מההרשאה המיועדת לסגירה אל הרשאותיו של משתמש אחר.
   4. שימוש בשם משתמש וסיסמאות
      1. שם המשתמש (User ID/Username) מיועד לשימוש אישי בלבד.
      2. מנמ"ר העירייה וספקים לא יבצעו הגדרת משתמשים גנריים לפעילות משתמשים אנושיים, אלא עבור שרתים ויישומים בלבד, תוך תיעוד בקבץ ייעודי.
      3. מדיניות הסיסמאות ברשת (AD) , תחנות הקצה והשרתים תוגדר על ידי המנמ"ר כדלהלן:
         1. על הסיסמא להיות שונה מחשבון המשתמש ושמו הפרטי.
         2. אורך הסיסמא יהיה 7 תווים לפחות.
         3. סיסמא תכיל לפחות אות אחת, וסיפרה אחת.
         4. הסיסמא לא תתבסס באופן קל לניחוש על שם המשתמש.
         5. הסיסמה תוחלף אחת ל-180 יום.
         6. אין לחזור על אותה הסיסמא במשך 10 מחזורי החלפה.
         7. מנמ"ר העירייה יגדיר נעילת משתמש לאחר 5 ניסיונות זיהוי כושלים, שחרור הנעילה יהיה לאחר 5 דקות/ע"י המנמ"ר
   5. אבטחת מידע בניהול כוח אדם
      1. 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.
      2. 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.
      3. 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.
      4. מנהל המאגר ידאג לקיים, אחת לשנתיים לפחות, 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.
      5. ספקים אשר מחזיקים/מנהלים מאגרי מידע ומערכות מאגרי מידע, אחראים למתן הרשאות גישה וקיום הדרכות לעובדיהם.
   6. שמירת מידע
      1. שמירת מידע במדיית אחסון נתיקה יתבצע ע"י מורשים לכך ע"י המנמ"ר, כאשר המידע יימחק עם הסיום בשימוש בו.
      2. על המשתמשים להימנע מאחסון מידע על גבי הכוננים הקשיחים המקומיים (D:,C:). מידע השמור מקומית על גבי מחשבים אישיים אינו מגובה, ומאובטח פחות מאשר כונני הרשת שמירת מסמכים תעשה על כונני הרשת בלבד (O:,N:,T:,Z:)
      3. ניתן לשמור מידע פרטי על כונן מקומי D:, C: שאינו מגובה.
   7. גיבויים
      1. מנמ"ר העירייה או ממונה מטעמו, יבצעו גיבויים לכל השרתים ברמה יומית לאמצעי אחסון נתיק, אשר יישמרו באמצעי חסין אש.
      2. כל בוקר יתעד המנמ"ר את תוצאות תהליך הגיבוי בקבץ ייעודי.
      3. קלטות הגיבוי יועברו על ידי המנמ"ר אחת ליום לאתר חיצוני (ניתן במבנה אחר של העירייה האזורית).
      4. המנמ"ר ישמור את הגיבויים למשך 24 חודשים, לכל הפחות.
   8. שימוש באינטרנט ודואר אלקטרוני
      1. המנמ"ר ינחה משתמשים שלא לפתוח קבצים המקושרים להודעות דואל או קישורים מתוך הודעות, במידה ומתרחש אחד מן הבאים:
         1. השולח אינו מוכר
         2. רשימת התפוצה לא רלוונטית לפעילות
         3. שם הקובץ אקראי ולא קשור לפעילות
         4. תוכן ההודעה חשוד ומזמין לפתוח הקובץ או הקישור
         5. הקישור מוביל לאתרים מפוקפקים
   9. בקרה
      1. מנמ"ר העירייה ייזום תהליך בקרה להרשאות המשתמשים בכלל המערכות לרבות לתיקיות בשרת הקבצים ולמערכות המנוהלות על ידי ספקים, אחת לשנה ויוודא מחיקה של חשבונות והרשאות שאינם רלוונטיות.
      2. היועץ המשפטי יוודא כי התייחסות להיבטי אבטחת מידע כלולה בכל מכרז למערכת מידע שמפרסמת העירייה.
   10. הגדרת סיכונים
       1. בסעיף זה מוגדרים הסיכונים להם חשוף המידע שבמאגר במסגרת הפעילות השוטפת של העירייה, לרבות אלה הנובעים ממבנה מערכות המאגר. **מצ"ב מבנה מאגרי המידע ורשימה מעודכנת של מערכות המאגר כנספח ב' לנוהל זה.**
       2. סיכונים טכנולוגיים:
          1. פגיעה בזמינות מאגרי המידע ובמערכות המשמשות למאגרי המידע כתוצאה מפגיעה מלאה או חלקית בהן.
          2. פגיעה בשרידות מאגרי המידע והמערכות המשמשות למאגרי המידע בשל כשל טכני או נזק.
          3. חדירה למאגרי המידע וחשיפת מידע.
          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. אובדן מידע בשל העדר גיבוי.
          6. עקיפת הרשאות בשל היעדר בקרות ברמה טכנולוגית.
          7. ספקים חיצוניים בעלי יכולת גישה מרחוק למאגרי המידע של העירייה.
       3. סיכונים ארגוניים ואנושיים:
          1. פעילות שגויה של משתמשים בשל חוסר מודעות לאבטחת מידע.
          2. גישת גורמים לא מורשים ופגיעה במאגרי המידע ובמערכות הנלוות להם.
          3. חוסר התאמה בין מצבת כוח האדם בפועל למצבת כוח האדם במאגרי המידע ובמערכות.
          4. העברת קבצים ומסמכים באופן לא מאובטח ו/או לגורמים לא מוסמכים.
          5. נזקים פיזיים למאגרי המידע ולציוד חומרה ותקשורת.
          6. אובדן או גניבת ציוד מחשוב נייד ונייח ומסמכים המכילים מידע רגיש.
   11. אירועי אבטחת מידע
       1. המנמ"ר אחראי לתיעוד כל מקרה בו התגלה אירוע המעלה חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה, במערכות שמתופעלות על ידי העירייה (להלן : "אירועי אבטחה").
       2. ספקים אשר מחזיקים/מנהלים מאגרי מידע ומערכות מאגרי מידע, אחראים לאירועי אבטחת מידע במערכות המאגרים שברשותם, לגבי מידע ושירותים של העירייה ולתיעוד האירועים.
       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.
       4. במאגרי מידע בעלי רמת אבטחת בינונית, יקיים המנמ"ר דיון לעניין אירועי האבטחה, אחת לשנה לפחות ויבחן את הצורך בעדכונו של נוהל זה.
       5. במאגרי מידע בעלי רמת אבטחה גבוהה, , יקיים המנמ"ר דיון לעניין אירועי האבטחה, אחת לרבעון לפחות ויבחן את הצורך בעדכונו של נוהל זה.
       6. המנמ"ר ידווח, באופן מיידי, ליועץ המשפטי של העירייה בקרות אירוע אבטחה חמור וכן ידווח לו על הצעדים שנקט בעקבות האירוע. היועץ המשפטי של העירייה ידווח לרשם באופן מיידי בקרות אירוע אבטחת מידע חמור וכן ידווח לו על הצעדים שננקטו בעקבות האירוע.
       7. המנמ"ר והספקים ישמרו תיעוד של אירועי האבטחה והנתונים שיצברו בהתאם לסעיף זה באופן מאובטח למשך 24 חודשים, לכל הפחות.
   12. הוראות לגבי התמודדות עם אירועי אבטחת מידע
       1. מנהל המאגר יכלול במסגרת הדרכות המודעות לעובדים, הנחיה לגבי חשיבות הזיהוי והדיווח על אירועים חשודים וחשיבות מהירות הדיווח למנמ"ר ולמנהל המאגר.
       2. המנמ"ר יבקש 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 למנמ"ר העירייה.
       3. אירוע שזוהה ואושר כאירוע אבטחת מידע על ידי המנמ"ר, יעבור תהליך סיווג על ידי המנמ"ר, 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.
       4. המנמ"ר יקבע את דרגת חומרת האירוע לפי גודל הנזק:
          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 המנמ"ר).
          2. בינונית – אירוע הגורם לפגיעה מקומית, אך חמורה ומשמעותית בפעילות החברה וביכולת ניהול הפעילות (השבתת הרשת המקומית כתוצאה ממתקפת CYBER).
          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 בעירייה. (וירוס במערכות התפעול, גניבת נתונים של עובדי העירייה).
       5. המנמ"ר ינתח ויטפל באירוע בהתאם לסוג האירוע כדלהלן:
          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).
          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.
          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.
       6. באירועים קריטיים או באירועים כמו פריצה או השתלטות על אפליקציות ומערכות תפעול בעירייה או אצל ספק חיצוני, המנמ"ר 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.
       7. המנמ"ר או הספק, לפני העניין, אחראי לסקור מערכות שכנות המתממשקות למערכת הפגועה (למשל גיבוי) על מנת לוודא כי אין צורך לבודד גם אותן.
       8. המנמ"ר יודיע לממונה אבטחת המידע על המקרה ועל צעדי הבידוד שבוצעו. המנמ"ר יוציא הודעה בהתאם למשתמשים ולבעלי התפקידים הרלוונטיים.
       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.
       10. לפני שנשקלת החזרת המערכות לתפקוד מלא, המנמ"ר 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.
       11. במידה והאירוע חייב מחיקת מידע/ פרמוט שרתים וכו', המנמ"ר 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.
       12. בדיקות לפני חזרה לפעילות:
           1. המנמ"ר או הספק, לפי העניין, יבצע בדיקה למערכות לאחר השחזור כדי לוודא כי אינן מכילות פרצות אבטחה ו/או פגיעות אחרות והאירוע אכן הסתיים.
           2. המנמ"ר או הספק, לפי העניין, יבצע בדיקה למערכות מבחינה פונקציונלית.
           3. במקרה והאירוע גרם לשינוי נהלים או תהליכים, ממונה אבטחת מידע יתדרך את כל הנוגעים בדבר, ויוודא שהתהליכים החדשים מוכנים ליישום.
           4. ממונה אבטחת מידע יוודא בדיקת כל המערכות המתממשקות למערכת הפגועה כדי לוודא כי לא נפגעו.
       13. העלאת המערכות, ממונה אבטחת מידע וסייבר יוודא :
           1. העלאת המערכות השונות, פתיחת הגישה לאפליקציות שנחסמו וכו'.
           2. העלאת השירותים אשר הורדו (מייל/ אינטרנט וכו') – בצורה הדרגתית ובניטור הפעילות.
           3. הודעה לכל המשתמשים והמעורבים בנושא על חזרה לפעילות שוטפת.
           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.
       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:
           1. מימוש נוהל זה, בחינה אם נדרש שיפור בתהליך התגובה המוגדר למעלה.
           2. האם נדרש שיפור במנגנוני הניטור ואיתור האירועים.
           3. כלים שעשויים לעזור בתהליך התגובה לאירועים, כמו שדרוג תכנת נתבים, התקנת firewalls פנימיים, שינוי כתובות IP, גישה למידע רגיש בשימוש באפליקציה ייעודית, וכדומה.
           4. שיפורים לעמידות העירייה לאירועים כאלה.
           5. שיפורים לתהליך ההתאוששות מאירועים אלו.
           6. תהליכי תקשורת בין הגורמים שטיפלו באירוע.
           7. מוכנות של המנמ"ר והספקים השונים לאירועים אלו.
       15. ממונה אבטחת מידע יוודא אחת לשנה כי הספקים מבצעים בחינה של חוקי הניטור שהוגדרו ותקינותם ואיכות האירועים שמתקבלים.
   13. ניהול מאובטח ומעודכן של מערכות המאגר
       1. המנמ"ר "ר יקפיד על ניהול ותפעול תקין של מערכות המאגר, לפי המקובל בהפעלות מערכות אלה.
       2. המנמ"ר יפריד, בהיקף ובמידה הסבירים האפשריים, בין מערכות המאגר אשר ניתן לגשת מהן למידע, לבין מערכות מחשוב אחרות המשמשות את העירייה.
       3. המנמ"ר 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.
       4. ספקים אשר מחזיקים/מנהלים מאגרי מידע ומערכות מאגרי מידע, אחראים לניהול מאובטח ומעודכן של מערכות המאגרים שברשותם.
   14. אבטחת תקשורת
       1. המנמ"ר 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.
       2. העברת מידע ממאגר מידע, ברשת ציבורית או באינטרנט, תיעשה תוך שימוש בשיטות הצפנה מקובלות.
       3. במאגר מידע שניתן לגשת אליו מרחוק, באמצעות רשת האינטרנט או רשת ציבורית אחרת, המנמ"ר ייעשה שימוש באמצעים שמטרתם לזהות את המתקשר והמאמתים את הרשאתו לביצוע הפעילות מרחוק ואת היקפה, וזאת בנוסף לשימוש באמצעי אבטחה לעיל.
       4. ספקים אשר מחזיקים/מנהלים מאגרי מידע ומערכות מאגרי מידע, אחראים לאבטחת התקשורת במערכות המאגרים שברשותם.
       5. תווך תקשורת מול ספקים מוצפן.
   15. ביקורות תקופתיות
       1. 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, במטרה לוודא עמידתה של העירייה בתקנות אבטחת מידע.
       2. המבקר ידווח בדו"ח הביקורת על התאמת אמצעי האבטחה לנוהל זה ולתקנות אבטחת המידע, יזהה ליקויים ויציע אמצעים הדרושים לתיקון המצב.
       3. מנכ"ל העירייה בשיתוף מבקר הפנים, ידון בדוחות הביקורת שיועברו לו ויבחן את הצורך בעדכון מסמך הגדרות המאגר או נוהל זה.
       4. העירייה תהיה רשאית לקיים ביקורת אחת לעניין כל מאגרי המידע שברשותה, המצויים באותה רמת אבטחת מידע ולהסתמך על בקורת שיבצעו מחזיקי מאגרים.
       5. מנכ"ל העירייה ישמור את דוחות הביקורת באופן מאובטח למשך 24 חודשים, לכל הפחות.
       6. המנמ"ר בשיתוף עם מבקר הפנים, יקבע נוהל לביצוע גיבויים לדוחות הביקורת, באופן תקופתי שגרתי.
   16. בקרה
       1. המנמ"ר יבחן, אחת לשנה, את הצורך בעדכון הנוהל.
       2. כמו כן, המנמ"ר יבחן את הצורך בעדכון הנוהל במקרים הבאים:
          1. בעת שינויים מהותיים במערכות המאגרים או בתהליכי עיבוד מידע.
          2. בעת סיכונים טכנולוגיים חדשים הנוגעים למערכות המאגר.

**נספח א' – רשימת הרשאות תקפות**

**נספח ב' - מבנה מאגרי המידע ורשימה מעודכנת של מערכות המאגר**