שם הנוהל: נוהל מדיניות אבטחת מידע		**מס׳ הנוהל:** 1	**עדכון מס׳:** 1
עדכון אחרון:28/1/2024	**תאריך עדכון: 19.8.25**	**דף מס׳:** 1	**מתוך:** 15

עיריית באר יעקב

נוהל מדיניות אבטחת מידע

מהדורות מסמך:

מס״ד	תאריך	עודכן ע״י	תיאור השינוי
1	28.4.2025	עזרא דיין	גרסה ראשונה
2	19.8.25	עזרא דיין	גרסה שנייה

בקרת מסמך:

גורם	פרטי גורם	תפקיד	תאריך	חתימה
עורך	עזרא דיין	ממונה אבטחת מידע העירייה	19/8/25	עזרא דיין
בודק	תמיר אטייב	מנמ״ר עירייה ואחראי מחשוב		
מאשר	דני אורן ,רו״ח	מנכל העירייה		

מסמך נערך על ידי חברת תשתיות מידע וטכנולוגיות בע״מ | משרד : 072-250-4385 | email: office@iti-il.com

שם הנוהל: נוהל מדיניות אבטחת מידע		**מס׳ הנוהל:** 1	**עדכון מס׳:** 1
עדכון אחרון:28/1/2024	**תאריך עדכון: 19.8.25**	**דף מס׳:** 2	**מתוך:** 15

1. כללי:

1.1. מטרת הנוהל

1.1.1. להגדיר את מדיניות העירייה (להלן: "**העירייה**") בנושאי אבטחת מידע ואת פעילויות המחשוב למניעה, תחזוקה וניהול משימות אבטחת מידע.

1.1.2. הצגת תפיסת העירייה ומחויבותה לנושא אבטחת המידע והגנת הסייבר וקביעת עקרונות מנחים ליישום אבטחת המידע בעירייה ולהעלאת מודעות של כל הגורמים בעירייה לנושאי אבטחת המידע והגנת הסייבר.

1.1.3. הצגת קביעת תפקידים והפרדת תפקידים, סמכויות, אחריות, מסגרת תהליכית וארגונית, והקצאת משאבים ותקציב, עבור פעילות אבטחת מידע והגנת הסייבר .

1.1.4. לוודא כי תפקידים בתחומי אחריות יופרדו על מנת להפחית אפשרויות לשינוי לא רצוי או מתוכנן או שימוש לא נכון בנכס.

1.1.5. להגדיר את תהליך ניהול מערכת אבטחת המידע בעירייה כולל התחייבות הנהלת העירייה ולוודא ביצוע התהליכים לאבטחת המידע מול בעלי תפקידים.

1.1.6. התחייבות העירייה לנהל תקציב מסודר בתחום אבטחת מידע בהתאם להגדרות תפקידים ואחריות כל בעל תפקיד.

1.2. הגדרות (בהתאם לתיקון 13 לחוק הגנת הפרטיות)

1.2.1. מסמך זה עושה שימוש במונחים מתחום הגנת פרטיות ואבטחת מידע. להלן הסברים למושגים מרכזיים, במטרה לאפשר הבנה לכלל הציבור, כולל תושבים, עובדים, ספקים, ומנהלים:

1.2.2. **מידע אישי**

1.2.2.1. כל מידע שניתן לזהות באמצעותו אדם, בין ישירות ובין בעקיפין. לדוגמה: שם, מספר זהות, כתובת, טלפון, תעודת עובד, כתובת דוא"ל, תמונה, מיקום גיאוגרפי, וכד.'

1.2.3. **מידע רגיש**

1.2.3.1. סוג מיוחד של מידע אישי שחשיפתו עלולה לגרום לפגיעה בפרטיות. לדוגמה: מידע רפואי, מידע על נטייה מינית, מוגבלות, אמונות דתיות או פוליטיות, נתונים ביומטריים (כמו טביעת אצבע או צילום פנים), ועוד.

מסמך נערך על ידי חברת תשתיות מידע וטכנולוגיות בע״מ | משרד : 072-250-4385 | email: office@iti-il.com
סיווג מסמך : בלמ״ס

1.2.4. **מאגר מידע**

1.2.4.1. קובץ או מערכת, ידנית או ממוחשבת, המכילה מידע אישי באופן שיטתי – לדוגמה: מערכת ניהול גבייה, מערכת נוכחות עובדים, מערכת רישום תלמידים, מערכת מצלמות אבטחה.

1.2.5. **נושא מידע**

1.2.5.1. האדם שעליו מצוי המידע – כגון תושב, עובד עירייה, ספק שירות, מועמד לעבודה, תלמיד או מבקר.

1.2.6. **עיבוד מידע**

1.2.6.1. כל פעולה שנעשית במידע האישי, כולל: איסוף, אחסון, שימוש, שינוי, העברה, הפצה, מחיקה, סיווג, או ניתוח של המידע.

1.2.7. **סיווג מידע**

1.2.7.1. קביעת רמת הרגישות של מידע בהתאם לתוכנו – מידע עשוי להיות רגיל, אישי, רגיש או מסווג. הסיווג משפיע על רמת ההגנה הנדרשת.

1.2.8. **משתמש מורשה / מורשה גישה**

1.2.8.1. עובד, ספק או מערכת ממוחשבת שקיבלו הרשאה מטעם העירייה לגשת למידע אישי, אך ורק לצורך ביצוע תפקידם.

1.2.9. **הסכמה מדעת**

1.2.9.1. הסכמה של נושא מידע לאחר שקיבל הסבר ברור על המידע שנאסף, המטרות, משך השמירה והזכויות שלו.

1.2.10. **זכות עיון, תיקון ומחיקה**

1.2.10.1. זכותו של אדם לבקש עותק מהמידע שנשמר עליו במאגרי העירייה, לתקן מידע שגוי או מיושן, ולבקש מחיקה של מידע שאינו דרוש עוד, בהתאם לחוק.

1.2.11. **עיקרון מזעור מידע**

1.2.11.1. עקרון לפיו העירייה אוספת אך ורק את המידע ההכרחי למטרות ידועות מראש, אינה שומרת מידע מעבר לנדרש, ואינה עושה בו שימוש חוזר למטרות נוספות שלא הוגדרו מראש.

1.2.12. **אבטחת מידע**

1.2.12.1. הגנה על מידע אישי ומערכות מידע מפני גישה, שימוש, שינוי או חשיפה בלתי מורשית – באמצעים טכנולוגיים, פיזיים וארגוניים.

1.2.13. **הגנת הסייבר**

1.2.13.1. מערכת האמצעים והפעולות שנוקטת העירייה כדי למנוע תקיפות, חדירות או שיבושים למערכות המידע שלה.

1.2.14. **הצפנה(Encryption)**

1.2.14.1. שימוש באמצעים טכנולוגיים להפיכת המידע לבלתי קריא ללא מפתח מתאים, לצורך שמירה על סודיות ושלמות המידע.

1.2.15. **ניתוח השפעה על פרטיות**

1.2.15.1. בדיקה מוקדמת שמתבצעת עבור מערכות חדשות או תהליכים משמעותיים, כדי לבחון את ההשפעה האפשרית על פרטיות נושאי מידע ולצמצם סיכונים מראש.

1.2.16. **ספק מידע / נותן שירות**

1.2.16.1. גורם חיצוני המספק שירותים לעירייה (למשל – תוכנה, מצלמות, מחשוב, ניתוח נתונים) וייתכן שיש לו גישה למידע אישי במסגרת השירות.

1.3. נושא תחום אבטחת מידע

1.3.1. אבטחת מידע בארגון הינו נרחב ורב גוני. תחום זה מרכז את המשימות שמבוצעות על מנת להבטיח שימוש ראוי במשאבי המחשוב של העירייה, שמירה על אמינות המידע, שמירה על זמינותו, מניעת רוגלות, חדירות לא מורשות ווירוסים למיניהם, הדרכת המשתמשים לשימוש נכון ומאובטח בציוד המחשוב, המידע ואמצעי האחסון בעירייה.

1.3.2. המדיניות מחייבת את כלל העובדים, לרבות צוות הנהלה, גזברית ,ספקי שירות חיצוניים, לרבות קבלנים, קבלני משנה וספקי מיקור חוץ. המדיניות חלה על כלל המערכות הממוחשבות המשמשות את העירייה, לרבות שרתים, מסדי נתונים וכל אמצעי מחשוב ותקשורת אחר שבניהול העירייה, בבעלותה ו/או בשליטתה.

1.4. הצהרת הנהלה לאבטחת מידע והגנת הסייבר

1.4.1. עקרונות המדיניות הקבועים במסמך זה גובשו על ידי ממונה אבטחת מידע והגנת הסייבר בעירייה ואושרו על ידי מנכ״ל העירייה

1.4.2. הצהרת מדיניות אבטחת מידע תפורסם לתושבי ועובדי העירייה באתר העירייה לצפייה לציבור ותתעדכן מעת לעת בהתאם לדרישות הדין.

1.4.3. בכל מקרה של שינוי בכללי המדיניות או שינוי שאינו זניח בסביבה הטכנולוגית יש לבצע אישור נוסף למסמך המדיניות.

1.4.4. לאחר אישור ועדכון המדיניות יש ליידע את כלל הגורמים הרלוונטיים כגון :הנהלה וגזברית העירייה, עובדים, ספקים וכו'(על השינויים שבוצעו.)

1.4.5. אחת לרבעון יתקיים דיון בנושא אבטחת המידע במאגרים לפי חוק הגנת הפרטיות ותקנותיו.

1.4.6. בדיון ישתתפו : מנכ״ל העירייה, ממונה אבטחת מידע ומנמ״ר העירייה וגורמים נוספים לפי הצורך.

1.5. יעדי העירייה:

1.5.1. שמירה על אבטחת המידע והגנת הסייבר היא גורם הכרחי להגנה על מידע אישי שבידי העירייה ולמזעור הסיכונים התפעוליים, להפחתת נזקים כספיים ונזקי מוניטין, לבקרה על שיתוף בנתוני עמידה בדרישות הדין והרגולציה.

1.5.2. להבטיח שמירה על אבטחת המידע והגנת הסייבר של העירייה, כתנאי הכרחי להגנה על מידע אישי שבידי ,למזעור הסיכונים התפעוליים, להפחתת נזקים כספיים ונזקי מוניטין, לבקרה על שיתוף בנתוני עמידה בדרישות הדין והרגולציה

1.6. ציות למדיניות ותקני אבטחת מידע:

העירייה פועלת ומצייתת למספר תקנים ורגולציות לשמירת ואבטחת המידע של תושביה.

1.6.1. חוק הגנת הפרטיות, התשמ"א - 1981 , התקנות לפיו)ובפרט, תקנות הגנת הפרטיות אבטחת מידע התשע"ז - 2017 (והוראות הרשות להגנת הפרטיות;)

1.6.2. תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים, תשמ"ו-1986.

1.6.3. חוק המחשבים, תשנ"ה 1995.

1.6.3.1. גופים:

1.6.3.1.1. משרד המשפטים- הרשות להגנת הפרטיות

1.6.3.1.2. מערך הסייבר הלאומי

מסמך נערך על ידי חברת תשתיות מידע וטכנולוגיות בע״מ | משרד : 072-250-4385 | email: office@iti-il.com

1.6.3.1.3. רשות האוכלוסין(רשם אוכלוסין)

1.7. העירייה תדאג ליידוע נושאי מידע – תושבים, ספקים, עובדים ומבקרים – אודות מטרות השימוש במידע, זהות מקבלי המידע, משך השמירה ודרכי פנייה. יידוע זה יבוצע באמצעים ברורים ונגישים לרבות באתר העירייה, טפסים ובממשקים דיגיטליים, בהתאם לחובת השקיפות בסעיפים 11-12 לתיקון 13.

ראה מדיניות פרטיות באתר העירייה

2. עקרונות מדיניות אבטחת מידע והגנת הסייבר

2.1. איסוף מידע, אחסונו, משך תקופת ההגנה עליו ואופן השימוש בו יעשו בכפוף לדרישות הדין והרגולציה החלות על העירייה.

2.2. רמת ההגנה על המידע האגור במערכות המחשוב של העירייה תיקבע על פי אופיו של אותו מידע סיווגו, והסיכון הנגזר ממנו.

2.3. הגנה על מאגרי מידע כנדרש בחוק, בהתאם למפורט במדיניות הגנת הפרטיות ועפ"י הוראות הממונה על הגנת הפרטיות.

2.4. העירייה תיישם אמצעים, שיטות ונהלים סבירים ומקובלים לשמירת זמינות המידע והגנתו מפני הרס, פגיעה ו/או שינוי לא מוסמך, ולצמצום סיכוני אבטחת מידע וסייבר והכל כמתחייב מהוראות כל דין.

2.5. הגישה למידע תהיה מורשית רק לגורמים אנושיים וממוחשבים ובמידה הנדרשת לביצוע תפקידם אשר הורשו לכך במפורש על-ידי ממונה מאגרי מידע כהגדרתם בחוק.

3. ייעוד הנוהל:

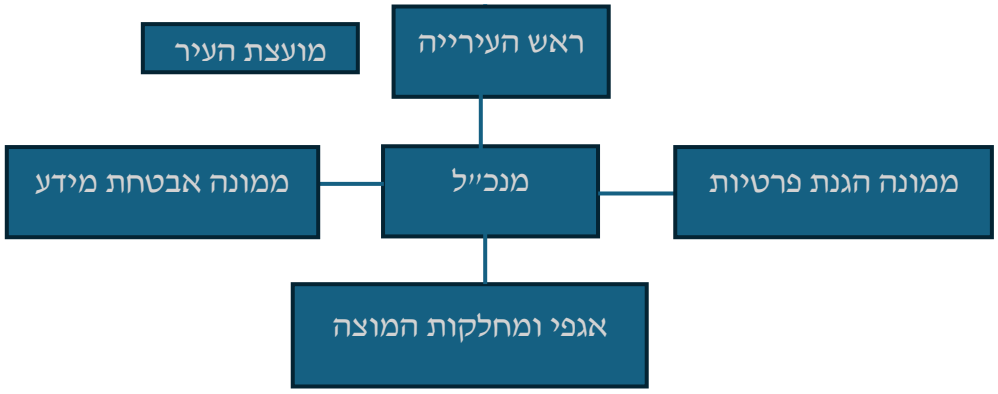
3.1. הנוהל מיועד לעובדי העירייה, ספקי המחשוב ומערכות המידע של העירייה, משתמשי העירייה וכל גורם בעירייה בעל גישה למערכות המחשוב. הנוהל מחייב כל גורם המטפל בשרתים בעירייה ו/או בתחנות העבודה ו/או במאגרי המידע.

3.2. על הנוהל להיות מפורסם לכלל עובדי הארגון וגורמים החיצונים רלוונטיים לעיל. (מזכירות העירייה/שירות לקוחות)

3.3. מדיניות אבטחת המידע תסקר לכל הפחות אחת לשנה על ידי ממונה אבטחת המידע והגנת הסייבר, כדי להבטיח שמירה, תיקוף, עדכניות, והתאמות נאותות ואפקטיביות של המדיניות.

3.4. השינויים יובאו לאישור מנכ״ל העירייה.

4. מבנה העירייה



5. אחריות הנהלת העירייה

5.1. הנהלת העירייה

5.1.1. הנהלת העירייה מחויבת לקדם הגנה יעילה על נכסי המידע, הבטחת שלמות ואמינות המידע, שמירה על זמינות מערכות המידע, יישום בקרות אבטחה בכפוף לרגולציה ובהתאם לסיכונים, שמירה על מוניטין העירייה על-ידי קיום עקרונות הסודיות, שלמות, אמינות וזמינות מאגרי המידע הנמצאים ברשותה.

מסמך נערך על ידי חברת תשתיות מידע וטכנולוגיות בע״מ | משרד : 072-250-4385 | email: office@iti-il.com
סיווג מסמך : בלמ״ס

5.1.2. הנהלת העירייה אחראית על הפצת מדיניות אבטחת המידע בעירייה, אספקת משאבים להקמה וניהול מערך אבטחת מידע, קביעת סיכונים ורמות סיכונים, ביצוע סקרי אבטחת מידע, מבדקים פנימיים וביצוע הדרכות אבטחת מידע לעובדים.

5.1.3. הנהלת העירייה תגדיר ותקצה משאבים ותקציב בתחום אבטחת מידע להקמת מערכות אבטחה ובקרה לצורך הפעלתן בתדירות קבועה, תחזוקתן ושיפורן המתמיד.

5.1.4. הנהלת העירייה תגדיר מה אחריות בעלי תפקידים בתחום אבטחת מידע, תוודא הגדרות תפקיד ברורות ,תמנע ותפחית אפשריות לשינוי לא מתוכנן או לא רצוי בנכס, או שימוש לא נכון בנכסי הארגון .

5.1.5. הנהלת העירייה תמנה ועדת משנה קבועה אשר תפעל כוועדת היגוי לאבטחת מידע והגנת הסייבר להלן – "ועדת היגוי" או "הוועדה"(.ועדת היגוי)

5.2. אחריות עובדי העירייה – כחלק ממדיניות אבטחת מידע

5.2.1. כלל עובדי העירייה מחויבים לתחום אבטחת המידע והגנת המידע כחלק בלתי נפרד מאחריותו המקצועית מכורח תפקידו.

5.2.2. .בעלי תפקידים יקפידו על יישום ואכיפת נהלי אבטחת המידע ,עידוד מודעות העובדים בנושא והבעת תמיכה בפעילות מנמ״ר העירייה וממונה אבטחת מידע.

5.2.3. העירייה תדרוש מעובדיה, ספקים וקבלני שירות (קבועים או מזדמנים ,)אחריות אישית ליישום כללי המדיניות בתחומי תפקידם ,ודיווח מידי על גורמי סיכון ואירועים המתרחשים בהיבט אבטחת המידע והגנת הסייבר.

5.2.4. כל עובד וספק הנותן שירות חיצוני בעירייה יחתמו על טופס התחייבות לשמירת סודיות ואבטחת מידע וקיום הוראות אבטחת המידע.

5.3. סיווג מידע

5.3.1. העירייה הינו גוף ציבורי שמטרתו לתת שירותים מוניציפליים לתושבי העירייה ובהיותו חשוף למידע רב אודות תושביו בעת העברת מידע ושמירת המידע הקיים בארגון לרבות שירותי גבייה. נדרש למנוע העברת מידע בצורה שאינה מבוקרת ולהבטיח בקרה נאותה.

5.3.2. העירייה תנהל בקרה ותיעוד אחר רשומות ומסמכים בעלי מידע רגיש ומסווג.

5.3.3. מידע המוגדר מסווג ורגיש יש לבצע רישום מאגר מידע מסודר במשרד המשפטים.

6. פעולות ובדיקות אבטחת המידע בארגון

6.1. תחומי אבטחת מידע והגנת הסייבר

האמצעים ליישום מדיניות אבטחת מידע והגנת הסייבר בעירייה כוללים הגדרת תפקידים, סמכויות, תחומי אחריות, אכיפת נהלים והנחיות לשימוש בכלים טכנולוגיים, הטמעה ויישום אבטחת מידע והגנת הסייבר בהיערכות למצבי חירום.

6.2. אבטחת מידע והגנת הסייבר כוללת:

6.2.1. אבטחת מידע פרטי, אישי ו/או רגיש אודות תושבי ועובדי העירייה, מידע אישי או רגיש במחקרים, מידע אקדמי, ספקים, מבקרים ותלמידים, באחסנה, בתעבורה או בשימוש.

6.2.2. אבטחה פיזית של ציוד מחשוב, תקשורת, כבלים וכל אמצעי אחסון של מידע.

6.2.3. אבטחת כניסות ויציאות למתחמים בהם נמצאות מערכות המחשוב ואמצעי התקשורת.

6.2.4. אבטחת עמדות קצה, תחנות עבודה, מחשבים ניידים, ציוד תקשורת וכל ציוד אחר, לרבות אמצעי הפלט לסוגיו ,נייר, מגנטי ואופטי, הנושא מידע בצורה דיגיטלית.

6.2.5. אבטחה לוגית של תוכנות, תהליכים, אפליקציות, מסדי נתונים, שרתים, תעבורת תקשורת ומאגרי מידע.

6.3. בקרת גישה של משתמשים ו/או גורמים חיצוניים למערכות מידע ומאגרי מידע.

6.3.1. כל משתמש מקבל הרשאות גישה בהתאם לתפקידו בלבד .(Least Privilege) המערכת כוללת תיעוד (לוגים) של כל גישה למידע אישי. אחת לשנה או בהתאם לדרישה תתבצע בקרת הרשאות מתועדת על ידי ממונה אבטחת מידע ומנמ״ר העירייה.

6.3.2. במערכות רגישות יושם אימות דו-שלבי (MFA) לכלל המשתמשים המורשים לגישה למידע אישי או רגיש.

6.3.3. כל משתמש מחויב בסיסמא אישית בהתאם למדיניות קביעת סיסמאות מאובטחות.

6.3.4. כל משתמש מקבל הרשאות גישה בהתאם לתפקידו בלבד .(Least Privilege) המערכת כוללת תיעוד (לוגים) של כל גישה למידע אישי. אחת לרבעון תתבצע בקרת הרשאות מתועדת על ידי ממונה אבטחת מידע. כלל המשתמשים מחויבים להשתמש בסיסמאות חזקות בהתאם למדיניות אבטחת מידע, הכוללות שילוב של אותיות, מספרים ותווים מיוחדים, ואשר מוחלפות בפרקי זמן קבועים בהתאם לנוהל.

6.3.5. ממונה אבטחת מידע ומנמ״ר העירייה מקיימים אחת לשנה בקרת הרשאות ובוחנים את הצורך בהמשך גישה בהתאם לתפקיד, לרבות ניתוח רמות גישה של משתמשים במערכות רגישות.

6.3.6. בקרה על העברת מידע לגורמים חיצוניים.

6.3.7. אבטחת מידע בניהול כוח אדם.

6.4. סקר סיכונים -הערכת סיכוני אבטחת מידע והגנת הסייבר

6.4.1. העירייה תקיים תהליך הערכת סיכוני אבטחת מידע וסייבר במערכות המידע, מערכות התקשורת והממשקים הכולל בתוכו זיהוי, מזעור או מניעה של סיכוני האבטחה העלולים להשפיע על המידע.

6.4.2. תהליך זה יתבסס על סיווג נכסי מידע, איומי אבטחת המידע ואופי העבודה במערכות העירייה.

6.4.3. תוצר הערכת הסיכונים ינחה את גזברית העירייה בהפניית משאבים נאותים להטמעת אמצעי אבטחה, בקרות ומיקוד סקרי סיכוני האבטחה במערכות העירייה ויספק מדרג רגישות של מערכות השונות המתבסס בין היתר על סיווג המידע.

6.4.4. ממונה אבטחת מידע והגנת הסייבר יבצע הערכת סיכונים פעם בשנה ובעת שינוי מהותי כמפורט.

6.5. נהלי אבטחת מידע

6.5.1. העירייה תכין נהלי אבטחת המידע, הוראות עבודה ותהליכי העבודה המפרטת את תפיסת ההנהלה לגבי אבטחת המידע והגנת הסייבר בעירייה והעקרונות המנחים ליישומה.

6.5.2. לכל תהליך בעירייה המטפל בניהול, הכנסה, תפעול, תחזוקה, גיבוי, העברה והוצאה של מידע ייכתב נוהל אבטחת מידע מפורט או הוראת עבודה מתאימה.

6.5.3. יישום בקרות אבטחת מידע יתבצע על פי נהלי העירייה והוראות העבודה בהתאם לניהול סיכוני אבטחה וסייבר באחריות מנמ״ר העירייה ובפיקוח ממונה אבטחת המידע והגנת הסייבר.

6.5.3.1. נהלי אבטחת המידע וסייבר יכללו לכל הפחות את כל הנושאים הבאים:

6.5.3.1.1. אבטחה פיזית.

מסמך נערך על ידי חברת תשתיות מידע וטכנולוגיות בע״מ | משרד : 072-250-4385 | email: office@iti-il.com
סיווג מסמך : בלמ״ס

6.5.3.1.2. אבטחה לוגית ויישומית.

6.5.3.1.3. אבטחת שרתים, עמדות עבודה ומערכות הפעלה.

6.5.3.1.4. אבטחת תשתיות תקשורת.

6.5.3.1.5. ניהול שינויים במערכות מידע ומערכות מחשוב.

6.5.3.1.6. הגנה מפני פוגענים, נוזקות וקוד זדוני/עוין.

6.5.3.1.7. זיהוי משתמשים והרשאות גישה כולל הרשאות.

6.5.3.1.8. העברת מידע לגורמים חיצוניים.

6.5.3.1.9. שימוש נאות לרבות בדואר אלקטרוני ובאינטרנט.

6.5.3.1.10. שימוש באמצעי מחשוב ניידים ומדיה נתיקה.

6.5.3.1.11. בקרת גישה מרחוק.

6.5.3.1.12. הצפנה.

6.6. אבטחת מידע והצפנה

6.6.1. המידע האישי המוזן למערכות העירייה מוצפן בעת מעברו בתקשורת (Data in Transit) וכן בהיותו מאוחסן (Data at Rest)באמצעים קריפטוגרפים התואמים את הנחיות מערך הסייבר הלאומי.

6.6.2. העירייה דורשת כי כל שירותי הענן ואחסון המידע יתבצעו בשרתים הנמצאים בתחום מדינת ישראל בלבד, בהתאם לחוק הגנת הפרטיות ובכפוף לחוזים מול ספקים הכוללים סעיף תחום שיפוט .(Data Locality)

6.6.3. העירייה מחייבת כי כל מידע בעל רגישות מיוחדת, המועבר מעמדות קצה או דרכן, יועבר באמצעות ערוצים מוצפנים בלבד, תוך שימוש באמצעי הצפנה תקניים, וזאת לשם הבטחת שלמות המידע, סודיותו ומניעת חשיפתו לגורמים בלתי מורשים .הנהלים/ההוראות יופצו לכלל העובדים או המשתמשים הרלוונטיים ויעברו תהליך בדיקה ועדכון בהתאם לצורך, עם שינוי משמעותי בסביבה הטכנולוגית או לאחר אירוע אבטחת מידע, ולכל הפחות אחת לשנה.

6.7. אירועי אבטחת מידע- טיפול באירועים

6.7.1. בעת טיפול באירועי אבטחת מידע, לרבות אירועי סייבר או חשש לדליפת מידע אישי, תפעל העירייה באופן הבא:

א. איסוף ממצאים טכנולוגיים וראייתיים;

ב. ביצוע תחקיר מסודר;(Post-Mortem) עי ממונה אבטחת מידע.

ג. דיווח מיידי לממונה אבטחת מידע, ליועץ המשפטי ולממונה הגנת פרטיות;

ד. הפקת דוח אירוע פנימי הכולל המלצות לתיקון ושיפור;

ה. עדכון נהלים בהתאם לממצאי התחקיר;

ו. דיווח לרשות להגנת הפרטיות ככל שמדובר באירוע חמור;

ז. תיעוד מלא של פעולות הזיהוי, הטיפול והשיקום;

ח. הפצת מסר פנימי לעובדים עם דגשים על ערנות ואחריות אישית.

6.8 הגנת פרטיות הדרכות ותסקירי פרטיות

6.8.1. העירייה תבצע הדרכות ייעודיות בנושאי הגנת פרטיות ואבטחת מידע אחת לשנה לעובדים, ולספקים לפי מידת הרלוונטיות.

6.8.2. עבור כל מערכת חדשה או שינוי מהותי בתהליכי עיבוד מידע אישי, מבוצע ניתוח השפעה על פרטיות (DPIA) בהתאם להנחיות הרשות להגנת הפרטיות ולדרישות תיקון 13

6.9 המשכיות עסקית

כל יחידות העירייה נדרשות לקבוע הוראות עבודה ונהלים כתובים להבטחת המשכיות עסקית, ובכלל זה:

6.9.1. מדיניות גיבוי ושחזור;

6.9.2. תכנון תגובה לאירועים קריטיים;

6.9.3. שמירה על זמינות ונגישות למידע חיוני;

6.9.4. ביצוע בדיקות תקופתיות להערכת מוכנות.

6.9.5. לעירייה נוהל גיבויים עדכני, הכולל:

א. תדירות גיבוי שוטפת בהתאם לסיווג המידע;

ב. שמירת הגיבויים במיקומים מאובטחים פיזית ודיגיטלית;

ג. ביצוע בדיקות שחזור אחת לרבעון לפחות;

ד. ניטור אוטומטי לתקינות תהליך הגיבוי;

6.9.6. עדכון הנוהל על סמך תחקירי אירועים ותובנות מהשטח.

6.10 התנהלות מול ספקים

6.10.1. העירייה תנהל ותתעד הסכמים עם ספקי שירותי מידע (לרבות חברות תוכנה, מערכות CRM, גבייה, מוקדים וכיו"ב) שכוללים: **סעיפי הגנת פרטיות ואבטחת מידע בהתאם לתקנות:**

6.10.1.1. התחייבות לסודיות, גיבוי, בקרה ואי-העברת מידע ללא אישור העירייה.

6.10.1.2. חתימה על הסכם עיבוד מידע מול הספק.

6.10.1.3. חובת ביצוע בדיקות אבטחת מידע למערכות בהן נעשה עיבוד מידע אישי.

6.10.1.4. קיום מנגנון התראה ודיווח על אירוע אבטחת מידע תוך 24 שעות מהרגע שזוהה.

6.10.1.5. לעירייה נוהל ספקים מוסדר, המחייב כל ספק לעמוד בדרישות אבטחת מידע, ובכלל זה:

6.10.1.6. קבלת תעודות אבטחת מידע מוכרות; לרבות מבדקי PT.

6.10.1.7. ביצוע מעקב תקופתי אחר הרשאות גישה;

6.10.1.8. איסור העברת מידע לצדדים שלישיים או מחוץ לגבולות ישראל ללא אישור מראש;

6.10.1.9. שמירה על המידע המאוחסן בענן בהתאם להנחיות הרשות להגנת הפרטיות;

6.10.1.10. עמידה בתיקון 13 לרבות עיון מחיקה תיקון של מידע;

6.10.1.11. החובה למחוק או לשמור מידע בהתאם לחוק תחול גם על קבלני משנה של הספקים, והעירייה תבצע בקרה על כך.

6.10.1.12. שימוש במידע רק למטרות שהוגדרו מראש ובשום אופן לא למטרות אחרות.

6.11. כל ספק, יקבל גישה למידע רק בהוראה מפורשת של העירייה, בהתאם להרשאות מגודרות ולפרקי זמן מאושרים. ספק נדרש לתעד כל גישה למידע אישי, ופעולות אלו נבדקות במסגרת ביקורת אבטחת מידע תקופתית

6.12. העירייה תבצע אחת לשנה ביקורת אבטחת מידע מול ספקים להם ניתנה הרשאה לעיבוד מידע אישי. הביקורת תכלול סקירת אופן ההרשאות, אמצעי הצפנה, והתחייבות להמשכיות עסקית ולדיווח על אירועים.

7. נושאי מידע-עיון, תיקון מחיקה

7.1. העירייה מתחייבת למתן מענה לפניות נושאי מידע תוך 30 יום, לרבות זכות לעיין, לתקן, למחוק מידע – ראה מדיניות פרטיות ותנאי שימוש אתר הרשות.

7.2. הפנייה של נושא המידע תעשה דרך אתר הרשות תתועד ותועבר לפי העניין לממונה אבטחת מידע, לממונה הגנת פרטיות וליועץ המשפטי לבחינה ומענה.

7.3. לכול פנייה בנושא הגנת פרטיות ניתן לפנות לdpo@iti-il.com

7.3.1. העירייה תיישם מדיניות שימור ומחיקת מידע (נוהל גריעת מידע אישי) באופן תקופתי לפי עקרון מזעור מידע.(Data Minimization) לרבות דיני הגנת הפרטיות וחוק הארכיונים.

7.3.2. שימוש במידע אישי יתבצע רק לצרכים שהוגדרו מראש, ואין לעשות שימוש חוזר במידע למטרות אחרות

7.3.3. מידע שאינו דרוש עוד – יימחק או יישמר בארכיון בתנאי הצפנה בכפוף להוראות הדין ורמת סיווג המידע.

7.3.4. יתבצע תיעוד פעולות מחיקה

7.3.5. אחת לשנה תיערך סקירה על כלל המאגרים.

7.3.6. חוזים עם ספקי שירות כוללים הוראות המחייבות את הספק למחוק מידע אישי בהתאם להנחיות העירייה, רק כאשר פקע הצורך החוקי או התפעולי בעיבודו, ולוודא שהמידע לא יועבר או יישמר שלא לצורך. הספקים מחויבים להעביר לעירייה דיווח תקופתי על ביצועי מחיקה או שימור בהתאם לנוהל.

8. אחריות סמכות ותוקף:

8.1. נוהל זה אינו מחליף את דרכי ההתערבות והטיפול הקיימים במקרים המובאים לעיל, אלא בא להוסיף עליהם.

8.2. האחריות והסמכות לביצוע נוהל זה הינה על ממונה אבטחת מידע.

8.3. אחריות מנמ״ר העירייה לפקח על אכיפת הנוהל ועמידה בדרשותיו.

8.4. נוהל זה ייכנס לתוקפו החל מיום פרסומו.

שם הנוהל: נוהל מדיניות אבטחת מידע		**מס׳ הנוהל:** 1	**עדכון מס׳:** 1
עדכון אחרון:28/1/2024	**תאריך עדכון: 19.8.25**	**דף מס׳:** 15	**מתוך:** 15

9. נספחים- נספח א- אנשי קשר עירייה- תחום אבטחת מידע

איש קשר	תפקיד	איימל
רו״ח, דני אורן	מנכ"ל	dani@b-y.org.il
מר' תמיר אייטיגב	ממ״ר עירייה-מנהל מחשוב ראשי	tamir@b-y.org.il
מר' עזרא דיין	ממונהד אבטחת מידע	ezradyn@iti-il.com

מסמך נערך על ידי חברת תשתיות מידע וטכנולוגיות בע״מ | משרד : 072-250-4385 | email: office@iti-il.com
סיווג מסמך : בלמ״ס