נוהל שימוש מאובטח בבינה מלאכותית (AI)

1. מטרות הנוהל

הנוהל נועד להבטיח שימוש מאובטח ואחראי בכלי בינה מלאכותית תוך הגנה על מידע רגיש וניהול סיכוני אבטחת מידע.

2. תחום התכולה

הנוהל חל על כל העובדים, בעירייה העושים שימוש בכלי בינה מלאכותית במסגרת העבודה.

3. הגדרות

- **בינה מלאכותית (AI):** כל כלי או מערכת המבוססים על טכנולוגיות למידת מכונה, ניתוח נתונים וחיזוי.
- **מידע רגיש**: כל מידע אישי, עסקי או סודי שעלול להזיק לעירייה אם ייחשף לגורמים בלתי מורשים.

4. כללי השימוש

4.1. סיווג מידע

- כל מידע שמוזן לכלי בינה מלאכותית יסווג לפי רמת רגישותו (רגיש, לא רגיש).

4.2. הגנה על מידע

- יש להימנע מהזנת מידע אישי, עסקי או סודי לכלי בינה מלאכותית שאינו מאובטח או שאין לו מדיניות פרטיות ברורה.
- מומלץ להשתמש בגרסאות מקומיות של כלי AI או בגרסאות עם הגנה חזקה על פרטיות המשתמש.

4.3. מדיניות פרטיות

- כל כלי בינה מלאכותית שבו משתמשים חייב להכיל מדיניות פרטיות שמכסה את השימוש במידע הנמסר.
- דליפת מידע רגיש: כלי AI עשויים לשמור את המידע שאתם מזינים בהם, כולל מידע אישי, עסקי או סודי. כדי להימנע מכך, יש להימנע משיתוף פרטים מזהים כמו מספרי טלפון, כתובות או סיסמאות וכו'.
- ניטור ושימוש במידע ללא ידיעתכם: חברות מפתחות AI עשויות להשתמש במידע שלכם לצורך שיפור הכלים שלהן או למטרות אחרות. חשוב לקרוא את מדיניות הפרטיות של הכלי ולבחור באפשרות שמונעת שיתוף מידע לצורכי פיתוח, אם קיימת.
- ניצול לרעה על ידי גורמים זדוניים: האקרים עלולים לנצל את המידע שאתם מזינים לצורך פעולות זדוניות כמו פישינג או התחזות. חשוב להשתמש בכלים רק דרך הפלטפורמות הרשמיות ולהימנע מהכנסת מידע רגיש למערכות לא מאובטחות.

4.4. ניהול משתמשים והרשאות

- יש להגדיר רמות הרשאה שונות למשתמשים בהתאם לתפקידם ולמידע שהם מטפלים בו.
- יש להבטיח שגישה לכלי ה AI - מתאפשרת רק למשתמשים מורשים בלבד.

5. הדרכות ופיקוח

- יש לקיים הדרכות לעובדים בנושא השימוש המאובטח בכלי AI.
- יש לבצע ביקורות תקופתיות כדי לוודא שהנהלים נשמרים וכלי ה AI - אינם מפרים את מדיניות העירייה.

6. דיווח על תקריות

- יש לדווח למנהל אבטחת המידע בעירייה על תקריות אבטחה הקשורות לשימוש בכל AI.
- יש לבדוק כל תקרית ולהפיק לקחים על מנת למנוע הישנות תקריות דומות.

7. עדכון נהלים

- הנוהל ייבדק ויעודכן בהתאם להתפתחויות טכנולוגיות ושינויים בסיכוני האבטחה.