



המועצה המקומית קרית-יערים (טלזסטון)

מספר נוהל: 01-02 מהדורה: 1	המועצה המקומית קרית יערים	
תאריך עדכון: 07.11.2019	נוהל אבטחת מידע- מאגרי מידע	

1. רקע

- 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, אשר מטרתה צמצום החשש מפני שימוש לרעה או פגיעה בשלמות המידע.
- 1.2. תקנות אבטחת הפרטיות (אבטחת מידע) התשע"ז-2017 (להלן: "תקנות אבטחת מידע"), קובעות עקרונות אבטחת מידע הקשורים בניהול ושימוש מידע במאגרי המידע, בהתבסס על תקני אבטחת מידע מקובלים בעולם.
- 1.3. אבטחת מידע במערכות המידע של המועצה המקומית (להלן: "המועצה") הינה חיונית להגנת המידע של המועצה והתושבים.

2. מטרת הנוהל

- 2.1. הגדרת כללי אבטחת מידע המחייבים את המועצה ועובדיה.
- 2.2. התאמת פעילות המועצה להוראות החוק והתקנות והנחיות הרשות להגנת הפרטיות, כפי שיעודכנו מעת לעת

3. הגדרות

- הגדרות ומונחים בתחומי הגנת הפרטיות, הינם בהתאם להגדרתם בחוק ובתקנות, נכון ליום עדכון הנוהל.
- 3.1. משתמש – אדם הפועל כדין ברשת המחשוב של המועצה
 - 3.2. בעל הרשאה – כהגדרתו בתקנה 1 לתקנות אבטחת מידע
 - 3.3. מאגר מידע- כהגדרתו בחוק ובתקנות
 - 3.4. אנטי וירוס- תוכנה המגינה על מערכות העריה מפני תוכנות זדוניות לסוגיהן.
 - 3.5. ממונה אבטחת מידע – מיש מונה ע"י המועצה בהתאם לכתב המינוי.

4. חלות הנוהל ואחריות

- 4.1. האחריות להבאת הנוהל לכלל המשתמשים במועצה הוא הממונה על משאבי האנוש.
- 4.2. האחריות ליישום הנוהל מוטלת על מזכיר המועצה, או מי שיוסמך לכך מטעמו.
- 4.3. האחריות לבקרת יישום הנוהל הוא הממונה על אבטחת המידע.

5. אבטחה פיזית

- 5.1. המועצה תפעל לבקרת גישה פיזית לחדר השרתים.
- 5.2. כניסה לחדר השרתים תותר לנציגים מורשים של ספק מיקור החוק, לו חוזה בתוקף עם המועצה.
- 5.3. במקרה הצורך, תותר גישה של איש התחזוקה של המועצה, לצורך אחזקה של מערכות החשמל.
- 5.4. אין לאפשר כניסת מבקרים לחדרי עובדי המועצה ללא ליווי של עובד.



המועצה המקומית קרית-יערים (טלזסטון)

- 5.5. בסיום יום העבודה, יש להשאיר סביבת עבודה נקיה, ללא מסמכים, ובמקרים של עובדים להם גישה למאגרי מידע, לנעול את החדרים בסיום יום העבודה.
- 5.6. יש להגביל כניסת מבקרים לבניין המועצה בסיום יום העבודה.
- 5.7. אין לאפשר חיבור של מבקרים לרשת המחשוב של המועצה. במקרים חריגים נדרש אישור של מזכיר המועצה.
- 5.8. אין לאפשר חיבור התקנים ניידים של מבקרים למערכות המועצה.
- 5.9. על שימוש בהתקנים ניידים ע"י עובדי המועצה יחולו ההוראות הבאות:
- 5.9.1. אין לחבר לרשת העיריה ו/או לשמור מידע על התקנים ניידים אשר לא הוקצו לעובד על ידי המועצה.
- 5.9.2. אין לבצע כל שימוש בהתקנים הניידים של המועצה באופן החורג ממסגרת התפקיד, הסמכות וההרשאות אשר ניתנו למשתמש.
- 5.9.3. על המועצה להגביל ככל הניתן ואף למנוע אפשרות חיבור של התקנים ניידים למערכותיה במתכונת ההולמת את רמת האבטחה של המאגר.
- 5.9.4. במקרה בו משתמש נתקל באירוע חריג, המעלה חשש לפגיעה בשלמות המידע במאגר או זליגתו אל מחוץ למערכות המאגר, עליו לדווח מיידית לממונה על אבטחת המידע, אשר ישתף את המזכיר בחשש, ויבדוק בהתאם.
- 6. הרשאות גישה**
- 6.1. בקשה להרשאות גישה תוגש ע"י העובד המבקש, לאחר אישור של הממונה עליו, למזכיר המועצה.
- 6.2. הרשאות הגישה למערכות תינתנה על בסיס "הצורך לדעת".
- 6.3. עובד, לו תותר גישה למאגר מידע, יעבור הדרכה פרטנית על חובותיו בהתאם לחוק ולתקנות.
- 6.4. על המערכת לאלץ החלפת סיסמא כל פרק זמן. על הסיסמא לעמוד בדרישות מקובלות של תווים נדרשים (אותיות גדולות וקטנות, מספר וסימנן).
- 6.5. אין לכתוב את הסיסמא בצמוד לתחנת הקצה.
- 6.6. חל איסור מוחלט למסור את סיסמת הגישה האישית.
- 6.7. חל איסור מוחלט לבצע פעולות במערכות המועצה תחת שם של עובד אחר.
- 6.8. המערכת תתנתק לאחר פרק זמן קצר (30 דקות) של חוסר שימוש בתחנות הקצה.
- 6.9. עם סיום תפקידו של העובד, על האחראי לדווח למזכיר על סיום התפקיד, והמזכיר יפעל לחסימת הרשאת הגישה.
- 6.10. בסיום יום העבודה, על העובד להתנתק ממערכות המועצה.
- 6.11. לכל עובד תוקצה כתובת מייל שהיא אישית ומיועדת לשימוש מקצועי לצורך ביצוע התפקיד במועצה.
- 7. שמירת מידע וגיבויים**
- 7.1. כל מערכות המועצה יגובו באופן סדיר ואוטומטי.
- 7.2. שמירת הגיבוי בהתאם לחשיבות ורגישות המידע.
- 7.3. שחזור מידע רגיש- רק באישור מזכיר המועצה.
- 7.4. מסמכי הנהלת חשבונות ייסרקו למערכת הנהלת החשבונות המנוהלת בענן.



המועצה המקומית קרית-יערים (טלזסטון)

7.5. על המשתמשים להימנע מלשמור מסמכים על גבי הכוננים הקשיחים המקומיים, אלא בשרתי המועצה.

8. משאבי אנוש- היבטי הגנת הפרטיות

- 8.1. כלל עובדי המועצה המחויבים לשמור על אבטחת המידע בהתאם להוראות נוהל זה.
 - 8.2. הליכי מיון עובדים ושיבוצם, יכללו בחינה של התאמת המועמד, כדי לברר שאין חשש כי העובד אינו מתאים לקבל גישה למאגר מידע בהתאם להגדרות התפקיד אליו הגיש מועמדות.
 - 8.3. לכל עובד חדש תינתן הדרכה לגבי אחריותו וחובותיו להגנת הפרטיות בהתאם להוראות החוק, התקנות ונוהל זה.
 - 8.4. לעובדים להם גישה למאגר מידע, ביום פרסום נוהל זה, תיערך הדרכה לגבי אחריותם וחובותיהם בהתאם להוראות החוק, התקנות והוראות נוהל זה.
 - 8.5. מנהל משאבי האנוש במועצה אחראי לבחינת התאמת המועמדים, ולקיום ההדרכות כאמור.
9. ביקורות תקופתיות
- 9.1. מטרת הביקורות התקופתיות הינה הבטחת התנהלות תקינה במערכות המועצה ובמאגרי המידע שלה, בהתאם להוראות החוק התקנות ונוהל זה.
 - 9.2. הממונה על אבטחת המידע יערוך בדיקות תקופתיות, לפחות פעם בשנתיים לפי תוכנית שתוגדר על ידו מראש ותאושר על ידי מזכיר המועצה.
 - 9.3. מבקרת המועצה תבחן את תוכנית הביקורת ואת הביקורות שיבוצעו על פיה, ותמליץ במידת הצורך על שינויים או דגשים נוספים.
10. אירוע אבטחת מידע
11. יישמר תיעוד לש אירוע אבטחת מידע למשך 12 חודשים לפחות.
- 11.1. משתמש הנתקל באירוע המעלה חשש לפגישעה בשלמות המידע או זליגת מידע ממאגר מידע, ידווח מיידית לממונה על אבטחת המידע או למזכיר המועצה.
 - 11.2. מורשה מטעם חברת מיקור החוץ התומכת במערכות המועצה ובמערכות המחשב, יבדוק את לוג נסיונות הגישה ויבדו וידווח על נסיונות חדירה למאגרי המידע.