04-6086800
04-6469532
1341 17902
www.ein-mahel.muni.il

مجلس محلي عين ماهل
מועצה מקומית עין מאהל

נוהל אבטחת מידע

מועצה מקומית עין מאהל

04-6086800
04-6469532
1341 17902
www.ein-mahel.muni.il

תוכן עניינים

שם הנוהל: אבטחת מידע במועצה המקומית

1. <u>כללי :</u>

א. כל מידע הצבור במערכות הממוחשבות של המועצה או הקשורות למועצה יאובטח ויוגן

כקבוע בסעיף 6 להלן: אין להשתמש בו למטרה שאינה מהמטרות המוטלות על העובד בתוקף תפקידו ואין לאפשר לגורמים כלשהם הקשורים ושאינם קשורים במועצה לעשות בהם שימוש.

ב. אי קיום הוראות הנוהל עלול להוות **עבירה משמעתית, עבירה פלילית** ועוולה אזרחית

הנושאים בצדם עונשים (לרבות עונשי מאסר), קנסות או תשלום פיצויים.

2. <u>הבסיס החוקי לנוהל :</u>

א. . חוק המחשבים, התשנ"ה – 1995.

ב. חוק הגנת הפרטיות, התשמ"א - 1981 ותקנותיו.

ג. . חוק הארכיונים, תשט"ו – 1955.

ד. . חוק חופש המידע, התשנ"ח – 1998.

3. <u>הגדרות :</u>

א. **"המועצה"** - לרבות תאגידיה.

ב. **"עובד"** - מי שעובד במועצה, למענה או מטעמה, לרבות עובד מועצה, עובד חוזה, יועץ או עובד בגוף המעניק שירותים למועצה.

ג. **"המנהל"** - ראש מנהל/אגף/יחידה עצמאית שהוסמך על ידי מנכ"ל המועצה להיות "מנהל מאגר מידע".

ד. **"אבטחת מידע"** - הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין.

ה. **"מידע"** - כל הנתונים והידע, בין בעל פה, בכתב, באיור, על גבי מדיה מגנטית, מוקלט, מוסרט, מצולם וכיו"ב, אשר נמצאים ברשות המועצה ו/או ברשותו של עובד, השייכים ל מועצה או הקשורים אליה בדרך ישירה או עקיפה, ו/או אשר הגיעו אליו מתוקף עבודתו במועצה, עבורה או מטעמה, לרבות מידע רגיש כהגדרתו להלן.

ו. **"מאגר מידע"** - אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב.

ז. **"מידע רגיש"** - דוחות כספיים, תוכנות עסקיות, תוכניות מחקר ופיתוח, נתוני שיווק, פטנטים, תהליכים שאינם נחלת הכלל; נתונים הקשורים לצנעת הפרט או נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישות, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו; קניין רוחני (כהגדרתו להלן); סודות מסחריים ומקצועיים וכל מידע אשר נרשם והוכרז כמידע רגיש על ידי גורם מוסמך במועצה.

ח. **"קניין רוחני"** - הזכויות שהדין מעניק ליוצר על פי יצירתו לרבות זכות יוצרים, פטנט, דגם, סימן מסחרי.

ט. **"שימוש אסור"** - נטילה, העברה, גילוי, מסירה, העתקה, צילום, שיכפול, שליחה, פרסום, פגיעה בפרטיות וכל ש ימוש אחר במידע, שלא למטרות המועצה וטובתה ושלא במסגרת העבודה בה.

י. **"מתקני המועצה"** - מתקנים בבעלות או בשימוש המועצה או בשימוש נותני שירות למועצה, הנוגעים בדבר.

יא. **"אורח"** - כל מי שנכנס למתקני, חצרי ומשרדי המועצה, בהיתר ובהתאם לנוהלי/הנחיות עבודתה ואינו נכלל בהגדרת עובד.

יב. **"חומרה"** - כלל ציוד המחשבים וציוד נלווה המבצעים עיבוד נתונים.

יג. **"תוכנה"** - כלל השיטות, התוכניות, הנהלים ושפות מחשבים הדרושים להפעלת מחשבים, לרבות כל מסמך המכיל מידע על תפעולם ותחזוקתם של מחשבים.

יד. **"המערכת"** - כלל החומרה, התוכנה והמידע הצבור במחשבים, המופעלים במועצה, או מי מטעמה וביחידותיה.

טו. **"עובדי המערכת"** - עובדי המועצה העוסקים במערכת, עובדי חברות כוח-אדם, עובדי החברה החדשה, ועובדי לשכות שירות שהמועצה מזמינה אצלן עיבוד נתונים, יועצים חיצוניים, עובדים של חברות בנות של המועצה, כ גון: החכ"ל, ואף עמותות בנות.

טז. **"סיסמה"** **"צפנים"** או **"קודים"** - סדרת מספרים או תווים המאפשרים גישה למערכת.

יז. **"פלט"** - כל מוצר של עבודת מחשב, בין שהוא מודפס על גבי נייר ובין שהוא מוצג אחרת, אופטית או אלקטרונית.

יח. **"מורשה"** - עובד המערכת שנחשף למידע והורשה לטפל בו כחלק מעיסוקו במועצה, ע"י הקצאת קוד אישי/צופן המאפשר לו כניסה למערכת.

4. <u>מטרה:</u>

הנוהל קובע את סדרי האבטחה של המידע הצבור במועצה, בתאגידיה ובמערכות הממוחשבות, מפני שינוי, השמדה, חשיפה במזיד או במקרה, לרבות:

א. מניעת חדירה לתוכנה או לחומרה לשם קריאה, כתיבה, מחיקה או שינוי של תכנים או מידע הצבורים במערכת - על ידי מי שאינם מורשים לכך.

ב. איסור העברת מידע מידי אדם מורשה, בין שהוא עובד המערכת ובין שהוא מורשה לקבל מידע מידי עובדי המערכת, לידי אדם שאינו מורשה.

ג. חלוקת התפקידים, הסמכויות והאחריות בתחומם הנוגעים בדבר.

5. <u>שמירה על סודיות מוחלטת:</u>

על כל עובד חלה חובת שמירת סודיות מוחלטת כלפי המועצה ובהתאם לכך עליו לנהוג על פי הדין, הנוהג, נהליה והנחיותיה. לפני תחילת עבודתו במועצה יחתום על תצהיר לשמירת סודיות (טופס 90-018). דוגמת הטופס בתוספת א' לנוהל.

6. אבטחת מידע:

א. עובד ינקוט, בתחום אחריותו בכל האמצעים לשם אבטחת המידע שברשותו, לרבות:

1. נעילת ארונות ומגירות המכילים מידע.
2. נעילת דלתות וחלונות במשרדים.
3. כיבוי המחשב בכל יציאה מהחדר ו/או בסיום העבודה.
4. הזנת סיסמה/צופן/קוד אישיים למחשב האישי והחלפתם מידי חצי שנה.
5. גריסת מסמכים.
6. הפעלת מערכות אזעקה במקום בו הותקנו, כאשר לא נוכח בו עובד/מאבטח.

ב. מידע רגיש יופקד בכספת והטיפול בו ייעשה על ידי עובד המועצה המוסמך מתוקף תפקידו, תוך נקיטת האמצעים לאבטחתו, ועל פי נווה לי והנחיות המועצה הנוגעים בדבר.

ג. אין להוציא מידע ממתקני ו משרדי המועצה, ללא אישור ממוסמך לכך. הוצאתו תהא לצורכי עבודה בלבד, ובמקרים אלה בלבד:

1. מסירת המידע היא במסגרת הסמכויות או התפקידים של מוסר המידע והיא דרושה למטרת ביצוע חיקוק או למטרה במסגרת הסמכויות או התפקידים של מוסר המידע או מקבלו.

2. מסירת המידע היא לגוף ציבורי הרשאי לדרוש אותו מידע על פי דין מכל מקור אחר.

3. מגוף ציבורי או למשרד ממשלתי או למוסד מדינה אחר, או בין משרדים או מוסדות באמור, אם מסירת המידע דרושה למטרת ביצוע כל חיקוק או למטרה במסגרת הסמכויות או התפקידים של מוסר המידע או מקבלו.

ד. העברה והפצה של מידע בתוך המועצה ובין העובדים לבניהם - תעשה תוך נקיטת כללי אבטחת מידע, הן בשימוש בדואר אלקטרוני של מסמכים כתובים, והן במסירת פריטים פיזיים (מדיה מגנטית / קלטת / דיסק / תרשים וכו').

ה. אחסון וביעור מסמכים יעשה בהתאם ל"חוק הארכיונים, תשט"ו– 1955 ", ולתקנות "הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"א - 1981 ", בתיאום עם הממונה על רשומות המועצה.

ו._בנוגע למידע ממוחשב, באחריות מנהל מאגרי מידע:-

1. לקיים מערכת אבטחת מידע בכל הרמות במועצה כנגד חדירה חיצונית.

2. לשלמות המידע, זמינותו וגיבויו.

3. לחיסיון המידע.

4. למתן הרשאות לעובדים בהתאם לצרכים.

5. הסרת הרשאות לעובד שנוייד בתוך המערכת או לעובד שסיים את עבודתו במועצה – יתואם בין מנהלת כוח האדם ומנהל מערכות המידע (המנמ"ר) במועצה.

6. לקיום כל חוק/תקנה הנוגעים בדבר, לרבות על ידי גורמי חוץ המחזיקים בהיתר של המועצה במידע שלה/עליה.

ז. המנהל אחראי לקיים מערכת אבטחת מידע פיזית לרבות:

1. בקרה ופיקוח על ביצוע חובות העובד בהתאם לנוהל.
2. מתן היתרים לכניסה למתקני ומשרדי המועצה.
3. מניעת אש, שיטפון, גניבה וכל סכנה אחרת למידע.

7. <u>השימוש במאגרי המידע :</u>

השימוש במאגרי מידע, ניהולם ואבטחתם יעשה בהתאם ל"חוק הגנת הפרטיות, תשמ"א 1981- ותקנותיו.

8. <u>רישום וניהול מאגרי מידע:</u>

א. כל מאגרי המידע במועצה מחויבים ברישום ב**"פנקס מאגרי המידע"** שבמשרד המשפטים, באחריות מנכ"ל המועצה ובאמצעות מנהל מערכות המידע במועצה.

ב. מנהלי מאגרי מידע במועצה יעבירו למנכ"ל רשימה מסודרת בדבר הקמה/ביטול מאגר מידע, מיד עם תחילת ביצוע; הרשימה תכלול את: אופי המידע הצבור במאגר והסיבה לניהולו.

9. <u>מידע לגורמי חוץ:</u>

א. קשר עם התקשורת יעשה בהתאם לנוהל דוברות.

ב. העברת מידע לגורמי חוץ ולצד שלישי:

1. מידע שגילויו מותר עפ"י הוראות חוק חופש המידע - יימסר באמצעות הממונה על חופש המידע במועצה.
2. מידע רגיש/מוגבל - יימסר באישור היועצת המשפטית למועצה, ולאחר חתימת הסכם סודיות בין המועצה לגורם שמבקש את המידע.
3. בהסכמי התקשרות של המועצה עם קבלנים וספקים חיצוניים המעניקים לחברה שירותים שונים, יעוגן בחוזה/הסכם נושא שמירת הסודיות ואבטחת המידע של אותם גופים כלפי המועצה.
4. המידע המועבר לגורמי חוץ לצד שלישי יהיה אך ורק המידע הנוגע ולפי הצורך, ורק לאחר אישור הגורם המוסמך לכך במועצה.

10. <u>דיווח ותחקור:</u>

א. עובד ידווח מידית, למנהל הממונה עליו ולמנהל מערכות המידע במועצה, על כל ידיעה או חשש בקשר להפרת האמור בנוהל זה או חריגה ממנו.

ב. מנהל האגף הממונה, ומנהל מערכות המידע במועצה, יבצעו תחקור של כל דיווח כנ"ל

ובעקבותיו יוציאו הנחיות והוראות למניעת הישנות חריגים.

11. <u>רשות כניסה למאגרי מידע:</u>

א. הגישה למאגרי מידע תתאפשר רק באמצעות קוד גישה וסיסמה שיאמתו את בלעדיות הגישה ע"י המורשים לצפות או להשתמש בו.

ב. **קוד הגישה בנוי משני רכיבים:**

1. שם משתמש הנקבע על- ידי מנהל הרשת, לדוגמה: ofra
2. **סיסמה הנקבעת על -ידי המשתמש:**

א) הסיסמה תהייה בנויה מלפחות 8 תווים;

ב) אין להקצות בסיסמה שני תווים זהים המופיעים ברצף;

ג) הסיסמה תהיה מורכבת מאותיות, מספרים וסימנים;

ד) המערכת מאלצת להחליף את הסיסמה מעת לעת באופן אוטומטי.

3. המנהל יקבע לגבי כל משתמש, את ההבחנה בין הרשאה לשלוף/לעיין במידע ובין

ההרשאה לרשום או לתקן מידע קיים.

4. עם העברת עובד לתפקיד אחר או פרישתו, יחליף המנהל מידית את שם המשתמש שהיה ידוע לעובד בתפקידו הקודם.

5. המנהל יקבע בתיאום עם המבקר את סוגי המאגרים שהגישה אליהם תאופשר לעובדי

הביקורת האחרים, למעט חומר רגיש שיהיה נגיש רק למבקר עצמו.

<u>תוכנת שליטה מרחוק:</u>

1. התקנת תוכנת השתלטות מרחוק מורשית רק בידיעתו ובאישורו מראש של מנהל מערכות המידע (מנמ"ר) במועצה וביצוע רק על ידו ובאישורו.

2. התקשרות מרחוק של עובדי קבלן או עובדי חברת חוץ בסיוע מודם חיוג ו/או בסיוע תוכנת השתלטות למחשב אשר נאגר בו מידע פנימי של המשרד או מחשב מחובר פיזית לרשת במשרד לצורך עבודות תחזוקה או כל צורך אחר - תתבצע אך ורק בפיקוח מלא של עובד המשרד. העובד יאשר את ה התקשרות (יפעיל אותה), ישגיח במהלכה ויוודא ניתוק מוחלט של הגורם החיצוני בתום ההתקשרות.

3. מקרים חריגים יטופלו לגופם ולגביהם יינתן אישור מראש ובכתב של מנהל מערכות המידע במועצה.

4. כל משתמש יישא באחריות אישית לגבי עמדת עבודתו, ינהג בכפוף להנחיות נוהל זה בכל הנוגע להתקשרות מרחוק וידווח לממונה על אבטחת מידע על תוכנות התקשרות אשר הותקנו שלא בהתאם לאישורים הנדרשים.

5. לצורך השתלטות על המחשב המארח חייבים להפעיל את אפשרויות האבטחה הקיימות בתוכנת השתלטות מרחוק:

א. שם משתמש;

ב. סיסמה בת 8 תווים לפחות, עפ"י ההנחיות שהוגדרו בסעיף 11 ב' מעלה;

ג. הפעלת אפשרות ניתוק לאחר חוסר פעילות של פרק זמן שייקבע ע"י הממונה על אבטחת מידע;

ד. הפעלת יומן LOG של פעילות המתבצעת באמצעות תוכנת ההשתלטות.

6. במידת הצורך ניתן להשתמש גם באפשרויות "Call Back" בהפעלת תכונות ההצפנה.

7. על המשתמש להודיע למנהל מערכות המידע במועצה על תופעות חריגות או בלתי מובנות שהתרחשו תוך כדי ו/או בסמוך לפעילות מורשית של התקנת תוכנות השתלטות מרחוק.

12. סיווג המידע:

א. המידע יסווג לארבע דרגות:

1. **גלוי -** מידע כללי שאיננו כולל נתונים אישיים על אדם פלוני או קבוצת אנשים פלונית, ואין בעצם גילויו כדי לפגוע באינטרס של פרט, של ציבור או של המועצה.

2. **רגיל -** מידע הכולל נתונים באמור לעיל, ומשום כך יש להגביל את הגישה אליו ואת תפוצתו לעובדי המועצה ועובדי המערכת בלבד.

3. **מוגבל -** מידע אשר רגישותו מבחינת פגיעת גילויו באנשים, קבוצת אנשים או אינטרס ציבורי עירוני מחייבת הגבלתו לידיעת אנשים הממלאים סוגי תפקידים רלוונטיים במועצה ונקיטת צעדי מגע פעילים למניעת הגעתו לידיעת אחרים.

4. רגיש - מידע אשר פגיעת גילויו קשה במיוחד, או מידע שהחוק הגביל את תפוצתו, הגישה למידע רגיש תהייה רק לאנשים נקובים ברשימה שמית שתיערך לגבי כל מסמך רגיש בידי המנהל, ותאושר על ידי ראש המועצה, או מי שהוסמך על ידיו לתת אישור כזה.

ב. המנהל יקבע לגבי כל מסמך או סוג מסמכים את דרגת החיסיון, ראש המועצה, מנכ"ל המועצה והיועץ המשפטי של המועצה יהיו מוסמכים להעלות/להוריד את דרגת החיסיון שקבע המנהל לגבי מסמך(ים).

ג. המנהל יקבע את תפוצתו של כל מסמך (מוגבל או רגיש).

ד. מסמך שייערך בדרגות **"מוגבל"** או **"רגיש"** יישא בראש כל עמוד את ציון דרגת החיסיון

שהוקצתה לו.

ה. המנהל ינהל רישום של המסמכים הרגישים. רישום זה עצמו יהיה רגיש.

13. ניתוב מידע וגריסת מסמכי מידע:

א. כל פלט ינותב אל הנמנעים שנקבעו בלבד, חומר מוגבל ורגיש יישלח במעטפות סגורות וחתומות ע"י חותמת "תוכן מסמך זה אסור לפרסום". החותמת תחצה את קו ההדבקה של המעטפה. המקבל חומר מוגבל/רגיש יבדוק את שלמות החותמת. נמצא מקום לחשד שהמעטפה נפתחה, יודיע על כך בכתב למנהל.

ב. חומר רגיש הנשלח על ידי שליח ילווה על ידי טופס שליחה. באין אפשרות לשלוח את החומר הרגיש בידי שליח, הוא יישלח בדואר רשום.

ג. פלט מוגבל או רגיש שנתקבל לשימוש, לא יימצא לעולם נגיש לאדם בלתי מוסמך, המשתמש בו לא ינטוש אותו אלא אם הוא נעול בכספת. נסתיים השימוש בו - הוא יועבר מייד לגריסה.

ד. פלט מוגבל או רגיש לא יצולם אלא ברשות המנהל ובאחריותו, התצלום דינו כדין מקור נוסף בכל הנוגע לשמירה עליו.

ה. לאחר שפלט מוגבל או רגיש בהעתק נוסף שמיוצר על ידי שימוש בנייר כימי – ייאספו גיליונות הנייר הכימי מייד לאחר צאתם מהמדפסת ויישלחו במשמורת לגריסה.

ו. בטרם שליחת חומר לגריסה, תיערך רשימת המסמכים הכלולים במשלוח. הרשימה תכלול ציון מספר העותקים של כל אחד מהמסמכים שנשלחו לגריסה.

ז. תהליך הגריסה יבוצע בתיאום עם הממונה על רשומות המועצה ובפיקוח מי שהמנהל מינהו לכך. על אדם זה לוודא שכל החומר שנמסר לגריסה עבר את התהליך. הוא לא ירשה ולא יניח לאיש להוציא דבר מהחומר שנמסר לגריסה ולא לעיין בו לפני הגריסה או במהלך התהליך.

14. כללי אבטחה פיזית של תחנת עבודה:

א. עובד היוצא מחדר עבודתו יסגור את תחנת העבודה בה הוא משתמש, ואם לא נוכח בחדר עובד אחר, ינעל את החדר.

ב. אין להשאיר ציוד מחשבים דולק/פועל לאחר שעות העבודה אלא על פי אישור הממונה על אבטחת המידע במועצה.

15. משמעת:

א. מנהל אבטחת המידע יערוך "דף מידע" שיכלול את עיקרי הוראות החוק ונהלים הנוגעים

למערכות מידע, לרבות:

1. את נוסחם של פרקים ב' עד ד' לחוק המחשבים, התשנ"ה – 1995

ב. דף המידע יעודכן תקופתית ויופץ לידיעת העובדים הנוגעים בדבר, לפחות אחת לחצי שנה. לדף המידע יצורף ספח שבו יאשר כל עובד בחתימתו כי הוא קרא והבין את תוכנו.

ג. כל עובד יידרש לחתום, עם כניסתו לעבודה על תצהיר סודיות (טופס 018-90) שדוגמתו בתוספת א' לנוהל.

ד. המעשים שלהלן ייחשבו לעבירה משמעתית, מבלי לפטור את עושיהם מתוצאותיהם בתחום הדין הכללי:

1. מסירת קוד לידי אדם אחר, זולת מה שמתחייב מהוראות כל דין.
2. שימוש בקוד של אדם אחר.
3. שימוש בקוד לכל מטרה שהיא, זולת עבודת העובד במערכת.
4. מסירת פלט לאדם לא מוסמך.
5. מסירת מידע כלשהו שהגיע לידיעת עובד המערכת במהלך עבודתו.

16. תוספת א'

<u>תצהיר סודיות</u>

אני, שם משפחה _____ שם פרטי _____

מספר זהות _____

העובד(ת) באגף/מחלקה _____ של מועצה

מקומית עין מאהל מצהיר(ה) בזאת לאמור;

1. הוסברו לי -

א. " הוראות "חוק הגנת הפרטיות תשמ"א - 1981 " והוראות "חוק המחשבים, התשנ"ה 1991- והאחריות המוטלת על ידי הוראותיו בקשר לעבודתי במועצה.

ב. הוראות הנוהל של המועצה בדבר אבטחת המידע .

2. אני מתחייב(ת) לשמור בסוד את כל אשר הגיע או יגיע לידיעתי במהלך מילוי תפקידי. לא אמסור כל מידע או כל מסמך שהגיע או שיגיע לידי למי שלא הוסמך כדין לקבלו מידי.

3. התחייבותי זו תישאר בתוקפה גם לאחר סיום עבודתי במועצה.

ולראיה באתי על החתום

תאריך _____ חתימת העובד(ת) _____

תפוצה: מקור - לתיק אישי; העתק - לעובד.

חתימה + חותמת יועץ המשפטי: _____