נוהל הנחיות אבטחת מידע לעובדים

מעקב אחר תיקוני מסמכים

תאריך	שם העורך	שם המאשר	גרסה	שינוי
01.06.2021			1	יצירת המסמך
01.11.2021			2	עדכון
01.02.2023			3	עדכון
30.01.2025	צביקה		3	עדכון
11.1.2026	**מעיין בר**	**מנכ"ל + מנמ"ר**	**4**	**עדכון**

1. <u>כללי</u>

1.1 אבטחת מידע והגנת הפרטיות הנה מרכיב מרכזי בשימוש השוטף במערכות טכנולוגיית המידע בהיבטים הטכנולוגיים, הארגוניים ובהיבטי כוח האדם ברמות השונות. לעובדי מועצה אזורית גולן ותאגידיה (להלן מועצה אזורית גולן), מנהלים ועובדים, השפעה מכריעה על רמת אבטחת המידע במועצה, וזאת על בסיס מחויבותם האישית למילוי קפדני של הוראות ונהלים בנושאי אבטחת המידע והגנת הפרטיות כפי שייגזרו ממדיניות המועצה.

1.2 במועצה האזורית גולן נעשה שימוש בעשרות מחשבים אישיים ואמצעים דיגיטליים שונים, לרבות טלפונים חכמים, טאבלטים, מחשבים ניידים ואמצעי קצה נוספים, המשמשים כתחנות קצה לצורך עבודה והתחברות לנכסי המידע של המועצה.
אמצעים אלה, מעצם אופיים וניידותם, עלולים להוות רמת סיכון גבוהה יותר לאבטחת המידע בהשוואה לתחנות קצה נייחות וסטנדרטיות, ועל כן מחייבים התייחסות ייעודית והחלת בקרות מתאימות.

1.3 הפעולות המבוצעות בעמדות העבודה השונות של כל משתמש ובחשבון המשתמש, <u>מנוטרות ומתועדות באמצעות מערכת הניטור של המועצה.</u>

1.4 תחנת הקצה מהווה את הכניסה לשרתי המועצה ועל כן טומנת בחובה סיכונים אבטחתיים פוטנציאליים רבים. נוהל זה מסייע למשתמשים למזער את אותם סיכונים קיימים.

1.5 בסביבת העבודה מסמכים רבים. על העובדים למנוע את השארתם חשופים ולא מוגנים, דבר העלול לגרום לחשיפתם לגורם לא רצוי, תהליך אשר יפגע במועצה אזורית גולן, בבעלותה ובשמה הטוב.

2. <u>המטרה</u>

2.1 הנוהל מסדיר את נושאי אבטחת המידע בפעילות המשתמשים השונים בתחנות הקצה השונות במועצה אזורית גולן.

2.2 הנוהל קובע את הכללים לגבי שמירת מחשבים ניחים וניידים, וכלל האמצעים הדיגיטליים המשמשים להתחברות לנכסי המידע בתוך משרדי מועצה אזורית גולן, או כאשר המשתמש מוציא אותם מחוץ לכותלי המועצה.

2.3 הנוהל קובע את הכללים לגבי שמירת מסמכי נייר בתוך משרדי מועצה אזורית גולן, או כאשר המשתמש מוציא אותם באישור מחוץ לכותלי המועצה.

2.4 הנוהל מסדיר את המותר והאסור בשימוש בדואר אלקטרוני ובגלישה ברשת האינטרנט.

3. <u>הגדרות</u>

3.1 **צרופה (Attachment)** – קובץ מצורף לתכתובת דואר אלקטרוני.

3.2 **משתמש קצה-** עובד מועצה אזורית גולן, עובד חיצוני המועסק ע"י מועצה אזורית גולן אשר משתמש בתחנת קצה ומתחבר למערכות המידע של מועצה אזורית גולן.

3.3 **סביבת עבודה** – תחנת הקצה בה משתמש עובד מועצה אזורית גולן, השולחן שלו והאזור הסמוך להם.

3.4 **תחנת קצה –** מחשב אישי או אביזר דיגיטלי אשר בו עושה שימוש משתמש הקצה**.**

3.5 **וירוס מחשבים –** תוכנה המפותחת ומופצת במטרה לגרום נזק במערכות מחשב, שרתים או תחנות קצה.

3.6 **תוכנת אנטי וירוס** – תוכנה אשר תפקידה לאתר ולהשמיד תוכנות המכילות וירוסי מחשבים ולהתריע כל כך.

3.7 **נעילת מסך –** תוכנה המופעלת בתחנת הקצה לאחר זמן מוגדר של אי פעילות, או באופן יזום ע"י משתמש הקצה. החזרה לעבודה הרגילה מתבצעת באמצעות פעילות בתחנת הקצה ע"י הקלדת סיסמא.

3.8 **קוד משתמש –** רצף תווים אישי גלוי המהווה את שמו / כינויו של המשתמש במערכת ממוחשבת אחת או יותר.

3.9 **סיסמה –** רצף תווים אישי סודי המוקלד לבקשת המערכות הממוחשבות והמהווה אמצעי לאימות זיהוי המשתמש.

3.10 **סיסמא ראשונית -** סיסמא המחויבת בהחלפה בעת הקלדתה למערכת.

3.11 **דואר אלקטרוני** – רשת דואר, המשמשת להעברת מסרים וקבצים ברשת האינטרנט.

4. <u>השיטה</u>

4.1 מדיניות האבטחה שהנך נדרש לעמוד בה כמשתמש קצה בסביבת העבודה כוללת את הנושאים הבאים:

- הגדרת משתמשים וסיסמאות גישה
- אחסון מידע ותוכנות בתחנות הקצה
- קבלת מידע מגורם חיצוני למועצה
- שימוש בדואר אלקטרוני
- הסדרת הגלישה ברשת האינטרנט
- אנטי וירוס
- אבטחה פיזית
- טיפול במסמכי נייר
- אבטחת מחשבים ניידים, Disk On Key או מכשירי טלפון ניידים ותחנות קצה למיניהן
- אבטחת מסמכים במשרדי מועצה אזורית גולן והמוצאים ממשרדי מועצה אזורית גולן
- הוראות כלליות

4.2 ניהול סיסמאות גישה

4.2.1 כמשתמש במועצה אזורית גולן, תקבל שם משתמש ייחודי (Username), אשר יאפשר לך לקבל הרשאות גישה למערכת. בנוסף תקבל סיסמה ראשונית אישית חסויה, המאפשרת כניסה (Login) לרשת המועצה, אותה עליך להחליף לאחר הכניסה הראשונית.

4.2.2 סיסמא זו הינה אישית, ואותה קבלת לשימושך האישי בלבד, לשם ביצוע עבודתך במועצה אזורית גולן. עליך לשמור את הסיסמא במקום חסוי ובטוח, שאינו חשוף לעיניים זרות. אל תעביר סיסמא זו לגורם כלשהו, כולל מנהל, גורם טכני או עובד אחר, ואל תרשום אותה במקום סמוך לתחנת הקצה, או בכל מקום אחר אשר עלול לחשוף אותה לאחר, או על מדיה כלשהי.

4.2.3 את הסיסמה עליך להחליף בהתאם למדיניות אבטחת המידע.

4.2.4 לאחר זמן מסוים, המוגדר ע"י המערכת, אשר בו לא תהיה פעילות בתחנת הקצה, תינעל התחנה ע"י שומר מסך. על מנת לשחרר את שומר המסך ולחזור לעבודה, עליך להקיש את סיסמת הכניסה לרשת המועצה. כמו כן, עליך לנעול בעצמך את התחנה ע"י הפעלת שומר המסך עם עזבך את מקומך.

4.2.5 במידה ושכחת את הסיסמא, או אם הנך סבור שהיא הגיעה לאחר, עליך לידע את מנהלך, ולפנות למנהל מחלקת מערכות מידע ומחשוב על מנת לקבל סיסמה זמנית חדשה, אותה תחליף עם הכניסה המחודשת למערכת.

4.2.6 חל איסור להשתמש בפרטי זיהוי אישיים של משתמש אחר במועצה, בין היתר לצורך עקיפת מנגנון הרשאות. במידה והנך סבור כי נדרשת הרשאה למילוי תפקידך במועצה, עליך לפנות למנהלך.

4.2.7 במידה ונמסרו לך סיסמא ושם משתמש שאינם שלך, אין להשתמש בהם ויש לדווח מידית למנהל מחלקת מערכות מידע ומחשוב.

4.3 מדיניות סיסמאות

4.3.1 אורך סיסמה מינימאלי – 8 תווים ובהתאם לנוהל סיסמאות.

4.3.2 מורכבות הסיסמה - שילוב של אותיות באנגלית, ספרות וסימן.

4.3.3 פרק זמן להחלפת הסיסמה – 180 ימים. מספר ימים לפני תוקפה של הסיסמה, כל משתמש יקבל התראה ממערכת המחשוב להחלפת הסיסמה. אל לך להתעלם מהודעה זו, עליך להחליף את הסיסמה עפ"י מדיניות הסיסמאות במועצה המפורטת לעיל.

4.4 קווים מנחים למורכבות סיסמה

4.4.1 הסיסמאות משמשות לבקרת גישה למערכות שונות במועצה. השימושים יכולים להיות – גישה לרשת, למערכת תוכנה, לדואר אלקטרוני לשומר מסך ולמרכיבים אחרים במערכות המידע של המעצה. כאשר בוחרים סיסמא חשוב שתהיה קשה לפיענוח. להלן דוגמאות הממחישות מהי סיסמא קלה וקשה לפיענוח.

4.4.2 סיסמה קלה לפענוח:

- מכילה פחות משבעה תווים.
- הסיסמא היא מילה שניתן למצוא במילון.
- הסיסמא היא מילה קצרה אשר נמצאת בשימוש שיגרתי כגון: שם פרטי או משפחה, שמות של בני משפחה, חיות מחמד, חברים, דמויות מוכרות, מונחי מחשב, פקודות, שמות חברות או מוצרים, ימי הולדת, כתובות, מספרי טלפון או מידע אישי אחר.
- הסיסמא היא תבנית של מספר או אותיות חוזרות או בעלות משמעות כגון: aaabbb, qwerty, 12223344, zywvuts וכן הלאה.

4.4.3 סיסמה קשה לפיצוח:

✓ מכילה גם אותיות (אנגלית) גדולות וגם קטנות.

- ✓ באורך 9 תווים ומעלה.
- ✓ הסיסמא היא לא מילה בשפה כלשהיא או בסלנג, לא מבוססת על נתונים אישיים, שמות משפחה וכו'.

4.5 קווים מנחים להגנה על הסיסמה

4.5.1 אין לגלות את הסיסמא לאיש. כולל מזכירות ומנהלים.

4.5.2 אין לרשום סיסמאות על פתקים ולהשאירן במקומות גלויים (כמו מסך המחשב, מתחת למקלדת, שולחן העבודה , בטלפון הנייד באופן לא מוצפן וכו').

4.5.3 אם יש חשד לכך שהסיסמא נחשפה בדרך כלשהיא, יש לדווח על כך למנהל אבטחת המידע ולשנות את כל הסיסמאות הנדרשות.

4.5.4 במידה והינך נכנס לסביבת העבודה באמצעות דפדפן מתחנת קצה שאינה שלך, באחריותך לא לשמור את הסיסמא בכניסה ולוודא התנתקות בסיום הפעילות.

4.6 כללי עשה ואל תעשה

4.6.1 אל תחשוף את הסיסמא שלך בטלפון לאף אחד .

4.6.2 אל תחשוף את הסיסמא שלך בדואר אלקטרוני.

4.6.3 אל תדבר על הסיסמא בנוכחות אחרים.

4.6.4 אל תחשוף רמזים לגבי מבנה הסיסמא.

4.6.5 אל תחשוף סיסמא בשאלונים.

4.6.6 אל תגלה את הסיסמא לבני משפחה .

4.6.7 אל תיתן את סיסמתך לחברים לעבודה בזמן שאתה בחופש.

4.6.8 אל תשתמש באותה סיסמא גם בעבודה וגם ביישומים פרטיים.

4.6.9 במידה והנך נדרש להעביר את הפרטים, אין לשלוח את שם המשתמש והסיסמה יחד ובאותה מדיה.

4.7 אחסון מידע ותוכנות בתחנות הקצה

4.7.1 במידה והינך נדרש להוסיף תוכנות לתחנת הקצה שבה הינך עובד, פנה לאישור מנהל מערכות מידע.

4.7.2 במידה וגילית תוכנה שמקורה אינו ברור לך, פנה למנהל מערכות מידע.

4.8 העברת מידע או קבלת מידע מגורם חיצוני למועצה

4.8.1 השימוש במחשבי המועצה ייעשה בכפוף לנהלי המועצה ובהתאם לחוקי מדינת ישראל.

4.8.2 בכל קבלה או העברת מידע מגורם חיצוני למועצה, בין אם בצורה דיגיטלית ובין בצורה פיזית, יש לוודא כי הגורם הינו מוכר ואמין ואין כוונת זדון בפעולתו, כגון התחזות, ריגול וכדומה. ועפ"י החלטות של הוועדה להעברה/קבלה מידע בין גופים ציבוריים של המועצה אשר תדון בכל בקשה בנושא.

4.8.3 עליך להימנע מלהגיב או ללחוץ על כפתורי גישה לאתרים הנשלחים מכתובות דואר לא ידועות. במידה ולחצת על הקישור, עליך להימנע ממסירת פרטים אישיים לגבי סיסמתך או שם המשתמש שלך ואל לך להקלידם בשום מקרה כתוצאה מהפניה ממכתב אלקטרוני או מאתר אינטרנט.

4.8.4 במידה והעברת המידע בוצעה באמצעים דיגיטליים, עליך לוודא אי קיום וירוסים בעזרת תוכנת אנטי וירוס.

4.8.5 אין להעביר מידע עסקי או חסוי של המועצה לכל גורם חיצוני, ללא קבלת אישור ממונה אבטחת מידע או בא כוחו.

4.8.6 הודעות בתחום מערכות מידע והמחשוב, יופקו בדואר פנימי המלווה בחתימה ו/או ציון פרטי מנהל מערכות מידע ויישלחו מכתובת הדוא"ל שלו או של מחלקת מערכות מידע של המועצה באמצעות כתובת דוא"ל - taln@megolan.org.il.

4.9 שימוש בדואר אלקטרוני ובתוכנות להעברת מסרים/קבצים (כולל ווטסאפ)

4.9.1 כעובד מועצה אזורית גולן תוגדר לך כתובת דואר אלקטרוני חיצונית כלפי כל העולם והינה בבעלות בלעדית של מועצה אזורית גולן.

4.9.2 תכתובות הדואר האלקטרוני במועצה מוגנות באמצעות מערכות למניעת קוד זדוני ומתועדות.

4.9.3 הקפד כי השימוש בדואר האלקטרוני יהיה לשימוש עסקי פנימי של מועצה אזורית גולן בלבד, השימוש לא יכלול תכתובות כגון מכתבי שרשרת, מכתבי פניה לציבור, פורנוגרפיה, מכתבי הסתה, קוד עוין, השתתפות בעצומות באינטרנט, הזדהות פוליטית, פרסומות ומודעות מכל סוג שהוא וכדומה אשר מקורם מחוץ למועצה אזורית גולן ואינו קשור לפעילות המועצה.

4.9.4 כמו כן, אל תעביר קבצים כגון קבצי ריצה, מוצרי תוכנה, תמונות, קבצי וידאו אודיו, קבצי פונטים, ועדכוני תוכנות אשר מקורם איננו במועצה אזורית גולן ובכללם קבצים שמקורם ברשת האינטרנט למחשב המחובר לרשת מועצה אזורית גולן. במידת הצורך פנה לקבלת מענה מצוות מערכות מידע ומחשוב.

4.9.5 אין להעביר מידע בדואר אלקטרוני חיצוני או באופן דיגיטלי כלשהו ובו תכנים הכוללים מידע רגיש, אלא לאחר הצפנת הקובץ לפחות.

4.9.6 אין לפתוח דואר אלקטרוני או צרופה ממקור בלתי מזוהה, או שתוכן ההודעה, שפתה או הקבצים המצורפים אליה אינם תואמים את הקשרם העסקי ו/או קבצים מצורפים המבקשים לבצע פעילות כלשהי לאיפוס סיסמה, או הזדהות אחרת, מחשש לתוכן זדוני. גם אם בטעות לחצתם על קישורם כאלה, אין למסור מידע אישי כלשהו ו/או לאשר החלפת סיסמה.

4.9.7 אין לעשות שימוש בהעברה אוטומטית של תיבת הדוא"ל של המועצה לדוא"ל אחר.

4.9.8 בעת התחברות לדוא"ל המועצה מהטלפון החכם או אמצעי דיגיטלי אחר , עליך לוודא קיום הבקרות הבאות:

- ✓ התקנת מנגנון הזדהות לתיבת הדואר האלקטרוני.
- ✓ התקנת שומר מסך עם סיסמה.
- ✓ התקנת תוכנה המונעת חדירת וירוסים (להלן: "אנטי וירוס"), וכי תוכנה זו מעודכנת ומתעדכנת באופן אוטומטי עם כל עדכון המופץ ע"י בית התוכנה.
- ✓ במידה ומתקבלת הודעת דוא"ל בלתי מזוהה או חשודה או הודעת שגיאה ו/או נצפתה התנהגות חשודה בדפדפן האינטרנט במהלך הגלישה, עליך לדווח על כך באופן מידי למנהל מערכות מידע.

4.10 הסדרת הגלישה ברשת האינטרנט

4.10.1 חל איסור מוחלט על הורדה והתקנת תוכנות מהאינטרנט.

4.10.2 בכל מקרה, דע כי חל איסור מוחלט על גלישה לאתרים הבאים:

- אתרים פורנוגרפיים
- אתרי הימורים
- חדרי שיחה פרטיים (צ'טים)
- אתרי שיתוף קבצים וכן אתרים המאפשרים הורדת תוכנות בלתי חוקיות, וזאת מחשש לחשיפת מועצה אזורית גולן לתביעות משפטיות.
- אתרים הנוגעים במידע הקשור לפריצה למערכות מחשב, וזאת מחשש למלכוד הגישה לאתר.
- אתרים בעלי תוכן בלתי נאות, העשוי לפגוע בשמה הטוב של מועצה אזורית גולן.

4.11 אנטי וירוס

4.11.1 בתחנת הקצה בה הנך משתמש, הותקנה תוכנת אנטי וירוס. במידה והתוכנה מצאה קבצים נגועים בתחנת הקצה, או שהתקבלה הודעה על אי-פעילות של התוכנה מסיבה כלשהי, עליך לעדכן את מנהלך, ולפנות למנהל הרשת או למנהל אבטחת המידע.

4.12 עמדת עבודה

4.12.1 הפעולות המבוצעות בעמדת העבודה של כל משתמש ובחשבון המשתמש, מנוטרות ומתועדות באמצעות מערכת הניטור של המועצה.

4.12.2 בעת עזיבת עמדת העבודה, עליך לנעול באופן יזום את עמדת העבודה וכן לסגור את דלתות המשרד.

4.12.3 בסוף כל יום עבודה, עליך לכבות את תחנת הקצה. במידה והנך נדרש להריץ פקודות עבודה ארוכות, ודא את נעילת המסך לפני יציאתך מהמשרד.

4.12.4 אין לחבר מחשב שאינו מחשב המועצה לרשת המקומית ואין לבצע כל שינוי בעמדת העבודה באורח עצמאי, כולל התקנת תוכנות, גם במקרים בהם התוכנה מוצעת חינם. במידת הצורך, יש לקבל אישור ממנהל מערכות מידע.

4.12.5 אין להוסיף רכיבי תקשורת, כגון מודם, לתחנת הקצה.

4.12.6 אין להשאיר במשרד או באופן גלוי מדיה נתיקה, כוננים שליפים, תקליטורים המכילים מידע רגיש בסוף יום העבודה.

4.12.7 אין לשמור קבצים באופן מקומי על עמדת העבודה אשר נדרשים לצורך ביצוע העבודה ואשר לא ישמרו באמצעות גיבוים במקרה של תקלות ואירועים שונים. יש לבצע שמירה על כונני הרשת בלבד. מידע זה אינו נשמר ולא יגובה בכל דרך ויאבד עם כל תקלה במחשב.

4.12.8 אם קיים חשד בדבר שימוש לא מורשה בתחנת הקצה , עליך לדווח **מידית** למנהלך ו-מנהל מערכות מידע.

4.13 טיפול במסמכי נייר

4.13.1 חל איסור על הוצאת מידע השייך באופן כלשהו למועצה. במידה ונדרש להוציא מידע, עליך לפנות למנהלך או למנהל מערכות מידע לצורך קבלת אישור מסודר והנחיות לאופן הוצאת המידע הרגיש.

4.13.2 בתום יום העבודה או בעת עזיבת מקום העבודה לזמן ארוך, יש להשאיר את סביבת העבודה כשמסמכים המכילים מידע רגיש מתויקים או מסודרים במקומם הראוי, ולנעול את החדר / ארונות / מגירות. אין להשאיר מסמכים בהם מופיע מידע רגיש חשופים בסביבת העבודה שלך. עליך להכניס מסמכים אלו למגירה או לארון, ולנעול אותם במפתח שימצא ברשותך.

4.13.3 מסמכים אשר נשלחו להדפסה או שצולמו או שנשלחו בפקס מהמדפסת / מכונת צילום / פקס, יאספו מיד בתום השליחה על ידי השולח. עליך לוודא כי המסמך לא יילקח (בשוגג או בזדון) ע"י אדם אחר.

4.13.4 יש לגרוס מסמכים המכילים מידע רגיש בתום השימוש בהם.

4.13.5 אם אבד מסמך המכיל מידע רגיש, יש לדווח מידית למנהלך.

4.14 אבטחת מחשבים ניידים,Disk On Key אביזרים דיגיטליים או מכשירי טלפון ניידים

4.14.1 חל איסור מוחלט על חיבור התקנים חיצוניים לעמדות העבודה, לרבות התקני USB, DOK, מודמים, נגני מדיה, טלפונים סלולריים וכל אמצעי אחסון או תקשורת אחר, לרבות באמצעות תווך תקשורת אלחוטי (כגון: Wireless, Bluetooth וכיו"ב). חריגה מהוראה זו תתאפשר אך ורק באישור מראש ובכתב של מנהל מערכות המידע.

4.14.2 אין לחבר מחשבים ניידים שלא בבעלות מועצה אזורית גולן לרשת המקומית ע"י חיבור כבל פיזי לרשת המועצה .

4.14.3 שימוש באמצעים דיגיטליים אלה והעברת קבצים דרכם, מחייבת אישורים מיוחדים של אבטחת מידע וכן בדיקת הקבצים בתוכנת אנטי וירוס לאי קיום וירוסים לפני העברתם.

4.14.4 יש לוודא כי אמצעי המחשוב הנייד נמצא בהשגחתך בכל עת. אין להשאיר אמצעי מחשוב נייד במכונית ללא השגחה. השימוש באמצעי המחשוב הנייד מוקצה לעובד במועצה בלבד.

4.14.5 בעת עזיבת הבית ללא אמצעי המחשוב הנייד, יש לכבות ולאחסן את אמצעי המחשוב הנייד במקום שאינו חשוף.

4.14.6 עליך לוודא נעילת המחשב האישי עם סיסמה אישית, באמצעות שומר מסך.

4.14.7 אל תעתיק תוכנות וקבצים למחשב, אלא בתיאום עם מנהל מערכות מידע ומחשוב או מנהל אבטחת המידע.

4.14.8 באם המחשב או כל אמצעי דיגיטלי שברשותך אבד, הודע למנהלך ולמנהל מערכות המידע **באופן מיידי.**

4.14.9 ככל שקיים צורך עסקי מוצדק, ובאישור המנהל הישיר ומנהל מערכות מידע, תתאפשר גישה למידע רגיש באמצעות טלפון חכם אך ורק באמצעות שירותי הענן הארגוניים המאושרים (כגון OneDrive ו-SharePoint), וזאת ללא שמירת המידע על גבי המכשיר עצמו. הגישה תתבצע בהתאם לאמצעי אבטחת המידע שייקבעו וינוהלו על-ידי מנהל מערכות מידע, לרבות מנגנוני הזדהות, הצפנה, ניהול הרשאות ובקרות מתאימות.

4.14.10 עליך לשמור על הטלפון החכם והמידע האגור בו, בדגש על שמירתו בטווח עין גם במהלך נסיעה ובמקום בטוח בבית.

4.14.11 עליך לוודא כי על הטלפון החכם יותקנו הבקרות הבאות:

- ✓ הגדרת סנכרון עדכוני גרסה ואבטחה.
- ✓ קיומו של מנגנון הזדהות של שם משתמש וסיסמא.
- ✓ עדכוני חתימות וגרסאות לפי דרישת היצרן.
- ✓ שומר מסך לאחר X זמן של חוסר פעילות
- ✓ הגדרת גישה מהטלפון החכם שלי לשירותי הדוא"ל של המועצה.

4.15 הוראות כלליות

4.15.1 יש להפעיל שיקול דעת לפני כל פעולה במחשב העלולה לגרום נזק.

4.15.2 זכרו, אם יש ספק – אין ספק! עדיף להתייעץ מראש ולשאול טרם ביצוע הפעולה.

4.15.3 יש לבחור סיסמא "קלה לזיכרון וקשה לפיצוח" בהתאם למדיניות הסיסמאות של המועצה.

4.15.4 טלפון חכם ואביזר דיגיטלי הינו מחשב לכל דבר ועניין ולכן עליך לנהוג בו בזהירות כפי שנוהגים במחשב בכפוף לנוהל זה.

4.15.5 אין ללחוץ על קישורים המגיעים בדוא"ל;

4.15.6 אין להשאיר את סיסמתכם על פתק בסביבת מחשב;

4.15.7 שם משתמש וסיסמה הינם אישיים, חסויים ואינם ניתנים להעברה. לעולם אין להעביר מידע הכולל פרטים מזהים של סיסמתכם לגורם בלתי מורשה ובוודאי שלא בדוא"ל או בטלפון.

4.15.8 יש להיזהר מהודעות או חלונות קופצים (Pop Ups), ולא ללחוץ על קישורים בהודעות מסוג זה.

4.15.9 נגישותם של עובדי חברות חיצוניות, המספקות שירותי מחשוב ותמיכה למועצה אזורית גולן, תיעשה בפיקוח ובתיאום עם מנהל מערכות המידע, ובליווי מלא.

4.15.10 במידה והנך צפוי להיעדר מעל 5 ימי עבודה רצופים, עליך לבצע את הפעולות הבאות:

- ✓ הודעה למנהלך הישיר.
- ✓ וידוא כיבוי תחנת הקצה.
- ✓ הכנסת כל מסמכי העבודה לארון, מגירה או אמצעי אחסון אחר שתמצא לנכון.

5. אחריות

על כל משתמשי הקצה במועצה אזורית גולן מוטלת האחריות לנהוג על פי כללי אבטחת המידע אשר נקבעו בנוהל זה, לנהוג בהתאם להוראותיו, ולדווח למנהל מערכות המידע על כל חריגת אבטחה בה נתקלו במהלך עבודתם השוטפת, על מנת לאפשר סביבה מאובטחת ככל הניתן למידע במועצה אזורית גולן.

במקרה של חשש לאירוע שעשוי להוות אירוע של אבטחת מידע וסייבר, כגון" חדירה לרשת, נעילת קבצים, השחתת אתר, דלף מידע בדוא"ל, חשיפת סיסמאות גישה, גישת גורמים לא מורשים משרתי הרשת ועוד, מחובתך לדווח מידית למנהל מערכות מידע ולמנהלך.

6. תחולה ותוקף

באחריות ממונה אבטחת מידע לעדכן נוהל זה והוא תקף מעת פרסומו.

הצהרת העובד

קראתי והבנתי את האמור בהתחייבות זו ואני חותם/ת עליה מרצוני:

שם העובד							**מס ת.ז**		

תאריך	**חתימת העובד**

הצהרת המעסיק (נציג מוסמך מטעם הארגון)

אני, הח"מ, מאשר/ת כי מר/גב'_____ קרא/ה את הצהרה זו בנוכחותי, וחתם/ה עליה רק לאחר שהצהיר/ה בפני כי הבין/ה את הכתוב בה ואת המשמעויות במקרה של הפרתה, והוא/היא מתחייב/ת לאמור בה מרצונו/ה.

שם המעסיק	**חתימה**	**תאריך**