



מדיניות אבטחת מידע

אוגדן נהלי אבטחת
מידע

מהדורה : 3.0

מס' נוהל : א-5.1.1

תפקיד : יועץ חיצוני

ערך : עזרא דיין

תפקיד : מנכ"לית
המועצה

אישר : ענת מור

עמוד 1 מתוך 17

עודכן בתאריך : 1/9/2020

מועצה אזורית הגלבוע

נוהל A. 5.1.1 – מדיניות אבטחת מידע

מהדורות מסמך :

מס"ד	תאריך	עודכן ע"י	תיאור השינוי
1	30.7.2019	עזרא דיין	גרסה ראשונה

בקרת מסמך :

גורם	שם	תפקיד	תאריך אישור	חתימה
כתב	עזרא דיין	ממונה אבטחת מידע המועצה	30/4/21	עזרא דיין
אישר	רון בגים	מנמ"ר		
אישרה	ענת מור	מנכ"לית		
מפרסם	עובד נור	ראש מועצה		

מדיניות אבטחת מידע



מועצה אזורית הגלבוע

אוגדן נהלי אבטחת
מידע

מהדורה : 3.0

מס' נוהל : א-5.1.1

תפקיד : יועץ חיצוני

ערך : עזרא דיין

תפקיד : מנכ"לית
המועצה

אישר : ענת מור

עמוד 2 מתוך 17

עודכן בתאריך : 1/9/2020

1. כללי :

1.1 מטרת הנוהל להגדיר את מדיניות המועצה האזורית הגלבוע (להלן : "המועצה") בנושא אבטחת מידע ואת פעילויות המחשוב למניעה, תחזוקה וניהול משימות אבטחת מידע.
1.2 תחום אבטחת מידע בארגון הינו נרחב ורב גוני. תחום זה מרכז את המשימות שמבוצעות על מנת להבטיח שימוש ראוי במשאבי המחשוב של המועצה, שמירה על אמינות המידע, שמירה על זמינותו, מניעת רוגלות, חדירות לא מורשות ווירוסים למיניהם, הדרכת המשתמשים לשימוש נכון ומאובטח בצידוד המחשוב, המידע ואמצעי האחסון במועצה.

2. מטרות וייעוד הנוהל :

2.1 הנוהל מיועד למשתמשי המועצה, ספק מתן שירותי מחשוב, ספקי מערכות המחשוב ומערכות המידע של המועצה, משתמשי המועצה וכל גורם המחזיק במידע עירוני. הנוהל מחייב כל גורם המטפל בשרתים במועצה ו/או בתחנות העבודה ו/או במאגרי המידע.
2.2 הנוהל מציג תיאור הפעולות שיש לבצע בתחום אבטחת מידע לרבות בתחום תשתית, ניהול הרשאות וסיסמאות, טיפול באירועים, הפצת מדיניות ומניעה.

3. תיאור התהליך :

3.1. התקנת תוכנות לא מאושרות

- 3.1.1 התקנת תוכנה לא מאושרת תכלול בין היתר את הרכיבים הבאים ;
 - תוכנה לא חוקית, תוכנה מועתקת ללא הרשאה או שנרכשה באופן אחר שלא בהתאם לתנאי הספק המורשה ולהנחיות המועצה.
 - כל תוכנה אחרת (גם אם נרכשה כחוק ע"י העובד באופן פרטי) המותקנת ללא קבלת אישור מנמ"ר המועצה.
- 3.1.2 השימוש בתוכנה לא מאושרת עלול לגרום לשיבושים במערכות המחשוב של המועצה.
- 3.1.3 כל משתמשי תחנות עבודה שבמחשבם קיימת או שהותקנה תוכנה לא מאושרת מחויבים להודיע על כך לספק המחשוב ו/או למנמ"ר המועצה באמצעות הדוא"ל. היה ועובד מצא שתוכנה לא מאושרת כלשהי הינה חיונית לעבודתו השוטפת עליו

מדיניות אבטחת מידע



אוגדן נהלי אבטחת
מידע

מהדורה : 3.0

מס' נוהל : א-5.1.1

תפקיד : יועץ חיצוני

ערך : עזרא דיין

תפקיד : מנכ"לית
המועצה

אישר : ענת מור

עמוד 3 מתוך 17

עודכן בתאריך : 1/9/2020

לפנות בדוא"ל למנמ"ר המועצה – אשר יבצע הסרה, או שתבוצע רכישה באופן חוקי ע"י המועצה, או שהתוכנה תקבל אישור התקנה ושימוש מן הגורמים המוסמכים.
3.1.4. במסגרת פעילות האחזקה השוטפת במחשבי המועצה יהיה טכנאי המחשוב רשאים למחוק כל תוכנה לא מאושרת בעת טיפולם בחומרה או בתוכנה.
3.1.5. האחריות לגבי השימוש בתוכנה לא מאושרת תהיה על המשתמש באופן אישי, גם כלפי המועצה וגם כלפי גורמים חיצוניים.

3.2. התקנת תוכנות המורדות מהאינטרנט

התקנת תוכנות כאלה במחשבי המועצה אסורה גם אם התוכנה מסוג Shareware ללא אישור מנמ"ר המועצה.

3.3. שימוש בדוא"ל של המועצה

3.3.1. שימוש בדואר אלקטרוני שלא לצורכי עבודה :
שרותי הדואר האלקטרוני הינם לצורכי עבודה בלבד. למניעת דלף מידע אין להשתמש בשירותי הדואר האלקטרוני להעברת מידע שלא לצרכי העבודה.
3.3.2. במקרים בהם נתקל עובד ו/או מנהל בחשד לשימוש שלא לפי הנחיות אלו עליו לפנות למנמ"ר המועצה.
3.3.3. קבלת דבר דואר מגורם לא ידוע :
במקרה בו משתמש מקבל דואר אלקטרוני עם צרופה מגורם לא ידוע עליו למחוק את ההודעה כדי למנוע העברת וירוסים וסוסים טרויאניים לתוך מחשבי המועצה כמו כן עליו להודיע מיידית טלפונית למנמ"ר המועצה.
3.3.4. שימוש בדואר אלקטרוני פרטי :
על העובדים להשתמש בשירותי הדואר האלקטרוני של המועצה בלבד. תתבצע חסימה מלאה של שימוש בשירותי דוא"ל פרטיים חיצוניים.
3.3.5. המעסיק ראשי לקיים פעולות למניעה וחסימה של וירוסים או מידע רגיש מלצאת החוצה- לכן, יש ביכולתו לבצע במייל המקצועי של העובד מעקב וגיבוי של נתוני התוכן ותקשורת של תכתובות המייל כחלק מפעולות הניטור הנדרשות.

מדיניות אבטחת מידע



אוגדן נהלי אבטחת
מידע

מהדורה : 3.0

מס' נוהל : א-5.1.1

תפקיד : יועץ חיצוני

ערך : עזרא דיין

תפקיד : מנכ"לית
המועצה

אישר : ענת מור

עמוד 4 מתוך 17

עודכן בתאריך : 1/9/2020

3.3.6. טיפול בספאם

3.3.6.1 מערכת סינון דואר אלקטרוני מנטרת באופן רציף כל העברת מידע מהמועצה ואליה בדואר אלקטרוני ומאתרת מידע מסוג ספאם ויכולה לחסום אותו.

3.3.6.2 עם גילוי אירוע, מנמ"ר המועצה, יבדוק את נתוני האירוע על מנת לברר את הסיבה לחסימת ההעברה.

3.3.6.3 המערכת מבטלת את העברת המידע האסור ומבצעת את הפעולות הבאות :

- העברת הודעת חסימה למנמ"ר המועצה בדוא"ל.
- רישום לוג של האירוע במערכת סינון הדואר
- על כל אירוע של ניסיון להעברת מידע שנחסם ע"י מערכת סינון דואר אלקטרוני יבדוק טכנאי מחשוב את סיבת החסימה, במקרה של חסימת שווא ישחרר הטכנאי את הדואר החסום.

3.4. דיווח, גילוי וטיפול בעת הופעת וירוס בתחנת עבודה או התפרצות וירוסים

3.4.1 בכל גילוי וירוס בתחנת עבודה, מבוצעות פעולות לנטרל נזק ולמנוע התפשטות וירוס ברשת.

3.4.2 בכל תחנת עבודה מותקנת תוכנת אנטי וירוס ברשת המנטרת את פעילות התחנה באופן שוטף.

3.4.3 עם גילוי וירוס בתחנה, מציגה תוכנת האנטי ווירוס הודעה מתפרצת על המסך המיועדת ליידע את המשתמש.

3.4.4 עם הופעת הודעה מתפרצת, יפעל המשתמש בהתאם להנחיות שלהלן :

- 3.4.4.1 המשתמש יסגור את כל התוכנות הפעילות.
- 3.4.4.2 המשתמש יבצע כיבוי מסודר של המחשב (Shut down)
- 3.4.4.3 המשתמש יודיע טלפונית ומיידית על גילוי ווירוס במחשבו למכרז השירות והתמיכה של המועצה טלפונית.
- 3.4.4.4 המחשב יישאר כבוי עד לבדיקתו על ידי אנשי המחשוב המועצה.



מדיניות אבטחת מידע

אוגדן נהלי אבטחת
מידע

מהדורה : 3.0

מס' נוהל : א-5.1.1

תפקיד : יועץ חיצוני

ערך : עזרא דיין

תפקיד : מנכ"לית
המועצה

אישר : ענת מור

עמוד 5 מתוך 17

עודכן בתאריך : 1/9/2020

3.4.5. פעולות אחראי אבטחת מידע בעת אירוע התפשטות וירוס ברשת עירונית :

- אחראי אבטחת המידע יגיע אל המחשב החשוד ויבצע בו את הפעולות הבאות ;
- בדיקת סטאטוס של הווירוס או הקובץ החשוד כנגוע בווירוס.
- סריקת החומר ע"י שני מנועי אנטי וירוס לפחות. במידת הצורך, פירוק הדיסק הקשיח והעברתו למנמ"ר המועצה לצורך המשך טיפול באמצעות חיבור של הדיסק לתחנת הלבנה לטיפול בהסרת הווירוס.
- החומר שנסרק ונמצא נקי יוחזר למשתמש.
- יעשה כל מאמץ לשמור על מירב החומר של המשתמש הנמצא על הדיסק הקשיח. יש לציין, באופן כללי לא אמור להיות חומר חשוב על הדיסק הקשיח של המשתמש אלא בשרתי המועצה באמצעות האפליקציות הייעודיות וספרית הקבצים ברשת.
- בדיקת עדכניות של מנוע התוכנה והחתימות - במחשב ועדכון במידת הצורך.
- סגירת התקלה במערכת דיווח תקלות מחשב.
- חיבור מחדש של המחשב לרשת ממנה הוצא המחשב.
- מילוי ושיגור טופס דיווח על אירוע וירוס בתחנת עבודה.

3.4.6. התנהלות בעת התפרצות וירוסים

- 3.4.6.1. על תחנות העבודה של המשתמשים מותקנת חבילת אנטי וירוס של חברת ESET.
- 3.4.6.2. הדרישה היא כי כל תחנת עבודה תעודכן באופן אוטומטי בגרסה העדכנית הקיימת לכל חבילה, בכפוף להמלצות ספק תוכנת האנטי וירוס.
- 3.4.6.3. נקודת המוצא צריכה להיות היא שהאנטי וירוס מעודכן לקובץ חתימות האחרון שיש, ושמונע האנטי וירוס הוא הגרסה האחרונה שיש.

זהו סדר הפעולות שיש לבצע כדי למגר וירוס במהירות האפשרית, גם במקרים שקיימת התפרצות של וירוס חדש ושהחבילות עצמן עדיין אינן מעודכנות בדרך הטיפול בו ואו הסרתו.

3.4.7. פעילות עדכון וטיפול בעת אירוע

מדיניות אבטחת מידע



מועצה אזורית הגלבע

אוגדן נהלי אבטחת
מידע

מהדורה : 3.0

מס' נוהל : א-5.1.1

תפקיד : יועץ חיצוני

ערך : עזרא דיין

תפקיד : מנכ"לית
המועצה

אישר : ענת מור

עמוד 6 מתוך 17

עודכן בתאריך : 1/9/2020

- 3.4.7.1 כניסה יומית לכלי הניהול של התוכנה לבדיקת מצב הווירוסים במועצה
- באחריות מנמ"ר המועצה
- 3.4.7.2 לוודא שבכלי הניהול מוגדר שבעת התפרצות וירוסים (נקבע ע"פ כמות
וירוסים ליחידת זמן) נשלח מייל לתפוצה המתאימה
- 3.4.7.3 בעת התפרצות וירוסים במועצה, אשר האנטי וירוס לא מצליח
להתמודד איתם, כגון וירוס חדש, או שינוי של וירוס קיים, יש להפעיל
סריקה ע"י יותר ממנוע אנטי וירוס אחד וזאת על מנת לזהות את הקובץ
הפוגעני.
- 3.4.7.4 הקובץ שנוצר ישלח לספק התוכנה אשר יספק שירותי תמיכה בכל
בעיות האנטי וירוס. הקובץ יועבר ליצרן אנטי וירוס. בהתאם לתקיפה יועבר
קובץ חתימות חדש.
- 3.4.7.5 במידה ולא עוזר חוזרים על הפעולה.
- 3.4.7.6 במקרים מסוימים ההתפרצות חוזרת על עצמה לאחר שעות או ימים,
מכיוון שהווירוס משנה התנהגות. (מוטציה של הווירוס). – במקרה זה נדרשת
תמיכה של יצרן אנטי וירוס.
- 3.4.7.7 בעת פתיחת הקריאה אצל ספק התוכנה יש לקרוא לנציג מטעמם אשר
אחראי ללוות את התהליך עד לפתרון.

3.5. הפצת אנטי וירוס

- 3.5.1 במועצה מותקנת תוכנת אנטי וירוס בתחנות העבודה והשרתים. דרך הפצתו של
האנטי וירוס בארגון לתחנות העבודה היא באמצעות policy ארגוני. הפצת אנטי
וירוס מתבצעת אוטומטית בכל מחשב בארגון, ברגע שמתחבר אל ה-Domain
מקבל את עדכון האנטי וירוס המתאים לו.
- 3.5.2 במקרה של המצאות אנטי וירוס אחר יש לבצע הסרה בעזרת כלי ההסרה של
הגרסה / התוכנה הקודמת.
- 3.5.3 אין להסיר אנטי וירוס מתחנה ללא אישור מנמ"ר המועצה.

3.6. הקשחת תחנת עבודה

מדיניות אבטחת מידע



אוגדן נהלי אבטחת
מידע

מהדורה : 3.0

מס' נוהל : א-5.1.1

תפקיד : יועץ חיצוני

ערך : עזרא דיין

תפקיד : מנכ"לית
המועצה

אישר : ענת מור

עמוד 7 מתוך 17

עודכן בתאריך : 1/9/2020

- 3.6.1 פעילות זו תכליתה לבנות סביבת עבודה בטוחה בתחנות העבודה של משתמשי הקצה במועצה. הקשחת תחנה מתבצעת באמצעות הפעלת מדיניות קבוצתית ב-AD.
- 3.6.2 הגדרות אשר מונעות גישה לא מאושרת לקובצי סיסטם, מונעות ממשתמשים לבצע שינויים לא רצויים להגדרות אבטחה, הגדרות אוטומטיות בהתקנת אנטי-ווירוס בתחנות והגדרות קבועות של שרתי Proxy לגלישה באינטרנט
- 3.6.3 הקשחת תחנת עבודה תבצע דרך Group policy objects - Active Directory. המטרה היא לבנות סביבת העבודה בטוחה למשתמשים, ללא חשש לפגיעה בצרכים היום-יומיים.
- 3.6.4 יש כמה GPO שמגבילים הרשאות משתמשים בתחנות עבודה :
- 3.6.4.1 Default Domain Policy
 - 3.6.4.2 Restrictions
 - 3.6.4.3 יש לבצע שינויים ובחירת הגדרות המגבילים הרשאות המשתמשים ע"פ המוגדר console הניהול של המערכת.

3.7. ניהול סיסמאות והקשחת סיסמאות בארגון

- 3.7.1 אבטחת המידע ברשת מתבססת על זיהוי אמין של המשתמשים.
- 3.7.2 הסיסמאות מיועדות לאמת את זהות המשתמשים ברשת. על מנת לצמצם הסיכון של שימוש לרעה בסיסמאות המשתמשים, נקבעו כללים ליצירת הסיסמאות ואופן השימוש בהן.
- 3.7.3 סיסמאות הינן הכלי להגן על חדירה למערכות ולמחשבי הארגון, למידור, למניעת ריגול, למניעת גרימת נזק, ולמניעת חשיפת מידע למי שאינו מוסמך לכך ולכן על הסיסמאות להיות מורכבות ועליהן להשתנות אחת לתקופה כמוגדר להלן :
- 3.7.4 סיסמת עבודה - מחרוזת בת 10 תווים אישית המורכבת מאותיות וספרות ללא על לפי בחירת המשתמש.
- 3.7.5 סיסמא ראשונית - סיסמא חד-פעמית המונפקת ע"י טכנאי המחשוב למשתמש בחשבון חדש, או במקרה של שכחת סיסמת עבודה המצריכה הנפקת סיסמא ראשונית חדשה.
- 3.7.6 משך זמן מרבי לתוקף סיסמה עבודה - פרק הזמן המרבי שנקבע לשימוש בסיסמת עבודה הוא 3 חודשים ממועד יצירתה.

מדיניות אבטחת מידע



מועצה אזורית הגלבע

אוגדן נהלי אבטחת
מידע

מהדורה : 3.0

מס' נוהל : א-1.1.5.

תפקיד : יועץ חיצוני

ערך : עזרא דיין

תפקיד : מנכ"לית
המועצה

אישר : ענת מור

עמוד 8 מתוך 17

עודכן בתאריך : 1/9/2020

3.7.7. אימות דו שלבי של הסיסמאות

3.7.8. משך זמן מזערי למוקף סיסמת עבודה - אם קיים חשש לדליפת הסיסמא, משתמש רשאי ויכול להחליף סיסמתו גם לפני שחלפו 6 חודשים ממועד יצירתה, אולם לא יותר מהחלפת סיסמא פעם אחת ביממה.

3.7.9. היסטוריית סיסמאות - על מנת למנוע שימוש חוזר בסיסמאות קודמות, המערכת שומרת את היסטוריית הסיסמאות של המשתמשים וחוסמת שימוש בסיסמא שכבר נעשה בה שימוש בעבר.

3.7.10. סודיות הסיסמא - סיסמאות הן אישיות וחל איסור לגלותן לאחר.

3.8. תהליך יצירה וניהול סיסמאות

3.8.1. עם הקמת חשבון חדש למשתמש, תקבע ע"י מקים המשתמש סיסמא ראשונית באמצעותה יבצע המשתמש כניסה ראשונה לחשבון.

3.8.2. עם כניסתו לחשבון באמצעות הסיסמא הראשונית, תדרוש המערכת באופן אוטומטי מהמשתמש ליצור לעצמו סיסמת עבודה קבועה שתשמש אותו במשך 6 חודשים.

3.8.3. סיסמא זו צריכה כאמור להיות בת 10 תווים שונים זה מזה, צירוף של אותיות וספרות בלבד. אין לכלול בסיסמא תווי פיסוק וסימנים מיוחדים.

3.8.4. על המשתמש לזכור את סיסמת העבודה שלו ולא לרשום אותה במקום ובאופן שמישהו מלבדו יוכל לראותה.

3.8.5. לאחר 3 חודשים של שימוש בסיסמא, יידרש המשתמש (באופן אוטומטי ע"י המערכת) ליצור לעצמו סיסמת עבודה חדשה וסיסמתו הקודמת תבוטל.

3.8.6. במידה ומשתמש חושש שסיסמתו נודעה לאחר, יפנה למרכז השירות ויפתח קריאה מתאימה לאיפוס סיסמא או הקמת סיסמא חדשה. לאחר שיקבלה יחליפה בסיסמת עבודה חדשה.

3.8.7. חל איסור על שימוש בסיסמא קולקטיבית המשמשת קבוצת משתמשים

3.8.8. מערכת בקרת אבטחת המידע מפקחת באופן רצוף על כל פעילות הסיסמאות, מתעדת ומתריעה על כל הפרה של הכללים. על אירועי הפרה של כללי הסיסמאות יש לעדכן את מנמ"ר המועצה.

מדיניות אבטחת מידע



מועצה אזורית הגלבע

אוגדן נהלי אבטחת
מידע

מהדורה : 3.0

מס' נוהל : א-5.1.1

תפקיד : יועץ חיצוני

ערך : עזרא דיין

תפקיד : מנכ"לית
המועצה

אישר : ענת מור

עמוד 9 מתוך 17

עודכן בתאריך : 1/9/2020

3.8.9. המטרה היא לבנות סיסמאות מורכבות המכילות : אותיות גדולות, קטנות, מספרים

וסימנים. הסיסמא תכיל לפחות 10 תווים (לדוגמה : A^be\$\$d712@)

3.8.10. לאחר קבלת החלטה לגבי מדיניות הסיסמאות, אפשר לשנות את ה- default domain policy ולאפשר קיום של סיסמאות ב- domain רק ב- complexity pattern.

3.8.11. מדיניות תוקף לסיסמאות עד 3-4 חודשים, המשתמש חייב לשנות את סיסמתו לחדשה שלא השתמש בה בעבר. הגדרה זאת נמצאת גם ב- GPO default domain policy.

3.9. ניהול משתמשים והרשאות (בכפוף לנוהל קליטת ועזיבת עובד)

3.9.1. יצירת משתמש חדש ברשת

3.9.1.1. קבלת בקשה ואישור להוספת משתמש וחיבורו לרשת.

3.9.1.2. יצירת המשתמש ב AD של הרשת.

3.9.2. עזיבת עובד וחשבונות לא פעילים

3.9.3. בעת עזיבת עובד יתקבל דוא"ל ממנהל משאבי אנוש המפרט פרטי המשתמש ותאריך עזיבתו.

3.9.4. טכנאי המחשוב יעבירו את חשבונות המשתמש שעוזב למצב DISABLE. יודגש, כי אין למחוק את החשבון מה- AD. תיבת הדואר של המשתמש תחסם.

3.9.5. עם סיום עבודתו של העובד יבוצע ייצוא של תיבת הדואר של העובד לקובץ PST והקובץ יגובה כחלק מנוהל הגיבוי של המועצה.

3.9.6. כעבור 30 יום לאחר עזיבתו של העובד החומר של העובד יועבר לתיקיית Disabled Users.

3.10. אחסון מידע

3.10.1. משתמשי המועצה נדרשים לאחסן מידע רב במסגרת עבודתם. מידע יאוחסן

בשרתי הקבצים / שרתי ניהול המסמכים של המועצה בלבד לאחסן בשרתי המועצה בלבד.

מדיניות אבטחת מידע



מועצה אזורית הגלבע

אוגדן נהלי אבטחת
מידע

מהדורה : 3.0

מס' נוהל : א-5.1.1

תפקיד : יועץ חיצוני

ערך : עזרא דיין

תפקיד : מנכ"לית
המועצה

אישר : ענת מור

עמוד 10 מתוך 17

עודכן בתאריך : 1/9/2020

- 3.10.2. ע"פ צורך ניתן לאחסן מידע במחשב המקומי או על גבי disk on key שנופק ע"י טכנאי המחשב של המועצה בלבד.
- 3.10.3. כמו כן יתכן צורך להשתמש במדיה מגנטית כדוגמת דיסק צרוב ודיסק קשיח.
- 3.10.4. אין להוציא מדיה מגנטית מחוץ לתחומי המועצה (דיסקים קשיחים, דיסקטים וכו').
- 3.10.5. בעת שליחת מחשב לתיקון במעבדת חוץ, יש להקפיד להוציא את הדיסק הקשיח מהמחשב. במקרה של דיסק תקול, יש להעבירו לצוות המחשב לצורך השמדת המדיה.

3.11. טיפול שוטף ברשת המחשב של המועצה

- 3.11.1. במקרה של גילוי וירוס - הקובץ יימחק. דיווח על גילוי וירוס מבוצע ע"פ נוהל טיפול בוורוסים.
- 3.11.2. במקרה של זיהוי הקובץ כדוא"ל - SPAM, הקובץ יימחק ללא הודעה כלשהי. במידה וקיים רצף הודעות SPAM שמקורן באותו המפיץ, נחסם המקור השולח על ידי מערכת סינון דואר אלקטרוני.
- 3.11.3. במקרה של סוג קובץ אסור בכניסה לרשת – תבוצע מחיקה של הדוא"ל עם קובץ הצרופה, ללא הודעה על ידי מערכת FW העירונית.
- 3.11.4. במקרה של קובץ גדול מהמורשה - ווידוא עם הנמען במועצה שהוא מצפה לקבל את הקובץ שנעצר בהסגר.
- 3.11.5. קובץ שהמגבלה היחידה שלו הוא גודלו ושהנמען שלו מצפה לו, ישוחרר לנמען.

4. אחריות, סמכות ותוקף:

- 4.1. נוהל זה אינו מחליף את דרכי ההתערבות והטיפול הקיימים במקרים המובאים לעיל, אלא בא להוסיף עליהם.
- 4.2. האחריות והסמכות לביצוע נוהל זה הינה על מנמ"ר המועצה ומי מטעמו בהתאם לאמור לעיל.
- 4.3. נוהל זה ייכנס לתוקפו החל מיום פרסומו.



מדיניות אבטחת מידע

אוגדן נהלי אבטחת
מידע

מהדורה : 3.0

מס' נוהל : א-5.1.1

תפקיד : יועץ חיצוני

ערך : עזרא דיין

תפקיד : מנכ"לית
המועצה

אישר : ענת מור

עמוד 11 מתוך 17

עודכן בתאריך : 1/9/2020

נספחים



מדיניות אבטחת מידע

אוגדן נהלי אבטחת
מידע

מהדורה : 3.0

מס' נוהל : א-5.1.1

תפקיד : יועץ חיצוני

ערך : עזרא דיין

תפקיד : מנכ"לית
המועצה

אישר : ענת מור

עמוד 12 מתוך 17

עודכן בתאריך : 1/9/2020

נספח א' - תקציר הנחיות משתמשי המועצה בעבודה עם משאבי המחשוב

1. השימוש במחשב ובמאגרי המידע של המועצה הנו לצורך עבודה בלבד וכפוף לנוהלי המועצה.
2. יש להקפיד על שימוש בסיסמאות, הסיסמא היא אישית ואסור להעבירה לאחר.
3. חל איסור להתקין תוכנות שלא באישור מנמ"ר המועצה.
4. חל איסור להתקין רכיב חומרה פרטי מכל סוג שלא באישור מנמ"ר המועצה.
5. לידיעתך, כל המידע ופעילות מערכות המחשוב של המועצה, מנוטרים ומבוקרים על ידי גורמי אבטחת המידע.
6. אין להשתמש במדיה ואמצעי אחסון חיצוניים שאינם שייכים למועצה.
7. אין להוציא חומרים מסווגים לרבות מדיה מגנטית מחוץ לאתרי המועצה.
8. יש להתחבר לרשת המיועדת לעבודתך בלבד.
9. אין להשאיר חומרים פתוחים ונגישים למי שאינו מורשה, סגור ונעל כל מידע לרבות אבטחה פיזית.
10. בכל מקרה של תקלה או בעיה יש לפנות למרכז התמיכה לפתרון תקלות מחשוב טלפונית או באמצעות דוא"ל.
11. אין להשאיר בשום מקרה מחשב נייד ברכב ללא השגחה.
12. יש לצאת מהרשת בסוף היום, אין לכבות את המחשב.
13. שימוש בציוד קצה (מדפסות, סורקים, מצלמות וכדו') לצרכי עבודה בלבד.
14. יש להקפיד על הדפסה דו-צדדית ככל הניתן.



מדיניות אבטחת מידע

אוגדן נהלי אבטחת
מידע

מהדורה : 3.0

מס' נוהל : א-5.1.1

תפקיד : יועץ חיצוני

ערך : עזרא דיין

תפקיד : מנכ"לית
המועצה

אישר : ענת מור

עמוד 13 מתוך 17

עודכן בתאריך : 1/9/2020

15. יש להתחבר לרשת המועצה מרחוק באמצעות נייד ומודם, עפ"י הנחיות מנמ"ר או ספק המחשוב של המועצה בלבד.



מדיניות אבטחת מידע

אוגדן נהלי אבטחת
מידע

מהדורה : 3.0

מס' נוהל : א-5.1.1

תפקיד : יועץ חיצוני

ערך : עזרא דיין

תפקיד : מנכ"לית
המועצה

אישר : ענת מור

עמוד 14 מתוך 17

עודכן בתאריך : 1/9/2020

נספח ב' - הדרכה והתחייבות למדיניות אבטחת מידע

1. אינטרנט

השימוש באינטרנט הינו לצרכי עבודה בלבד. בשום אופן אין לבצע שימוש בעייתי בגלישה באינטרנט כגון: גלישה באתרי הימורים, פורנוגרפיה, פרסום מידע בעייתי באינטרנט (כגון כתיבת תגובות ופוסטים פוגעניים), ניסיונות לעקוף בקרות אבטחת מידע וכד'.
קיים ניטור תמידי לגלישה באינטרנט.

2. דואר אלקטרוני

- 2.1. הדואר האלקטרוני הינו לשימוש צרכי עבודה בלבד.
- 2.2. יש לנקוט זהירות מרבית בעת שליחת דואר אלקטרוני כך שלא יועבר מידע רגיש אל גורם אשר אינו זקוק לו.
- 2.3. פרטיות הדואר מוגבלת, על העובד לדעת שבכל עת ניתן לגשת אל תיבת הדואר שלו בהתאם לצרכי הארגון והחוק.
- 2.4. אין לשלוח הודעות לנמענים אשר אינם מעוניינים בכך.
- 2.5. אין לשלוח הודעות שרשרת.
- 2.6. אין לשלוח הודעות תוך התחזות לאחר.
- 2.7. הודעות דואר חשודות יש למחוק מיידית ולדווח למנמ"ר המועצה.

3. רשת

- 3.1. ברשת המחשוב של המועצה קיים מידע רב. כל עובד נדרש לשיקול דעת ואסור לו לנסות לגשת למידע אשר אליו יש לו הרשאות אך מאידך אין זה מעניינו.
- 3.2. מידע ארגוני יש לאחסן על רשת המחשוב. מידע אשר נמצא על הדיסק הקשיח המקומי אינו מגובה.
- 3.3. בסוף יום עבודה יש לצאת מהרשת ע"י ניתוק המשתמש מהרשת בלבד (לא לכבות את המחשב).
- 3.4. ניתוק זה מתבצע ע"י לחיצה על מקש התחל ובחירה בניתוק של המשתמש

4. רשתות אלחוטיות



מדיניות אבטחת מידע

אוגדן נהלי אבטחת
מידע

מהדורה : 3.0

מס' נוהל : א-5.1.1

תפקיד : יועץ חיצוני

ערך : עזרא דיין

תפקיד : מנכ"לית
המועצה

אישר : ענת מור

עמוד 15 מתוך 17

עודכן בתאריך : 1/9/2020

- 4.1. כאשר כרטיס הרשת האלחוטית אינו בשימוש עליו להיות במצב של "DISABLE".
- 4.2. אין לנסות להתחבר לרשתות אלחוטיות זרות.
- 4.3. אין להתחבר לרשת אחרת / אינטרנט מהיר במקביל לחיבור לרשת של המועצה.

5. מחשבים ניידים

- 5.1. אין להשאיר מחשבים ניידים ללא השגחה במקום ציבורי.
- 5.2. אין להשאיר מחשבים ניידים ברכב.
- 5.3. מחשב נייד אשר נשאר במועצה בתום יום עבודה עליו להינעל בתוך ארון.
- 5.4. אין להתקין על המחשבים הניידים של המועצה תוכנות לא חוקיות, תוכנות לשיתוף קבצים לדוגמא uTorrent וכן אין לגלוש לאתרים לא ראויים (סקס, אלימות, הימורים) גם אם החיבור לאינטרנט נעשה שלא ברשת המועצה, שכן אתרים אלו מכילים לרוב וירוסים וסוסים טרויאניים.

6. אחר

- 6.1. מידע המאוחסן במערכות המידע של המועצה הינו רכוש המועצה.
- 6.2. שימושים לא אתיים בצידוד המחשוב של המועצה יגרור צעדים משמעותיים כנגד העובד.

הריני מאשר כי קראתי והבנתי את האמור לעיל והנני מסכים לכל.

שם	תאריך	חתימה



מדיניות אבטחת מידע

		מדיניות אבטחת מידע	
		מהדורה : 3.0	מס' נוהל : א-5.1.1
תפקיד : יועץ חיצוני	ערך : עזרא דיין	עמוד 16 מתוך 17	עודכן בתאריך : 1/9/2020
תפקיד : מנכ"לית המועצה	אישר : ענת מור		

נספח ג' - דיווח על אירוע וירוס בתחנת עבודה

המקור הראשוני לאירוע

SOC	
דיווח משתמש	
מחלקת מחשוב	

(סמן X בתיבה המתאימה)

פרטי האירוע:

	עיתוי הגילוי
	זיהוי המחשב הנגוע
	שם המשתמש הפעיל בתחנה
	תיאור המדיה הנגועה
	סוג/שם הווירוס
	סטטוס ההדבקה
	המלצות לפעולה
	סטטוס אירוע



מדיניות אבטחת מידע

אוגדן נהלי אבטחת
מידע

מהדורה : 3.0

מס' נוהל : א-5.1.1

תפקיד : יועץ חיצוני

ערך : עזרא דיין

תפקיד : מנכ"לית
המועצה

אישר : ענת מור

עמוד 17 מתוך 17

עודכן בתאריך : 1/9/2020