1 מטרת הנוהל

מטרת הנוהל להגדיר את מדיניות מועצה אזורית גזר (להלן: "**המועצה**") בנושאי אבטחת מידע ואת פעילויות המחשוב למניעה, תחזוקה וניהול משימות אבטחת מידע.
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 בציוד המחשוב, המידע ואמצעי האחסון במועצה.

2 תיחום הנוהל

הנוהל מיועד לעובדי המועצה, לקבלן המחשוב של המועצה- חברת נטקור פתרונות מחשוב (להלן: "**הקבלן**"), ספקי מערכות המחשוב וספקים נוספים בתחומי מערכות המידע של המועצה, משתמשי המועצה וכל גורם המחזיק במידע השייך למועצה. הנוהל מחייב כל גורם המטפל בשרתים במועצה ו/או בתחנות העבודה ו/או במאגרי המידע והאחראי.
הנוהל מציג תיאור הפעולות שיש לבצע בתחום אבטחת מידע לרבות בתחום תשתית, ניהול הרשאות וסיסמאות, טיפול באירועים, הפצת מדיניות ומניעה.

3 תהליכי עבודה

להלן תהליכי עבודה הנכללים בנוהל:

3.1 **התקנת תוכנות לא מאושרות.**

3.2 **התקנת תוכנות המורדות מהאינטרנט.**

3.3 **שימוש בדוא"ל של המועצה.**

3.4 **טיפול בספאם.**

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

3.6 **התנהלות בעת התפרצות וירוסים.**

3.7 **הפצת אנטי וירוס.**

3.8 **הקשחת תחנת עבודה.**

בית חשמונאי ד.נ שמשון 9978900
טל. 08-9274040
פקס. 08-9247115
www.gezer-region.muni.il
מועצה אזורית גזר

3.9 **ניהול סיסמאות והקשחת סיסמאות בארגון.**

3.10 **תהליך יצירה וניהול סיסמאות.**

3.11 **ניהול משתמשים והרשאות (בכפוף לנוהל קליטת ועזיבת עובד).**

3.12 **אחסון מידע.**

3.13 **טיפול שוטף ברשת המחשוב של המועצה.**

4 מדיניות המועצה בתחומי אבטחת המידע

4.1 התקנת תוכנות לא מאושרות

4.1.1 התקנת תוכנה לא מאושרת תכלול בין היתר את הרכיבים הבאים:

4.1.1.1 תוכנה לא חוקית, תוכנה מועתקת ללא הרשאה או שנרכשה באופן אחר שלא בהתאם לתנאי הספק המורשה ולהנחיות המועצה.

4.1.1.2 כל תוכנה אחרת (גם אם נרכשה כחוק ע"י העובד באופן פרטי) המותקנת ללא קבלת אישור קבלן המחשוב או יועץ המחשוב של המועצה.

4.1.2 השימוש בתוכנה לא מאושרת עלול לגרום לשיבושים במערכות המחשוב של המועצה.

4.1.3 כל משתמשי תחנות עבודה שבמחשבם קיימת או שהותקנה תוכנה לא מאושרת מחויבים להודיע על כך לקבלן המחשוב ו/או לתמיכה באמצעות הדוא"ל. היה ועובד מצא שתוכנה לא מאושרת כלשהי הינה חיונית לעבודתו השוטפת עליו לפנות בדוא"ל לקבלן – אשר יבצע הסרה, או שתבוצע רכישה באופן חוקי ע"י המועצה, או שהתוכנה תקבל אישור התקנה ושימוש מן הגורמים המוסמכים.

4.1.4 במסגרת פעילות האחזקה השוטפת במחשבי המועצה, יהיו עובדי המחשוב רשאים למחוק כל תוכנה לא מאושרת בעת טיפולם בחומרה או בתוכנה.

4.1.5 האחריות לגבי השימוש בתוכנה לא מאושרת תהיה על המשתמש באופן אישי, גם כלפי המועצה וגם כלפי גורמים חיצוניים.

בית חשמונאי ד.נ שמשון 9978900
טל. 08-9274040
פקס. 08-9247115
www.gezer-region.muni.il
מועצה אזורית גזר

4.2 התקנת תוכנות המורדות מהאינטרנט

4.2.1 התקנת תוכנות כאלה במחשבי המועצה אסורה גם אם התוכנה מסוג Shareware ללא אישור היועץ / קבלן המחשוב.

4.3 שימוש בדוא"ל של המועצה

4.3.1 שימוש בדואר אלקטרוני שלא לצורכי עבודה:

4.3.1.1 שרותי הדואר האלקטרוני הינם לצורכי עבודה בלבד. למניעת דלף מידע, אין להשתמש בשירותי הדואר האלקטרוני להעברת מידע שלא לצרכי העבודה. במקרים בהם נתקל עובד ו/או מנהל בחשד לשימוש שלא לפי הנחיות אלו עליו לפנות לקבלן.

4.3.2 קבלת דבר דואר מגורם לא ידוע:

4.3.2.1 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 מיד טלפונית לקבלן המחשוב.

4.4 טיפול בספאם

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

4.4.2 עם גילוי אירוע, הקבלן יבדוק את נתוני האירוע על מנת לברר את הסיבה לחסימת ההעברה.

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

4.4.3.1 העברת הודעת חסימה לקבלן בדוא"ל.

4.4.3.2 רישום לוג של האירוע במערכת סינון הדואר.

בית חשמונאי ד.נ שמשון 9978900
טל. 08-9274040
פקס. 08-9247115
www.gezer-region.muni.il
מועצה אזורית גזר

4.4.4 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.

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

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

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

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

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

4.5.4.1 המשתמש יסגור את כל התוכנות הפעילות.

4.5.4.2 המשתמש יבצע כיבוי מסודר של המחשב (**Shut down**).

4.5.4.3 המשתמש יודיע טלפונית מיד על גילוי ווירוס במחשבו למכרז השירות והתמיכה של המועצה.

4.5.4.4 המחשב יישאר כבוי עד לבדיקתו על ידי קבלן המחשוב.

4.5.5 פעולות יועץ המחשוב בעת אירוע התפשטות וירוס ברשת המועצה:

4.5.5.1 היועץ יגיע אל המחשב החשוד ויבצע בו את הפעולות הבאות:

4.5.5.1.1 בדיקת סטאטוס של הווירוס או הקובץ החשוד כנגוע בווירוס.

4.5.5.1.2 סריקת החומר ע"י שני מנועי אנטי וירוס לפחות. במידת הצורך, פירוק הדיסק הקשיח והעברתו לקבלן לצורך המשך טיפול באמצעות חיבור של הדיסק לתחנת הלבנה לטיפול בהסרת הווירוס.

בית חשמונאי ד.נ שמשון 9978900
טל. 08-9274040
פקס. 08-9247115
www.gezer-region.muni.il
מועצה אזורית גזר

4.5.5.1.3 החומר שנסרק ונמצא נקי יוחזר למשתמש.

4.5.5.1.4 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.

4.5.5.1.5 בדיקת עדכניות של מנוע התוכנה והחתימות - במחשב ועדכון במידת הצורך.

4.5.5.1.6 סגירת התקלה במערכת דיווח תקלות מחשוב.

4.5.5.1.7 חיבור מחדש של המחשב לרשת ממנה הוצא המחשב.

4.5.5.1.8 מילוי ושיגור טופס דיווח על אירוע ווירוס בתחנת עבודה.

4.6 התנהלות בעת התפרצות וירוסים

4.6.1 על תחנות העבודה של המשתמשים מותקנת חבילת אנטי וירוס של חברת ESET.

4.6.2 הדרישה היא כי כל תחנת עבודה תעודכן באופן אוטומטי בגרסה העדכנית הקיימת לכל חבילה, בכפוף להמלצות ספק תוכנת האנטי וירוס.

4.6.3 נקודת המוצא צריכה להיות מערכת אנטי וירוס מעודכנת לקובץ חתימות האחרון שיש, ושמנוע האנטי וירוס הוא הגרסה האחרונה שיש. זהו סדר הפעולות שיש לבצע כדי למגר וירוס במהירות האפשרית, גם במקרים שקיימת התפרצות של ווירוס חדש ושהחבילות עצמן עדיין אינן מעודכנות בדרך הטיפול בו ואו הסרתו.

4.6.4 פעילות עדכון וטיפול בעת אירוע

4.6.4.1 כניסה יומית לכלי הניהול של התוכנה לבדיקת מצב הווירוסים במועצה - באחריות הקבלן.

בית חשמונאי ד.נ שמשון 9978900
טל. 08-9274040
פקס. 08-9247115
www.gezer-region.muni.il
מועצה אזורית גזר

4.6.4.2 לוודא שבכלי הניהול מוגדר שבעת התפרצות וירוסים (נקבע ע"פ כמות וירוסים ליחידת זמן) נשלח מייל לתפוצה המתאימה.

4.6.4.3 בעת התפרצות וירוסים במועצה, אשר מערכת אנטי וירוס לא מצליחה 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.

4.6.4.4 הקובץ שנוצר יישלח ליצרן אנטי וירוס (תמיכה) אשר יספק שירותי תמיכה בכל בעיות האנטי וירוס. בהתאם לתקיפה יועבר קובץ חתימות חדש.

4.6.4.5 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.

4.6.4.6 בעת פתיחת הקריאה אצל ספק התוכנה יש לקרוא לנציג מטעמם אשר אחראי ללוות את התהליך עד לפתרון.

4.7 הפצת אנטי וירוס

4.7.1 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.

4.7.2 במקרה של המצאות אנטי וירוס אחר יש לבצע הסרה בעזרת כלי ההסרה של הגרסה / התוכנה הקודמת.

4.7.3 אין להסיר אנטי וירוס מתחנה ללא אישור קבלן המחשוב.

4.8 הקשחת תחנת עבודה

בית חשמונאי ד.נ שמשון 9978900
טל. 08-9274040
פקס. 08-9247115
www.gezer-region.muni.il
מועצה אזורית גזר

4.8.1 פעילות זו תכליתה לבנות סביבת עבודה בטוחה בתחנות העבודה של משתמשי הקצה במועצה. הקשחת תחנה מתבצעת באמצעות הפעלת מדיניות קבוצתית ב- AD.

4.8.2 הגדרות אשר מונעות גישה לא מאושרת לקובצי סיסטם, מונעות ממשתמשים לבצע שינויים לא רצויים להגדרות אבטחה, הגדרות אוטומטיות בהתקנת אנטי-וירוס בתחנות והגדרות קבועות של שרתי Proxy לגלישה באינטרנט.

4.8.3 הקשחת תחנת עבודה תתבצע דרך Group policy objects - Active Directory. המטרה היא לבנות סביבת העבודה בטוחה למשתמשים, ללא חשש לפגיעה בצרכים היום-יומיים.

4.8.4 יש כמה GPO שמגבילים הרשאות משתמשים בתחנות עבודה:

4.8.4.1 **Default Domain Policy**

4.8.4.2 **Restrictions**

4.8.5 יש לבצע שינויים ובחירת הגדרות המגבילים הרשאות המשתמשים ע"פ המוגדר console הניהול של המערכת.

4.9 ניהול סיסמאות והקשחת סיסמאות בארגון

4.9.1 אבטחת המידע ברשת מתבססת על זיהוי אמין של המשתמשים.

4.9.2 הסיסמאות מיועדות לאמת את זהות המשתמשים ברשת. על מנת לצמצם הסיכון של שימוש לרעה בסיסמאות המשתמשים, נקבעו כללים ליצירת הסיסמאות ואופן השימוש בהן.

4.9.3 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:

בית חשמונאי ד.נ שמשון 9978900
טל. 08-9274040
פקס. 08-9247115
www.gezer-region.muni.il
מועצה אזורית גזר

4.9.3.1 סיסמת עבודה - מחרוזת בת 6 תווים אישית המורכבת מאותיות וספרות לפי בחירת המשתמש.

4.9.3.2 סיסמא ראשונית - סיסמא חד-פעמית המונפקת ע"י טכנאי המחשוב למשתמש בחשבון חדש, או במקרה של שכחת סיסמת עבודה המצריכה הנפקת סיסמא ראשונית חדשה.

4.9.3.3 משך זמן מרבי לתוקף סיסמת עבודה - פרק הזמן המרבי שנקבע לשימוש בסיסמת עבודה הוא 6 חודשים ממועד יצירתה.

4.9.3.4 משך זמן מזערי לתוקף 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.

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

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

4.10 **תהליך יצירה וניהול סיסמאות**

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

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

4.10.3 סיסמא זו צריכה כאמור להיות בת 6 תווים שונים זה מזה, צירוף של אותיות וספרות בלבד. אין לכלול בסיסמא תווי פיסוק וסימנים מיוחדים.

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

בית חשמונאי ד.נ שמשון 9978900
טל. 08-9274040
פקס. 08-9247115
www.gezer-region.muni.il
מועצה אזורית גזר

4.10.5 לאחר 6 חודשים של שימוש בסיסמא, יידרש המשתמש (באופן אוטומטי ע"י המערכת) ליצור לעצמו סיסמת עבודה חדשה וסיסמתו הקודמת תבוטל.

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

4.10.7 חל איסור על שימוש בסיסמא קולקטיבית המשמשת קבוצת משתמשים.

4.10.8 מערכת ניהול המשתמשים (DC) מפקחת באופן רצוף על כל פעילות הסיסמאות, מתעדת ומתריעה על כל הפרה של הכללים. במידה ומתרחש ניסיון גניבת זהות משתמש – יעביר קבלן המחשוב הודעה ליועץ המחשוב וזאת לאחר חסימת המשתמש מגישה למערכות המחשוב של המועצה.

4.10.9 הסיסמאות במועצה יהיו מסוג סיסמאות מורכבות המכילות: אותיות גדולות, קטנות, מספרים וסימנים. הסיסמא תכיל לפחות 6 תווים (לדוגמה: Absd12@).

4.10.10 המועצה מפעיל מדיניות סיסמאות באמצעות ה- default domain policy ומאפשר קיום של סיסמאות ב- domain רק ב- complexity pattern.

4.10.11 לפי המדיניות, ייקבע תוקף לסיסמאות. כל פרק זמן נתון של 3 חודשים, המשתמש חייב לשנות את סיסמתו לחדשה שלא השתמש בה בעבר (עד 5 סיסמאות אחרונות). הגדרה זאת חלה גם ב- GPO default domain policy.

4.11 **ניהול משתמשים והרשאות (בכפוף לנוהל קליטת ועזיבת עובד)**

4.11.1 יצירת משתמש חדש ברשת

4.11.1.1 קבלת בקשה ואישור להוספת משתמש וחיבורו לרשת.

4.11.1.2 יצירת המשתמש ב **AD** של הרשת.

בית חשמונאי ד.נ שמשון 9978900
טל. 08-9274040
פקס. 08-9247115
www.gezer-region.muni.il
מועצה אזורית גזר

4.11.2 עזיבת עובד וחשבונות לא פעילים

4.11.2.1 בעת עזיבת עובד, יתקבל דוא״ל ממנהל הכספים (האחראי גם על משאבי האנוש) המפרט פרטי המשתמש ותאריך עזיבתו.

4.11.2.2 טכנאי המחשוב יעביר את חשבונות המשתמש שעוזב למצב **DISABLE**.

יודגש, כי אין למחוק את החשבון מה- **AD**. תיבת הדואר של המשתמש תחסם.

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

4.11.2.4 כעבור 30 יום מעזיבתו של העובד, החומר של העובד יועבר לתיקיית **Disabled Users**.

4.12 **אחסון מידע**

4.12.1 משתמשי המועצה נדרשים לאחסן מידע רב במסגרת עבודתם. מידע יאוחסן בשרתי הקבצים / שרתי ניהול המסמכים (במערכת הגבייה – שרת ה IFN) של המועצה בלבד לאחסן בשרתי המועצה בלבד.

4.12.2 ע״פ צורך ניתן לאחסן מידע במחשב המקומי או על גבי disc on key שנופק ע״י קבלן המחשוב בלבד.

4.12.3 כמו כן יתכן צורך להשתמש במדיה מגנטית כדוגמת דיסק צרוב ודיסק קשיח.

4.12.4 אין להוציא מדיה מגנטית מחוץ לתחומי המועצה (דיסקים קשיחים, דיסקטים וכו׳).

4.12.5 בעת שליחת מחשב לתיקון במעבדת חוץ, יש להקפיד להוציא את הדיסק הקשיח מהמחשב. במקרה של דיסק תקול, יש להעבירו לקבלן המחשוב לצורך השמדת המדיה.

בית חשמונאי ד.נ שמשון 9978900
טל. 08-9274040
פקס. 08-9247115
www.gezer-region.muni.il
מועצה אזורית גזר

4.13 טיפול שוטף ברשת המחשוב של המועצה

4.13.1 במקרה של גילוי וירוס - הקובץ יימחק. דיווח על גילוי וירוס מבוצע ע"פ נוהל טיפול בווירוסים.

4.13.2 במקרה של זיהוי הקובץ כדוא"ל - SPAM, הקובץ יימחק ללא הודעה כלשהי. במידה וקיים רצף הודעות SPAM שמקורן באותו המפיץ, ייחסם המקור השולח על ידי מערכת סינון דואר אלקטרוני.

4.13.3 במקרה של סוג קובץ אסור בכניסה לרשת – תבוצע מחיקה של הדוא"ל עם קובץ הצרופה, ללא הודעה על ידי מערכת FW של המועצה.

4.13.4 במקרה של קובץ גדול מהמורשה - ווידוא עם הנמען במועצה שהוא מצפה לקבל את הקובץ שנעצר בהסגר.

4.13.5 קובץ שהמגבלה היחידה שלו הוא גודלו ושהנמען שלו מצפה לו, ישוחרר לנמען.

5 אחריות, תחולה ותוקף

5.1 **אחריות לביצוע הנוהל : קבלן המחשוב במועצה, חברת נטקור פתרונות מחשוב.**

5.2 **הנוהל חל על כל עובדי וספקי המחשוב של המועצה.**

5.3 **תוקף : לפי החלטת מנכ"ל המועצה.**

6 אישור הנוהל

תאריך :	שם המאשר :	חתימה :

בית חשמונאי ד.נ שמשון 9978900
טל. 08-9274040
פקס. 08-9247115
www.gezer-region.muni.il
מועצה אזורית גזר

7 נספחים

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

7.1.1 השימוש במחשב ובמאגרי המידע של המועצה הנו לצורך עבודה בלבד וכפוף לנהלי המועצה.

7.1.2 יש להקפיד על שימוש בסיסמאות, הסיסמא היא אישית ואסור להעבירה.

7.1.3 חל איסור להתקין תוכנות שלא באישור קבלן המחשוב ו/או יועץ המחשוב.

7.1.4 חל איסור להתקין רכיב חומרה פרטי מכל סוג שלא באישור קבלן המחשוב ו/או יועץ המחשוב.

7.1.5 לידיעתך, כל המידע ופעילות מערכות המחשוב של הקבלן, מנוטרים ומבוקרים על ידי מערכות אבטחת המידע.

7.1.6 אין להשתמש במדיה ואמצעי אחסון חיצוניים שאינם שייכים למועצה.

7.1.7 אין להוציא חומרים מסווגים לרבות מדיה מגנטית מחוץ לאתרי המועצה.

7.1.8 יש להתחבר לרשת המיועדת לעבודתך בלבד.

7.1.9 אין להשאיר חומרים פתוחים ונגישים למי שאינו מורשה, סגור ונעל כל מידע לרבות אבטחה פיזית (נעילה באמצעות סמל WIN + מקש "L").

7.1.10 בכל מקרה של תקלה או בעיה יש לפנות למוקד התמיכה של קבלן המחשוב לפתרון תקלות מחשוב טלפונית או באמצעות דוא"ל.

7.1.11 אין להשאיר בשום מקרה מחשב נייד ברכב ללא השגחה.

7.1.12 יש לצאת מהרשת בסוף היום, אין לכבות את המחשב.

7.1.13 שימוש בציוד קצה (מדפסות, סורקים, מצלמות וכדו') לצרכי עבודה בלבד.

7.1.14 יש להקפיד על הדפסה דו-צדדית ככל הניתן.

7.1.15 יש להתחבר לרשת המועצה מרחוק באמצעות חיבור מאובטח SLSVPN בלבד, עפ"י הנחיות קבלן המחשוב ו/או יועץ המחשוב.

בית חשמונאי ד.נ שמשון 9978900
טל. 08-9274040
פקס. 08-9247115
www.gezer-region.muni.il
מועצה אזורית גזר

7.2 נספח ב' - הדרכה והתחייבות למדיניות אבטחת מידע

7.2.1 אינטרנט

7.2.1.1 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'.

7.2.1.2 קיים ניטור תמידי לגלישה באינטרנט.

7.2.2 דואר אלקטרוני

7.2.2.1 הדואר האלקטרוני הינו לשימוש צרכי עבודה בלבד.

7.2.2.2 יש לנקוט זהירות מרבית בעת שליחת דואר אלקטרוני כך שלא יועבר מידע רגיש אל גורם אשר אינו זקוק לו.

7.2.2.3 פרטיות הדואר מוגבלת, על העובד לדעת שבכל עת ניתן לגשת אל תיבת הדואר שלו בהתאם לצרכי הארגון והחוק.

7.2.2.4 אין לשלוח הודעות לנמענים אשר אינם מעוניינים בכך.

7.2.2.5 אין לשלוח הודעות שרשרת.

7.2.2.6 אין לשלוח הודעות תוך התחזות לאחר.

7.2.2.7 הודעות דואר חשודות יש למחוק מיד ולדווח לקבלן המחשוב.

7.2.3 רשת

7.2.3.1 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.

7.2.3.2 מידע ארגוני יש לאחסן על רשת המחשוב. מידע אשר נמצא על הדיסק הקשיח המקומי אינו מגובה.

בית חשמונאי ד.נ שמשון 9978900
טל. 08-9274040
פקס. 08-9247115
www.gezer-region.muni.il
מועצה אזורית גזר

7.2.3.3 בסוף יום עבודה יש לצאת מהרשת ע"י ניתוק המשתמש מהרשת בלבד (לא לכבות את המחשב).

7.2.3.4 ניתוק זה מתבצע ע"י לחיצה על מקש התחל ובחירה בניתוק של המשתמש

7.2.4 רשתות אלחוטיות

7.2.4.1 כאשר כרטיס הרשת האלחוטית אינו בשימוש עליו להיות במצב של "**DISABLE**".

7.2.4.2 אין לנסות להתחבר לרשתות אלחוטיות זרות.

7.2.4.3 אין להתחבר לרשת אחרת / אינטרנט מהיר במקביל לחיבור לרשת הקווית של המועצה.

7.2.5 מחשבים ניידים

7.2.5.1 אין להשאיר מחשבים ניידים ללא השגחה במקום ציבורי.

7.2.5.2 אין להשאיר מחשבים ניידים ברכב.

7.2.5.3 מחשב נייד אשר נשאר במועצה בתום יום עבודה, עליו להינעל בתוך ארון.

7.2.5.4 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.

7.2.6 אחר

7.2.6.1 מידע המאוחסן במערכות המידע של המועצה הינו רכוש המועצה.

7.2.6.2 שימושים לא אתיים בציוד המחשוב של המועצה יגרור צעדים משמעתיים כנגד העובד.

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

שם העובד	תאריך	חתימה

בית חשמונאי ד.נ שמשון 9978900
טל. 08-9274040
פקס. 08-9247115
www.gezer-region.muni.il
מועצה אזורית גזר

7.3 נספח ג' - דיווח על אירוע וירוס בתחנת עבודה

7.3.1 המקור הראשוני לאירוע

	SOC
	דיווח משתמש
	גילוי ע"י ספק המחשוב

(סמן X בתיבה המתאימה)

7.3.2 פרטי האירוע:

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

בית חשמונאי ד.נ שמשון 9978900
טל. 08-9274040
פקס. 08-9247115
www.gezer-region.muni.il
מועצה אזורית גזר