נהלי מחשוב ואבטחת מידע – נוהל התאוששות מאסון

1. רקע

1.1. מועצה אזורית גזר (להלן המועצה) הינה גוף ציבורי המספק שירותים מוניציפליים בשגרה ובחירום לתושביו.

1.2. המועצה מפעילה מערכות מחשוב – שרתים, מחשבים וציוד תקשורת נלווה; מערכות מידע - לניהול המידע ולמתן שירותים מוניציפליים: חינוך, רווחה, הנדסה, ניהול הכנסות וניהול כספי של המועצה; מערכות טלפוניה – מרכזיית טלפונים לטובת מענה לציבור ולקיום שוטף של פעילות המועצה. המועצה מפעילה עשרות אתרים המקושרים ביניהם ברשתות תקשורת ואינטרנט – מוסדות חינוך וגני ילדים, מוסדות ובנייני המועצה (להלן מערכות ICT).

1.3. מערכות ICT חשופות לאיומים ופגיעות מצד תוקפים (חלקם פרטיים וחלקם כמערך לוחמה אלקטרוני מאורגן) כחלק ממאמץ מלחמתי נגד מדינת ישראל ומוסדותיה, על מנת לשתק מערכי שירותים לטובת תושבי המדינה ו/או לפגוע בתשתיות (מים, חשמל, תקשורת וכו') כחזית לחימה נוספת במדינת ישראל. בנוסף, מופעלים איומים על מערכות ICT במטרה לבצע נזקים, ואנדליזים, גניבת מידע, ולטובת דרישות כופר כספי. פעולות אלו, מתבצעות באופן שוטף, על ידי גורמים עוינים ומתגברות בעת אירועי לחימה ומבצעים צבאיים. (להלן איומי סייבר)

1.4. המועצה, כחלק מדרישות משרד הפנים ומטה הסייבר במשרד ראש הממשלה, מחויבת לפעול על מנת להגן בפני האיומים השונים ולפעול על מנת לצמצם את הפגיעה בתשתיות המחשוב ומערכות ה ICT בשגרה ובחירום.

1.5. בהתאם להוראות החוק, התקנות, הנחיות משרד הפנים והרשות הלאומית להגנת הסייבר, החליטה הנהלת המועצה להגדיר נוהל התאוששות מאסון (BCP) במערכות ה ICT (להלן הנוהל).

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

2. מושגים

מושג	הסבר
מועצה	מועצה אזורית גזר
מתקפה קבירנטית (או סייבר)	איום תקיפת מערכות מחשוב חיוניות של מתקני תשתית קריטיים למטרת גרימת נזק (כולל לחיי אדם),פגיעה ברציפות התפקודית, השבתה ו /או דלף מידע מסווג הינו בין האיומים המרכזיים הרלוונטיים למתקנים אילו ואשר רמת סבירותם למימוש בעולם המודרני הינה גבוהה
מתקן	מתקנים המפעילים תשתיות קריטיות – כגון מתקני ביוב ו/או מתקנים בהם פועלים תשתיות של המועצה כגון : מוסדות חינוך, מוסדות רווחה, אתרי המועצה וכיו״ב
ממונה תמ״ח	קב״ט המועצה המשמש גם כממונה אבטחת מידע.
מערכות קריטיות	ברשת ה IT : לפי עדיפות : שרת מערכת גבייה וגזברות EPR, שרת דוא״ל, שרת GIS, שרת DC + FS ברשת ה OT : מערכות בקרת מתקנים
ספק המחשוב	חברת נטקור פתרונות מחשוב- פתרונות תקשורת מחשוב ורשתות (פרטי אנשי קשר בנספח לנוהל)
ספק מערכות הנדסיות	חברת בר טכנולוגיות – ספק מערכת לניהול וועדה מקומית לתכנון ובנייה ומערכות GIS נלוות

3. תוכנית התאוששות (BCP)

3.1. מדיניות בתחום מערכות המידע

3.1.1. מסמך זה מתאר את מדיניות ונהלים להתאוששות מאסון טכנולוגי, כמו גם תוכניות ברמת התהליך לשחזור פלטפורמות טכנולוגיות קריטיות ותשתיות תקשורת. מסמך זה מסכם נהלים מומלצים.

3.1.2. המשימה היא להבטיח זמינות של מערכות המידע, שלמות וזמינות הנתונים כמו גם המשכיות עסקית.

3.2. מטרות

המטרה העיקרית של תכנית התאוששות מאסון היא לפתח, לבדוק ולתעד תכנית בנויה היטב וקלה להבנה אשר תסייע למועצה להתאושש במהירות וביעילות ככל האפשר מאסון או חירום בלתי צפויים אשר קוטע את פעילות מערכות המידע והפעילות העסקית.

מטרות נוספות כוללות את הפעולות הבאות:

- הצורך להבטיח שכל העובדים מבינים את תפקידם ביישום תכנית זו.
- הצורך להבטיח כי מדיניות מבצעית תבוצע כחלק מכל הפעילויות המתוכננות.
- הצורך להבטיח שהסדרי החירום המוצעים יעילים מבחינת עלות / תועלת.
- הצורך לשקול את ההשלכות באתרים אחרים של המועצה.
- יכולות התאוששות מאסון צריכות להיות ישימות גם ללקוחות מפתח וספקים.

3.3. סקירת תכנית פעולה

3.3.1. עדכון תכנית

הכרחי שעדכון תהליך התאוששות מאסון יהיה מובנה כראוי ומבוקר. בכל פעם ששינויים שנעשו בתכנית עליהם להיבדק ויש לוודא שהם מתאימים באופן מלא לתוכנית. תיקונים צריכים להיעשות גם לחומרי ההדרכה. תהליך זה יהיה כרוך בשימוש בתוכנית רשמית לשנוי נהלי הבקרה, תחת שליטתו של מנכ״ל המועצה.

3.3.2. תיעוד תכנית

עותקים של תכנית זו, תקליטור, ועותקים קשיחים יהיו מאוחסנים במקומות מאובטחים שיוגדרו על ידי המועצה. לכל חבר הנהלה בכיר יונפק תקליטור ועותק קשיח של התכנית אליו תהיה לו גישה בביתו. גם לכל אחד מחברי צוות ההתאוששות מאסון והשחזור יונפק תקליטור ועותק קשיח של התכנית אליו תהיה לו גישה בביתו. עותק אב של התוכנית יישמר באתר ייעודי לשם כך.

3.3.3. אסטרטגיית גיבוי

להלן מפורטים תהליכים עסקיים מרכזיים ואסטרטגיית גיבוי. האסטרטגיה שנבחרה היא לאתר התאוששות מלא במשרדי המועצה
אסטרטגיה זו כרוכה בתחזוקה של אתר משוכפל בשיקוף מלא שיאפשר מיתוג מיידי בין האתר החי (מטה) ואתר הגיבוי.

3.4. ניהול סיכונים

קיימת קשת של איומים הרסניים פוטנציאליים אשר יכול להתרחש בכל עת ומשפיעים על מתן שירות ותהליכים עסקיים. לקחנו בחשבון מגוון רחב של איומים פוטנציאליים ותוצאות הדיונים שלנו נכללים בסעיף זה. כל מצב אסון או חירום סביבתי פוטנציאלי נבדק. הפוקוס כאן הוא ברמה של שיבוש עסקי, שיכול לנבוע מכל סוג של אסון:

אסון פוטנציאלי	דירוג השפעה	דירוג הסתברות	תיאור קצר של תוצאות אפשריות ופעולות מתקנות
מבול	4	1	כל הציוד הקריטי נמצא בקומת קרקע במשרדי המועצה
אש	4	3	מערכת גילוי וכיבוי אש כולל מטפי גז בחדר המחשבים
מלחמה	5	1	קיים מיגון ברמת דלת פלדלת וחדר ללא חלונות מוגן. (אינו מותקן במקלט)
מעשה טרור קבירנטי	3	2	עדכוני FW יומיים
מעשה חבלה	3	4	עדכוני FW יומיים
הפסקת חשמל ארוכה	4	3	יתירות אל-פסק יחד עם גנרטור המתנה אוטומטי.

אסון פוטנציאלי	דירוג השפעה	דירוג הסתברות	תיאור קצר של תוצאות אפשריות ופעולות מתקנות
			מערך שנבדק מידי שבוע יתירות חיבורי תקשורת מספקים שונים לתוך הבניין. יתירות קו אינטרנט WAN

מקרא: הסתברות : 1 – גבוהה מאוד ; 5 – נמוך מאוד

השפעה: 1 – הרס מוחלט ; 5 – מטרד מינורי

3.5. תגובת חירום

3.5.1. העלאת כוננות, הסלמה ותכנית פעילות

אירועים מפעילי תוכנית. האירועים שיפעילו את תוכנית ה- DR הם:

- אובדן מוחלט של כל התקשורת
- אובדן מוחלט של חשמל
- הצפה של המקום
- אובדן של האתר הראשי של המועצה – בית חשמונאי

3.5.2. נקודת התכנסות

במידה והפעלת השרתים מהמועצה לא מתאפשרות ו/או לא ניתנת לגישה, תכנית ההתאוששות מגדירה 2 נקודות פינוי / התכנסות:

- עיקרי – הפעלת חדר שרתים ממועצה אזורית נחל שורק. (הגיבוי לחדר השרתים של המועצה מתבצע דרך קבע לחדר השרתים במוא"ז נחל שורק)
- חלופי – מטה מל"ח בניין המועצה

3.5.3. צוות תגובת חירום –תפקידים ואחריות

- ספק המחשוב – אחריות על רשת ה IT של המועצה ורשת הטלפוניה

נהלי מחשוב ואבטחת מידע – נוהל התאוששות מאסון

- ספק מע' המידע – אחריות על מערכות הגבייה של המועצה
- ספק מע' הנדסיות – אחריות על שירות למערכת ההנדסיות של המועצה

אחריות בעלי תפקידים במועצה:

- יועץ המחשוב – זמינות 24/7 למתן סיוע טכני וייעוץ בכלל תחומי המחשוב, רשת IT ורשת OT ומע' המידע של המועצה.
- ממונה תמ"ח – זמינות לפי קריאה למתן סיוע לוגיסטי בתחומי המחשוב של המועצה.
- רשימת טלפונים ואנשי קשר מובאת בנספח לנוהל.

3.5.4. הפעלה של צוות תגובת החירום

כאשר מתרחש אירוע החירום צוות התגובה חייב להיות מופעל. ההנהלה תחליט אם צריך להפעיל את תוכנית ההתאוששות מאסון ולבצע את הפעולות הבאות.

- תגובה מיידית לאסון פוטנציאלי ויצירת קשר עם לשירותי החירום;
- הערכה של היקף האסון והשפעתו על העסקים, מרכז הנתונים, וכו';
- קבלת החלטה אילו אלמנטים של תכנית ה- DR צריכים להיות מופעלים;
- להקים ולנהל את צוות ההתאוששות מאסון כדי לשמור על שירותים חיוניים ולחזור לפעולה רגילה;
- לוודא שהעובדים מיודעים על אירוע האסון ולהקצות תחומי אחריות ופעילות כנדרש.

3.6. צוות התאוששות מאסון

ההנהלה תיצור קשר עם הצוות ההתאוששות מאסון. אחריות הצוות כוללת:

- החזרת שירות / תקשורת למתקני המים והביוב שנפגעו בתוך 1 יום עבודה;
- שיחזור השירותים המרכזיים בתוך 3 ימי עבודה מתחילת האירוע;
- שיחזור השירותים המרכזיים לעסקים כרגיל בתוך 7 ימי עבודה מתחילת האירוע;
- תיאום פעילויות צוות ההתאוששות מאסון, מגישי עזרה ראשונה, וכוי.
- דיווח לצוות תגובת החירום.

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

3.7. התראה, הפעלה והסלמת תוכנית חרום

מדיניות והליך זה הוגדרו כדי להבטיח כי במקרה של אסון או משבר, לאנשים תהיה הבנה ברורה עם מי צריך להיות בקשר. נהלים הוגדרו על מנת להבטיח כי תקשורת תתקיים במהירות תוך הפעלת התאוששות מאסון.
תכנית התאוששות מאסון תסתמך בעיקר על אנשי מפתח בהנהלה וצוות עובדים שיוכלו לספק את הכישורים הטכניים וכישורי הניהול ההכרחיים כדי להשיג התאוששות טכנולוגית ועסקית חלקה.
ספקים של סחורות ושירותים חיוניים ימשיך לתמוך בהתאוששות של הפעילות העסקית במועצה עד שזו תחזור למצב פעולה רגיל.

3.7.1. התראה לשעת חירום

על האדם שגילה את האירוע לקרוא לחבר בצוות החירום לפי הסדר הרשום: צוות תגובת חירום אם לא זמינים נסה את:
צוות תגובת החרום הוא האחראי על הפעלת תוכנית ההתאוששות מאסון שהוגדרו בתכנית זו, כמו גם במקרה של כל התרחשות אחרת שמשפיעה על היכולת של המועצה להתנהל כרגיל.
אחת המשימות במהלך השלבים המוקדמים של אירוע החירום הוא להודיע לצוות ההתאוששות מאסון כי אירוע חירום התרחש. ההודעה תבקש מחברי צוות החירום להתאסף באתר בו התרחשה הבעיה ותספק מספיק מידע כדי שהתקשורת תהיה יעילה מספיק. קבוצת השחזור העסקי תהיה מורכבת מנציגים בכירים ממחלקות העסקים העיקריות של המועצה. מנהל קבוצת השחזור העסקי יהיה חבר בכיר בצוות הניהול של המועצה ויהיה אחראי ללקיחת אחריות כוללת של התהליך ההתאוששות בכדי להבטיח שהמועצה תחזור לפעילות רגילה מוקדם ככל האפשר.

3.8. תהליך התאוששות מאסון להנהלה

חברי צוות ההנהלה ישמרו עותק קשיח של השמות ומספרי קשר של כל אחד מהעובדים במחלקות שלהם. בנוסף, לחברי צוות הניהול יהיו עותק קשיח של תוכנית ההתאוששות מאסון וההמשכיות העסקית של המועצה בבתיהם, במקרה שהבניין המטה אינו נגיש, שמיש, או שזה נהרס.

נהלי מחשוב ואבטחת מידע – נוהל התאוששות מאסון

3.8.1. יצירת קשר עם העובדים

המנהלים ישמשו כנקודת קשר למחלקותיהם, עובדים מיועדים יקראו לעובדים אחרים כדי לדון במשבר / אסון ובתוכניות ההתאוששות המידיות של המועצה.

3.8.2. צוות גיבוי

אם חבר צוות מנהל או המיועד ליצור קשר עם אנשי צוות אחרים אינו זמינים, חבר צוות הגיבוי הייעודי יבצע את תפקידי היידוע.

3.8.3. הודעות / עדכונים מוקלטים

למידע העדכני ביותר על האסון והתגובה של הארגון, יש לאפשר לחברי הצוות להתקשר למוקד שיוגדר מראש . ההודעות יכללו נתונים על טיבו של האסון, אתרי ההתארגנות, ועדכונים על עבודת חידוש הפעילות.

3.8.4. אתר שחזור חלופי

במידת צורך, האתר החם שהוגדר מראש יופעל והודעה על כך תינתן באמצעות הודעה מוקלטת או באמצעות תקשורת יזומה עם חברי הצוות.

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

4. נספח רשימת בעלי תפקידים

#	תחום אחריות	פרטי איש קשר ודרכי התקשרות
1	ספק המחשוב (רשת IT וטלפוניה)	חב' נטקור משרדים: 1-700-706-806 נייד ארז מוסקוביץ' (מנהל טכני אחראי): 054-991.0840
2	ספק מע' הבקרה	קבלן תחזוקת מתקנים של המועצה שמואל הררי מנהל מח' אחזקה: משרדים 08-9274003; נייד 052-5344562.
3	ספק מע' המידע לגבייה וניהול הכנסות	חברת EPR- systems 02-9947199 אלי אלול מנהל טכני אחראי: 052-833.6997
4	יועץ המחשוב – עזרא דיין	משרדים: 072-2504385 נייד: 052-6704546
5	קב"ט המועצה וממונה תמ"ח - אליק מגורי כהן	משרדים: 08-9274060 נייד: 052-289.1362