מספר הנוהל : 63	מועצה אזורית עמק המעיינות
שם הפרק: ארגון ושירות	
שם הנוהל : נוהל טיפול באירועי אבטחת מידע וסייבר	הוראות נוהל זה גוברות על כל הוראות קודמות בנוהל קודם
הנוהל אושר בהחלטת: מטה המועצה 03.07.2022	תאריך פרסום: 03.07.2022

נוהל טיפול באירועי אבטחת מידע וסייבר

1. כללי

המידע האגור במאגרי המידע ובמערכות המחשוב הינו משאב קריטי, עיקרי ובעל ערך מהותי לפעילות המועצה. על כן, ההגנה והשמירה על המידע, מניעת שיבושו ומניעת שימוש לא מאושר בו, מהווים מטרה מרכזית עבור הנהלת המועצה והעובדים.

2. מטרת הנוהל

- קביעת נוהל אחיד אשר יגדיר את אופן הדיווח והטיפול באירועי אבטחת מידע.
- צמצום הנזק הנובע מאירועי אבטחת מידע, ניטור אירועים אלו וביצוע הפקת לקחים.
- הגדרת תהליך הדיווח על אירועי אבטחת מידע וקביעת זהות הגורמים המעורבים בתהליך זה.
- הגדרת התהליך והמתודולוגיה של תגובה לאירועי אבטחת מידע.

3. אחריות ליישום הנוהל

מנהל מערכות מידע, מנהלי אגפים, מנהלי מחלקות היועץ המשפטי.

אחריות ליישום סעיפים 8 ו-9 חלה על כל עובדי הרשות.

תפוצה : כל עובדי המועצה

4. הגדרות

- **נכס מידע** – מאגר נתונים, רכיב מערכת (לרבות חומרה ותוכנה) המשמש לאחסון, ניהול, עיבוד והעברה של מידע, ו/או לתפעול, שליטה ובקרה
- **אירוע אבטחת מידע או אירוע סייבר –** כל מקרה של **תקיפת נכס מידע** השייך לרשות, העלול לפגוע בסודיות, שלמות או זמינות מערכות או המידע, לרבות שימוש במידע בלא הרשאה או בחריגה מהרשאה

- **משבר סייבר (Cyber Crisis)/אירוע סייבר משמעותי** : אירוע סייבר אשר עלול להיות לו השפעה מהותית על המועצה. מצב שיש בו איום ממשי לפגיעה בנכס מידע הקשור לתהליך ליבה, או פגיעה בו בפועל, אשר עלול לגרום נזק קריטי לשגרת הפעילות של המועצה, לתדמית, לנזק כלכלי.
- **התרעת אבטחת מידע** - דיווח על קיומו של אירוע אבטחת מידע באמצעות מערכת ניטור ובקרה ממוחשבת או בכל אמצעי אחר.
- **איום** – אפשרות פוטנציאלית לפגיעה בנכס מידע של המועצה, ו/או בסודיות ,שלמות ,או זמינות של מידע, לרבות שימוש במידע בלא הרשאה או בחריגה מהרשאה.
- **חשיפה** - חולשה של נכס או מערכת מידע העלולה להיות מנוצלת על ידי איום.
- **השפעה** - תוצאה של אירוע אבטחת מידע.
- **התקפה** - שורה של צעדים הננקטים על ידי תוקף עם כוונה לממש איום על המידע/הנכסים הארגוניים.
- **שינוי מידע** - שינוי בלתי מורשה של תוכן או מאפיינים של מידע.
- **פעילות מתקנת –** פעילות המבוצעת לצורך התמודדות עם אירוע אבטחת מידע שקרה.
- **פעילות מונעת –** פעילות המבוצעת לצורך מניעת אירועי אבטחת מידע וכן הישנות של אירוע אבטחת מידע שקרה בעבר.
- **צוות תגובה טכנולוגי – CSIRT (Computer Security Incident Response Team) –** צוות מקצועי להתמודדות עם ההיבטים הטכנולוגיים הקשורים לאירוע הסייבר והשפעתם הישירה על נכסי הסייבר של המועצה כמפורט בס' 7.1 להלן.
- **צוות ניהול משבר –** צוות לניהול האירוע/ המשבר מעבר להיבטים הטכנולוגיים. התמודדות עם השלכות בהיבטים פנים-ארגוניים וחוץ –ארגוניים כגון: השלכות של רציפות תפקודית, השלכות עסקיות, השלכות כלכליות, השלכות משפטיות, השלכות רגולטוריות, השלכות תדמיתיות ועוד כמפורט בס' 7.2 להלן.
- **משתמש קצה-** כל עובדי המועצה.

5. מסמכים / נהלים קשורים

טופס תיעוד אירוע אבטחת מידע – ימולא על ידי ממונה אבטחת מידע וסייבר.

מספר הנוהל : 63	מועצה אזורית עמק המעיינות
שם הפרק: ארגון ושירות	
שם הנוהל : נוהל טיפול באירועי אבטחת מידע וסייבר	**הוראות נוהל זה גוברות על כל הוראות קודמות בנוהל קודם**
הנוהל אושר בהחלטת: מטה המועצה 03.07.2022	**תאריך פרסום: 03.07.2022**

6. מסגרת נורמטיבית

מדיניות הרשות להגנת הפרטיות בנוגע לקבלת דיווח אירוע אבטחה חמור - 2018 ;

תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017;

7. צוותי תגובה לאירועי אבטחת מידע וסייבר

7.1. צוות תגובה טכנולוגי - לאירועי אבטחת מידע וסייבר **יוקם צוות תגובה טכנולוגי** (CSIRT) אשר יורכב מבעלי התפקידים הבאים:

- מנהל מערכות מידע– ראש הצוות
- ממונה אבטחת מידע וסייבר
- מנהל רשת
- בעלי תפקידים נוספים על פי העניין, כגון יועצים חיצוניים, ועוד.

הצוות הטכנולוגי יפעל לניהול , לצמצום ולעצירת השפעות האירוע בהיבט הטכנולוגי וידווח באופן שוטף לצוות ניהול המשבר.

כמו כן, צוות התגובה הטכנולוגי יפנה לקבלת סיוע מהגורמים החיצוניים של המועצה (רשות הסייבר הלאומית, ייעוץ סייבר, ניטור לוגים ועוד) על פי הצורך והערכת המצב.

במסגרת זו, גם תישקל פנייה לIL -cert להתייעצות וקבלת סיוע בהתאם לצורך.

7.2. צוות ניהול משבר - למשברי CYBER , ו/או לאירועי אבטחת מידע וסייבר משמעותיים (דרגת חומרה חמורה), **יוקם צוות ניהול משבר** אשר יורכב מבעלי התפקידים הבאים:

- מנכ"לית המועצה – ראש הצוות;
- צוות תגובה טכנולוגי בהתאם להגדרתו בסעיף 7.1 לעיל;
- יועמ"ש ראשי ;
- מנהל הכספים;
- מנהלת אגף הון אנושי ומינהל;
- בעלי תפקידים נוספים על פי העניין.
- צוות ניהול <u>המשבר ינהל את האירוע בהיבטים **מעבר** להיבטים הטכנולוגיים</u> ויתייחס לתחומים שונים בהתאם לסוג האירוע, להשלכותיו השונות ולהיקפו, כגון:
  - דוברות (הודעות ותגובות לתקשורת, מבוטחים ועוד על פי העניין) - **באחריות המנכ"ל;**
  - הודעות לתושבים, ספקים, עובדים – עפ"י העניין) – **מנהלי אגפים לפי תחום אחריות או מי שיוסמכו על ידם;**
  - דיווח למשרד הפנים– **באחריות היועמ"ש הראשי;**
  - דיווחים לרשות להגנת הפרטיות- **באחריות היועמ"ש הראשי**

מספר הנוהל : 63	מועצה אזורית עמק המעיינות
שם הפרק: ארגון ושירות	
שם הנוהל : נוהל טיפול באירועי אבטחת מידע וסייבר	**הוראות נוהל זה גוברות על כל הוראות קודמות בנוהל קודם**
הנוהל אושר בהחלטת: מטה המועצה 03.07.2022	**תאריך פרסום: 03.07.2022**

- הפעלת התוכנית להמשכיות עסקית של הרשות במלואה או חלקים ממנה על פי העניין – **באחריות מנהלת אגף הון אנושי.**
- ניהול סחיטות ובקשות כופר - **באחריות מנהל הכספים ;**
- היבטים משפטיים/רגולטוריים - **באחריות היועמ"ש הראשי;**
- פנייה למשטרה - **באחריות היועמ"ש הראשי;**
- ועוד

הצוותים יפעלו לניהול האירוע/ המשבר, לצמצום ועצירת נזקים ולהפקת לקחים.

8. גילוי וזיהוי אירועי אבטחת מידע

לרב, ניתן לגלות אירוע אבטחת מידע באופנים הבאים:

8.1. זיהוי ע"י אנשי מחלקת המחשוב באמצעות מערכות/כלי זיהוי אוטומטיים:

- כלים/ מנגנונים ייעודיים לאבחון והתראה, כדוגמת מערכת אנטי וירוס, מערכת FW, וכו'.
- הודעות ועדכונים מגופים חיצוניים כדוגמת: ספקי תוכנות האנטי וירוס, ספקי מערכות, רשות Cert-IL.
- התראות המיוצרות על ידי מערכות מידע (אזהרות מערכת או הודאות שגיאה).

8.2. זיהוי ע"י משתמשי קצה:

- משתמש קצה, המבחין באי סדירות או אירועים חשודים בסביבת העבודה שלו (לדוגמא: איבוד גישה לקבצים, תקלות במערכות, נעילת משתמש, התראות מוזרות על המסך ואירועים נוספים כמפורט בהמשך הנוהל).
- משתמש המבחין באי סדירות של תהליכים בסביבת העבודה שלו (לדוגמא, ניצול לרעה של סמכויות עובדים לצורך עדכון/שיבוש/שינוי מידע ותהליכים עסקיים).
- משתמש המבחין בחריגה מנהלי העבודה התקינים והמקובלים בחברה.

משתמשי קצה ידווחו על כל פעילות חשודה, או לא רגילה בחשבונות שלהם וסביבת העבודה שלהם. לדוגמא:

- נעילה פתאומית של שם המשתמש.
- זמן כניסה אחרון לא הגיוני (במערכות המציגות מידע זה).
- סימנים לפעילות לא ידועה (לדוגמא: קבצים חדשים , שינוי בשולחן העבודה).
- הפרה של נוהלי אבטחת מידע על ידי העובד או על ידי עובדים אחרים.
- קיום או חשד לפרצה / חשיפה באבטחת המידע באחת המערכות.
- חשד שמידע נפגע או עלול להיפגע (נחשף ,שונה או נמחק).
- ניסיונות (מוצלחים או כושלים) להשגת גישה לא מאושרת למערכת או למידע.
- הפרעה של חוסר זמינות בשירות.

- שינוי בחומרת או תוכנת מערכת ללא אישור בעל המערכת.

8.3. מנהלי מערכות הינם מקור חשוב לדיווח על אירועי אבטחה. באמצעות הידע הטכני הרב שצברו, הם יכולים לזהות אירועי אבטחה מתוך כלל האירועים במערכות. על מנהלי המערכות להיות ערניים לאירועים חשודים במערכת כדוגמת:

- תהליכים, או אפליקציות לא רגילות.
- חיבורי רשת לא מוכרים.
- ניסיונות כניסה כושלים החוזרים על עצמם.
- קבצים ששונו שלא באופן סביר או רצוי, או שנמחקו ללא שהיו אמורים להימחק.
- פעילות מרובה / לא מוכרת ברשת המחשוב או באחת המערכות.

9. הליך דיווח על קרות אירוע אבטחה בתוך הרשות

9.1. באחריות כל עובדי הרשות לדווח מידית על כל חשד לאירוע אבטחת מידע. הדיווח יימסר למנהל הישיר, או למוקד תמיכה טכנית, או ישירות לאחד מחברי צוות התגובה הטכנולוגי כמפורט בסעיף 7 לעיל.

9.2. דיווחים יימסרו באמצעות טלפון וישלח תיעוד של האירוע בדואר אלקטרוני או באמצעות מערכת הפניות של הרשות.

9.3. במקרים בהם יש חשיבות למהירות התגובה למניעה/צמצום הנזק, דיווח ראשוני יבוצע באופן ישיר או טלפונית על מנת להבטיח תגובה מהירה ואפקטיבית.

9.4. מקבל ההודעה, לרבות מוקד תמיכה טכנית, יעדכן באופן מידי את מנהל מערכות מידע אשר יכנס את צוות התגובה הטכנולוגי.

9.5. מנהל מערכות מידע ידווח על האירוע למנכ"ל הרשות ויקבע האם יש צורך בכינוס צוות ניהול המשבר בכל שלב של האירוע, על פי אופי האירוע והשלכותיו.

9.6. אירועים אשר מערבים הפרה של נהלים על ידי עובדי המועצה ידווחו על ידי מנהל מערכות מידע גם למנהל המחלקה הרלוונטית.

9.7. צוות התגובה הטכנולוגי יערוך ניתוח ראשוני של האירוע וינחה את משתמשי הקצה כיצד לפעול.

10. שלבים לתגובה לאירוע סייבר

כל אירוע סייבר יכול לכלול טיפול שונה בהסתמך על מקורו והנזק הפוטנציאלי, עם זאת התהליך הכללי של תגובה לאירוע סייבר יכלול, לאחר גילויו ודיווח עליו לגורמים האחראים ברשות, את השלבים הבאים:

מספר הנוהל : 63	מועצה אזורית עמק המעיינות
שם הפרק: ארגון ושירות	
שם הנוהל : נוהל טיפול באירועי אבטחת מידע וסייבר	הוראות נוהל זה גוברות על כל הוראות קודמות בנוהל קודם
הנוהל אושר בהחלטת: מטה המועצה 03.07.2022	תאריך פרסום: 03.07.2022

10.1. ניתוח – בירור מקיף ותחקור של אופי ההתרחשות לצורך הבנת האירוע, תוך איסוף מידע וראיות, בידוד הרכיב הנגוע, חקירה לאיתור פרצות נוספות ובחינת השלכות האירוע על הארגון מעבר להיבט הטכנולוגי במידת הצורך.

10.2. הערכות מצב – קבלת תמונת מצב עדכנית ותוצאות ניתוח האירוע, בחינת דרכי פעולה להתמודדות עם האירוע , קבלת החלטות.

10.3. הכלה ובלימה – נקיטת צעדים לבלימת המתקפה ומניעת התרחבותה לנכסי מידע אחרים ברשות, השגת שליטה, ועצירת החמרת הנזק שנגרם מהאירוע , אם נגרם, מעבר להיבטים הטכנולוגיים (פגיעה במידע רגיש, פגיעה ברציפות תפקודית, נזק כלכלי, נזק תדמיתי ועוד).

10.4. זיכוי/הכרעה – נטרול רכיבי הפגיעה והסרתם מנכסי המידע של המועצה תוך מאמץ למזער את הנזק שנגרם.

10.5. התאוששות והפקת לקחים– חזרה מבוקרת לשגרה ולפעילות תקינה, הכרזה על סיום המשבר, ביצוע תחקיר מקיף והפקת לקחים.

לאחר סיום הטיפול באירוע, באחריות ממונה אבטחת מידע וסייבר **לפעול תחקור מעמיק של האירוע** במטרה לזהות ולהבין את הפרצות והליקויים שאפשרו את קיום האירוע ולהגדיר את הצעדים שיש לנקוט על מנת למנוע הישנות של אירועים אלו בעתיד (פעילות מונעת) ולתעד את התחקיר בהתאם.

11. תיעוד האירוע

11.1. איסוף מידע ותיעוד יתבצע לאורך כל תהליך ההתמודדות עם האירוע ועד לסיומו ויכלול איסוף של כל המידע הידוע אודות האירוע. המידע ייאסף מגורמים פנימיים (לדוגמא משתמשי מערכת, מנהלי רשת וכו') וכן ממקורות חיצוניים (לדוגמא: אינטרנט, מאגרי מידע ציבוריים, מומחים חיצוניים, יועצים וכו'). כל החומר הרלוונטי לאירוע יתועד וישמר.

11.2. איסוף ותיעוד ראיות משפטיות: במידה והאירוע קרה כתוצאה מהפרת נהלים על ידי אחד מעובדי המועצה, או במידה והאירוע ידרוש פעולה משפטית כנגד גורם חיצוני כלשהו יש לאסוף ולתעד ראיות בקפדנות. חשוב לשמור על שלמות ומהימנות הראיות על מנת לנקוט באמצעים המשפטיים הנדרשים בעת הצורך. היועץ המשפטי, או מי מטעמו, ייעץ למנהל אבטחת המידע בנושא איסוף הראיות ותיעודן.

11.3. דוח אירוע - באחריות ממונה אבטחת מידע להפיק, בגין כל אירוע סייבר או משבר סייבר דוח אירוע אשר יכלול לכל הפחות את הפרטים הבאים:

- פרטי המשתמש המדווח.
- תאריך וזמן האירוע.
- תיאור מפורט של האירוע.
- תיאור של פעולות שננקטו בתגובה (במידה וננקטו).

- הפקת לקחים ופעילות ליצירת בקרה מונעת/ מגלה/ מתקנת (במידה ורלוונטי).
- פירוט הגורמים אשר קיבלו דיווח על האירוע, במידה ובוצע דיווח (הרשות להגנת הפרטיות, משרד הפנים)

12. חובת דיווח אירוע/משבר סייבר

12.1. דיווח לרשות להגנת הפרטיות על אירוע חמור –

בעל מאגר מידע שחלה עליו חובת אבטחה בינונית או גבוהה (כהגדרתן בתקנות) מחויב להודיע באופן מידי לרשות על אירוע אבטחה חמור וכן ידווח לרשות על הצעדים שנקט בעקבות האירוע.
על הדיווח להתבצע **תוך 24 שעות ממועד גילוי האירוע** ובכל מקרה **לא יאוחר מ 72 שעות** מאותו מועד.
הדיווח **באחריות מזכיר המועצה והיועמ"ש הראשי** ויתבצע באמצעות טופס דיווח מקוון המפורסם באתר האינטרנט של הרשות
https://formspdf.justice.gov.il/PrivacyProtectionAuthority/ReportingSecurityIncident.aspx

לאחר דיווח האירוע, יחל תהליך מול רשות הגנת הפרטיות כמפורט להלן:

- הרשות תבחן את פרטי הדיווח ,ונציג הרשות ייצור קשר עם הגורם המדווח על מנת לאמת את המידע ובמידת הצורך לקבל פרטים נוספים אודות האירוע , ובכדי לקבוע האם יש צורך בפרטים נוספים (במילויו של טופס דיווח מורחב שיועבר למדווח בכדי לאסוף פרטים נוספים הנדרשים לשם בחינת אופן הטיפול באירוע.)
- לאחר קבלת כל הפרטים על האירוע, תקבע הרשות את חומרת האירוע בין היתר בהתחשב בקריטריונים הבאים : רגישות המידע שדלף ,מקור הנזק ,היקף דלף המידע ,האם המידע דלף בפועל מחוץ לארגון או שרק קיים סיכון שידלוף ,כמות נושאי המידע שיש חשש שמידע אודותיהם דלף ,הנזק שעלול להיגרם לנושאי המידע, הנזק שעלול להיגרם לגורם המדווח ,למגזר או למשק ,והתנהלות הארגון בקשר עם האירוע ומוכנותו. בהתאם לסיווג חומרת האירוע ,תקבע הרשות את המשך הטיפול באירוע – קביעת הנחייה להמשך מעקב אחר הטיפול באירוע , קביעת הנחיות לתיקון ליקויים ,פיקוח או חקירה בחצרי הגורם המפוקח ,קביעה פורמלית כי הגורם המפוקח הפר את הוראות החוק ו/או התקנות ,ובמקרים המתאימים הטלת סנקציות לרבות התלייה או ביטול רישום המאגר ,בכפוף למתן זכות שימוע . בנוסף ,תקבע הרשות האם נדרש להודיע על האירוע לנושאי המידע שעלולים להיפגע מן האירוע ,ועל אופן ההודעה ותזמונה.
- בהחלטה להודיע על אירוע אבטחה חמור לנושאי המידע יילקח בחשבון האם המידע האישי אכן דלף בפועל או שרק קיים סיכון לכך שידלוף ,וכן מה מידת הנזק הצפויה לנושאי המידע . ההחלטה לחייב הודעה לנושאי המידע תבוצע בהתייעצות עם מערך הסייבר ,ובהתאם לנסיבות גם בתיאום עם הרגולטור המגזרי.

- קביעת הפרה כמתואר לעיל ,תפורסם באתר הרשות ו/או באופן פומבי אחר ,על פי שיקול דעתה של הרשות.
- במקרה שהרשות הנחתה לבצע תיקון ליקויים בעקבות האירוע ,ינוהל מהלך בקרה ויעדכן הגורם המפוקח את הרשות באשר לתהליך תיקון הליקויים. והרשות תהיה רשאית לערוך בקרה בנושא. יודגש כי אי דיווח כנדרש על פי התקנות או הפרת הוראות הרשות מהוות הפרה בפני עצמה ,ולרשות עומדות סמכויות האכיפה כמפורט בחוק.

13. טיפול משמעתי

- במידה והתבצעה עבירת אבטחת מידע יש לשקול צעדים משמעתיים נגד מבצעי העבירה.
- **המלצה על נקיטת צעדים משמעתיים כנגד עובדי המועצה:** צעד זה יבוצע על ידי הממונה על אבטחת המידע וסייבר ברשות. חומרת הצעדים תיקבע בהסתמכות על הפרמטרים הבאים:
  - ❖ האם הפרת הנהלים בוצעה מתוך כוונה תחילה או כתוצאה מרשלנות.
  - ❖ היקף הנזק שנגרם.
  - ❖ עבירות אבטחה / משמעת קודמות של העובד.

  המלצה להמשך הטיפול המשמעתי הנדרש תועבר למנהל משאבי אנוש ומנכ"ל.

מספר הנוהל : 63	מועצה אזורית עמק המעיינות
שם הפרק: ארגון ושירות	
שם הנוהל : נוהל טיפול באירועי אבטחת מידע וסייבר	הוראות נוהל זה גוברות על כל הוראות קודמות בנוהל קודם
הנוהל אושר בהחלטת: מטה המועצה 03.07.2022	תאריך פרסום: 03.07.2022

14. דגשים לטיפול באירועי אבטחה ספציפיים

להלן דגשים לטיפול באירועי אבטחת מידע. **בכל אירוע יש לפעול על פי הוראות הנוהל המלא** תוך וידוא כי הדגשים המפורטים להלן מבוצעים.

מס'	אירוע	תגובה
1	התרעה על סימני פריצה ברכיבי תקשורת (לוגים של המערכת, שינויים בלתי מוסברים בקבצי מערכת או בקבצי אבטחה) (פגיעה בסודיות / שלמות / זמינות המידע).	▪ בעת גילוי סימני פריצה לרשת או זיהוי רשת אלחוטית שאינה מורשית, יש ליידע את הממונה על אבטחת המידע. ▪ צוות התגובה יפעל לגילוי מקור התקיפה והערכת מידת הנזק שנגרם לארגון ולמידע. ▪ צוות התגובה יחליט על צעדי מנע שניתן לנקוט במערכת, על מנת למנוע הישנות האירוע. ▪ הממונה על אבטחת המידע ידווח ל הנהלת הרשות ויוחלט על דיווח לגורמים נוספים במידת הצורך ומהות הנזק שנגרם, לרבות לחברת האם. ▪
2	אירועי התקפה מסוג **Denial Of Service** , נפילות בלתי מוסברות של שרתים. (פגיעה בזמינות).	▪ צוות המחשוב יידע את הממונה על אבטחת המידע. ▪ הממונה על אבטחת המידע יידע את מנהל אבטחת המידע בדבר האירוע ויפעיל את צוות התגובה לאירועי אבטחת מידע. ▪ צוות התגובה יפעל לחקירת האירוע – לרבות מקור ומאפייני המתקפה. ▪ מחלקת מערכות המידע וממונה אבטחת המידע יבחנו אפשרויות להעלאת רמת האבטחה של המערכת המותקפת. ▪ הממונה על אבטחת המידע יבצע אסקלציה לגורמי הנהלה, במידת הצורך.
3	אירוע התקפה מסוג כופרה (Ransomware)	▪ עם התפרצות האירוע, צוות המחשוב יידע את הממונה על אבטחת המידע. ▪ הממונה על אבטחת המידע יפעיל את צוות התגובה לאירועי אבטחת המידע לצורך עצירת האירוע ולצורך ביצוע חקירה של המתקפה. ▪ צוות המחשוב ינתק את התחנה שהודבקה בכופרה מהרשת. ▪ סיסמת המשתמש ששימש את וירוס הכופרה להצפנת הקבצים תוחלף מידית.

מספר הנוהל : 63	מועצה אזורית עמק המעיינות
שם הפרק: ארגון ושירות	
שם הנוהל : נוהל טיפול באירועי אבטחת מידע וסייבר	**הוראות נוהל זה גוברות על כל הוראות קודמות בנוהל קודם**
הנוהל אושר בהחלטת: מטה המועצה 03.07.2022	**תאריך פרסום: 03.07.2022**

		▪ יאותרו כלל הקבצים שהוצפנו ברשת ע"י חיפוש סיומות רלוונטיות בהתאם לסוג הכופרה. ▪ הקבצים המוצפנים ישוחזרו מהגיבוי האחרון הזמין. ▪ המחשב הנגוע יפורמט ויוחזר לשימוש. ▪ הממונה על אבטחת המידע ידווח להנהלת הרשות ויוחלט על נקיטת צעדים נוספים ודיווח לגורמים נוספים במידת הצורך ומהות הנזק שנגרם, לרבות לחברת האם.
4	עובד הרשה ביודעין לגורם זר לפעול תחת "זיהוי המשתמש" שלו (פגיעה בסודיות / שלמות / זמינות).	▪ סיסמתו של העובד שמסר את הסיסמא שלו לעובד אחר תוחלף באופן מידי. ▪ דיווח מידי יועבר לממונה הישיר על העובד, אשר ישקול יחדיו עם הממונה על אבטחת המידע נקיטת צעדים משמעתיים נוספים כנגד העובד – בשיתוף מנהלת משאבי אנוש.
5	עובד פעל במסגרת הרשאות של עובד אחר שהשאיר את מסופו פתוח **(עבירת משמעת).**	▪ סיסמתו של העובד שהשאיר את מסופו פתוח תוחלף לסיסמא חדשה באופן מידי. ▪ דיווח מידי יועבר לממונה הישיר על שני העובדים (העובד שהשאיר את מסופו פתוח והעובד שניצל את המצב כדי לגשת לעמדה ולבצע פעולות לא מורשות בשם אותו משתמש) אשר ישקול יחדיו עם הממונה על אבטחת המידע נקיטת צעדים משמעתיים נוספים כנגד שני העובדים בשיתוף מנהלת משאבי אנוש. ▪ צוות התגובה יבחן השלכות של האירוע והאם נגרם נזק – ויפעל בהתאם להנחיות נוהל זה
6	עובד פיצח במכוון סיסמא של עובד אחר (עבירת משמעת).	▪ סיסמתו של העובד שסיסמתו פוצחה, תוחלף באופן מיידי. ▪ דיווח מידי יועבר לממונה הישיר על העובד, אשר ישקול יחדיו עם הממונה על אבטחת המידע נקיטת צעדים משמעתיים נוספים כנגד העובד שפיצח את הסיסמא בשיתוף מנהלת משאבי אנוש. ▪ צוות התגובה יבחן השלכות של השימוש בסיסמה והאם נגרם נזק- ויפעל בהתאם להנחיות נוהל זה
7	עובד גילה כי נעשו ניסיונות גישה (לא מוצלחים) לחשבונו, ע"י גורם זר (גילוי ראשון). (ניסיון לפגיעה בסודיות / שלמות / זמינות).	▪ העובד ידווח לממונה על אבטחת המידע וכן למנהלו הישיר. ▪ העובד יחליף את סיסמת הגישה שלו. ▪ מנהל אבטחת המידע יחקור את האירוע. ▪ יש לבחון הידוק פרמטרי אבטחה במערכת בכלל, ולגבי המשתמש הספציפי בפרט.

מספר הנוהל : 63	
שם הפרק: ארגון ושירות	
שם הנוהל : נוהל טיפול באירועי אבטחת מידע וסייבר	**הוראות נוהל זה גוברות על כל הוראות קודמות בנוהל קודם**
הנוהל אושר בהחלטת: מטה המועצה 03.07.2022	**תאריך פרסום: 03.07.2022**

		▪ צוות התגובה יבחן השלכות של האירוע - ויפעל בהתאם להנחיות נוהל זה