נוהל מאגרי מידע

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

1. כללי

1.1. הגדרות :

1.1.1. "**מאגר מידע**" - אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט : (1) אוסף לשימוש אישי שאינו למטרות עסק ; או (2) אוסף הכולל רק שם, מען ודרכי התקשרות שכשלעצמו אינו יוצר אפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף ;

1.1.2. "**מידע**" - נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו ;

1.1.3. "**מידע רגיש**" - (1) נתונים על אישיותו של אדם, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו ; (2) מידע ששר המשפטים קבע בצו, באישור ועדת החוקה חוק ומשפט של הכנסת, שהוא מידע רגיש ;

1.1.4. "**מנהל מאגר**" - מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לעניין זה ;

1.1.5. "**ממונה אבטחת מידע**" - אדם שמונה לממונה על אבטחת מידע לפי סעיף 17ב לחוק הגנת הפרטיות תשמ"א-1981 (להלן : "**החוק**") או אדם שמנהל המאגר קבע כי הוא אחראי על אבטחת המידע שבמאגר המידע. לעניין זה, ובהתאם לסעיף 17ב לחוק, הממונה יהיה אחראי לאבטחת המידע במאגרים המוחזקים במועצה וכן לא ימונה כממונה מי שהורשע בעבירה שיש עמה קלון או בעבירה על הוראות החוק.

1.1.6. "**משתמש**" - מי שקיבל, על פי הוראות נוהל זה, הרשאת גישה למאגר מידע של המועצה.

1.1.7. "**בקרה לוגית**" - ניטור שוטף ממוחשב אחר הפעילות במערכת הממוחשבת, תוך התמקדות באירועים חריגים או רגישים.

1.1.8. "**פיקוח לוגי**" - מעקב אחר פעילויות במחשב גם לאחר ביצוע הפעילות ובהשהיית זמן כלשהו.

1.1.9. "**אמצעים מגנטיים**" - אמצעים עליהם ניתן לאחסן תכנות ונתונים באופן מגנטי כולל אמצעים מגנטיים נתיקים הניתנים להפרדה פיסית מציוד המחשוב.

1.1.10. "**סיסמה**" - רצף של תווים המהווים ביחד תנאי סף להתחברות אל מערכת ממוחשבת ו/או לצורך קבלת הרשאה מהמערכת הממוחשבת לצורך ביצוע פעולות.

1.1.11. "**לוג**" - יומן אירועים ופעולות המנוהל אוטומטית על ידי התכנה ובו נרשמות פעולות המבוצעות במחשב.

1.1.12. "**רמת אבטחה**" - על פי הגדרתה בתקנות הגנת הפרטיות. רמת אבטחה החלה על מאגר מידע על פי סיווג המידע הקיים בו.

1.1.13. "**אירוע אבטחה**"- מקרה בו עובד או מערכת הקיימת ברשות ספקי המחשוב ומערכות המידע, מעריכים עפ"י המידע העומד לרשותם ו/או על פי תסמינים כגון השתלטות על מחשב המועצה, פעילות לא סבירה (אנומליה, תהליכים שאינם מוסברים) של שרת או מערכת מידע תפעולית או ארגונית, כי קיימת או עלולה להתקיים מתקפה על מערכות המחשוב של המועצה ו/או על מאגרי המידע ו/או על נכסים דיגיטליים של המועצה.

1.2. **מבוא / נושא** :

1.2.1. פרק ב' לחוק עוסק בהגנה על הפרטיות במאגרי מידע ובהגדרות הרלוונטיות לחוק כגון "אבטחת מידע", "מאגר מידע", "מידע", "מידע רגיש", "מנהל מאגר", וסימן א' לחוק עוסק בין היתר בנושאים כגון חובת רישום מאגרי המידע בפנקס מאגרי המידע, זכות העיון במידע המוחזק במאגר המידע ובאחריות לאבטחת המידע שבמאגר המידע.

1.2.2. תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), תשמ"ו-1986 (להלן: "התקנות"), הינן תקנות אשר הותקנו מכוח החוק, וקובעות מגוון תחומים והנחיות עליהם יהיה אחראי מנהל המאגר בתחום אבטחת המידע כגון: עריכת רשימה מעודכנת של מורשי הגישה למאגר המידע לפי הרשאות הכניסה השונות, קביעת סדרי בקרה לגילוי פגיעות בשלמות המידע ותיקון ליקויים, הקמת קובץ נהלים שבו יפורטו אמצעי האבטחה, תדירות החלפת סיסמאות, ניהול יומן אירועים חריגים וכו'.

1.2.3. החוק והתקנות קבעו הלכה למעשה, את ההוראות הכלליות הדרושות לניהול מאגר מידע.

1.2.4. בהתאם להוראות החוק והתקנות החליטה הנהלת המועצה למסד בנוהל את הליך ניהול ואבטחת מאגרי המידע המצויים בבעלות המועצה.

2. מטרות הנוהל

2.1. למסד את אופן ניהול ואבטחת מאגרי המידע המצויים בבעלות המועצה.

2.2. לקבוע את כללי ניהול אבטחת המידע ומידור המידע המצוי במאגרי המידע מפני משתמשים שאינם מורשים.

3. השיטה

3.1. **הנחיות כלליות ליישום הנוהל :**

3.1.1. מורשי הגישה למאגרי המידע יקפידו על יישומן המלא של הנחיות נוהל זה המתייחסות אליהם.

3.1.2. ממונה אבטחת מידע יקבע ויפרסם את הפרמטרים לניהול מערכת הסיסמאות המחייבת את כלל המשתמשים, יפקח, יבקר ויאכוף את יישום הנוהל. קביעת כללי אבטחת המידע תבוצע בנפרד, עבור כל מערכת מידע המנהלת מערכת סיסמאות אוטומטית.

3.1.3. מנהל המאגר וממונה אבטחת מידע ידאגו ליישם הנחיות נוהל זה, כל אחד בתחומו, כמפורט להלן.

3.1.4. למען הסר ספק, ממונה אבטחת מידע יהיה כפוף להוראות והנחיות מנהל המאגר, וכל הסמכויות המוקנות לממונה אבטחת מידע על פי נוהל זה יהיו מוקנות גם למנהל המאגר ו/או מי מטעמו.

3.1.5. מנהל המאגרים יודיע לרשם מאגרי המידע, בכתב, את שמו של ממונה אבטחת מידע במאגרים.

3.1.6. נוהל זה הנו כפוף ומשלים להוראות כל דין, ואינו בא לגרוע מכל הוראה מחייבת הקבועה בדין. בכל מקרה של סתירה או אי התאמה בין הוראות נוהל זה להוראות הדין, תגברנה האחרונות.

3.2. **אחריות:**

3.2.1. למועצה רישום מאגרי מידע משנת 2005 , להלן הקישור : https://data.gov.il/dataset/pinkas/resource/fd56bf5b-7918-4906-99e4-b0e5102ae268 - (סטטוס רישום מאגרים הגנת הפרטיות)

3.2.2. מאגרי המידע בתהליך רישום במשרד המשפטים – רשם המאגרים ע"ש המועצה,

3.2.3. המועצה פועלת לקידום של רישום מאגרים נוספים בשנת 2022.

3.3. **אופן הקמת מאגר מידע חדש :**

3.3.1. אחת לשנה לפחות, וכן בכל מקרה שבו יקבע ממונה אבטחת מידע של המועצה, תבחן המועצה את תהליכי העבודה והמידע הנשמר במועצה באמצעים הדיגיטליים כדוגמת : מערכות מידע, מערכות אחסון מידע ומידע הנשמר בצורה מאורגנת.

3.3.2. כל מאגר מידע ייבחן מול דרישות חוק הגנת הפרטיות ורישום מאגרי מידע, תקנות, חוזרי משרד הפנים ורשות הסייבר ופרקטיקה דומה ברשויות מקומיות.

3.3.3. המועצה תקים צוות בדיקה המורכב מיועמ"ש המועצה או מי מטעמו, גזבר המועצה, מנהל המחלקה שברשותו המאגר וממונה אבטחת המידע אשר יבחנו את עמידת המאגר בדרישות.

3.3.4. במידה והמאגר נדרש לרישום ברשם המאגרים – תפנה המועצה באמצעות בעלי מאגר המידע לרשם משרד הפנים ותבצע רישום של המאגר.

3.3.5. המועצה תגדיר במסמך רישום המאגר, על פי העניין, את הפרמטרים הבאים: בעל המאגר, מנהלי המאגר, מורשי הצפייה במאגר, רמת האבטחה החלה עליו על פי דין (בסיסית, בינונית, גבוהה), מטרות ותכלית המאגר - שימוש במידע במאגר אפשרי רק למטרה לשמה הוקם.

3.4. **עיון במאגר המידע והעברת מידע ממאגר מידע**:

3.4.1. זכות העיון במאגר מידע תועבר לאחר בחינה משפטית למורשים בלבד, אשר ייבחנו על פי רמת הצורך בחשיפת המאגר לעיון.

3.4.2. התניה לצפייה במאגר המידע - עמידה של המורשה בדרישות תקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי הדין בערעור על סירוב לבקשת עיון), תשמ"א-1981, לרבות עיון בשלוש שפות (עברית, ערבית ואנגלית). חתימת המעיין על מסמך שמירה על סודיות והדרכה מסודרת על ידי מנהל המאגר.

3.5. **בקשה להעברת מידע ממאגר מידע בין גופים**:

3.5.1. במידה והועברה בקשה להעברת מידע ממאגר מידע מגוף חיצוני, היא תבחן על ידי ועדה המונה, לכל הפחות, את יועמ"ש המועצה או מי מטעמו, גזבר המועצה, מנהל המחלקה שברשותו המאגר וממונה אבטחת המידע.

3.5.2. הוועדה תהיה רשאית לאשר או לדחות את הבקשה וכן להתנותה בתנאים, בהתאם לשיקולי הגנת הפרטיות של הרשומים במאגר מול הזכות לעיון במאגרי מידע, כמפורט בדרישות תקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי הדין בערעור על סירוב לבקשת עיון), תשמ"א-1981.

3.6. **כללים לניהול מאגרי המידע ואבטחת המידע שבמאגרים**:

3.6.1. אבטחת המידע במאגרים תתבסס על מנגנון האבטחה המובנה במערכת ההפעלה. יש להפעיל את מירב האופציות שהמנגנון מספק.

3.6.2. לכל המשתמשים יוקצו עם הצטרפותם סיסמאות אישיות, ורק על פיהן תתאפשר הגישה למאגרים.

3.6.3. לגבי כל אחד מהמשתמשים, ללא יוצא מן הכלל, יוגדר באופן אישי ותקבענה לו ההרשאות הבלעדיות לו.

3.6.4. מנהל המאגר וממונה אבטחת מידע יהיו אחראים לקביעת ההרשאות של המשתמשים. יישום ההרשאות יבוצע על ידי מנהל המאגר בתיאום עם ממונה אבטחת המידע.

3.6.5. למען הסר כל ספק מודגש, כי ההרשאה איננה רק אפשרות גישה למאגר מידע מסוים, אלא גם הגדרה מדויקת של הפעילויות שרשאי משתמש לבצע במאגר : אחזור ו/או עדכון ו/או תוספת ו/או מחיקה.

3.6.6. משתמש הפונה למאגר המידע, יתבקש להזדהות. רק במקרה שהזיהוי עבר בהצלחה, יקבל המשתמש על המסך את פרטי מאגר המידע אליו הוא רשאי לפנות. הרשימה לא תכלול מאגרי המידע שאינם בהרשאה.

3.6.7. זיהוי משתמש יהיה באמצעות שמו (USER ID). במקרה של בעיה בזיהוי המשתמש, תיחסם התקשורת ותוצג הודעה. רק מנהל המאגר או מורשה מטעמו, יוכלו לבצע שחרור החסימה, לאחר שבדקו את המקרה לגופו.

3.6.8. מאגרי המידע לא יישמרו על התקנים ניידים כדוגמת כונן נייד או מחשב נייד.

3.6.9. המאגרים לא יועברו באמצעות דוא"ל ו/או התקן חיצוני נייד שאינו מוגן באמצעות שני אמצעי אבטחה שונים (כדוגמת : הצפנה מוגנת סיסמה חזקה הנמסרת באמצעי שונה, העברה באמצעות התקן כספות וירטואלי – CyberArk, והגנה פיזית נוספת על ההתקן באמצעי שונה).

3.6.10. לא יתאפשר מעבר ממאגר מידע אחד למשנהו, אלא דרך יציאה וכניסה מחדש באמצעות מערכת הסיסמאות.

3.6.11. באחריות מנהל המאגר לבדוק כל משתמש אחת לשנה לצורך עדכון מפת ההרשאות. הביצוע יהיה ביוזמת מנהל המאגר ובתיאום עם ממונה אבטחת המידע.

3.6.12. ממונה אבטחת מידע יוסיף או ינפה אנשים מרשימת המשתמשים רק בהתאם לפניה בכתב מטעם מנהל המאגר. הודעה על הוספה או גריעה מהמאגר תימסר למשתמש.

3.6.13. עזיבת משתמש ו/או החלטה על ביטול הרשאה, תועבר מיידית לידיעת ממונה אבטחת מידע, וזה יבטל את הרשאות הגישה של המשתמש.

3.7. **זיהוי בסיסמא** :

3.7.1. כל משתמש יוכל לגשת אך ורק אל מאגרים המותרים לו, תוך מזעור אפשרויות חשיפת סיסמאות האישיות. מעבר לזיהוי הפונה אל המערכת ע"י שמו, תתאפשר הפניה רק באמצעות סיסמא. הסיסמא תהווה את החוליה העיקרית בהגנה על הרשאות הגישה.

3.7.2. לכל המשתמשים יוקצו, עם הצטרפותם למאגר, סיסמאות אישיות ורק על פיהן תתאפשר הגישה למאגר. את הסיסמאות יקצה מנהל האבטחה. את סיסמאות הראשוניות יקצה מנהל האבטחה על פי הדרישה של מנהל המאגר הרלוונטי.

3.7.3. הסיסמא הראשונית תשמש לצורך כניסה ראשונית חד-פעמית למאגר המידע. עם כניסתו הראשונה לחשבונו במערכת, על המשתמש להחליפה לפני כל פעולה אחרת. מכאן והלאה הסיסמא תוחלף ע"י המשתמש ובאחריותו.

3.7.4. הסיסמא לא תופיע על המסך בעת הקשתה.

3.7.5. חל איסור מוחלט למסור/לחשוף סיסמאות ויש לשמור עליהן בסודיות. בפרט, אין לתלות את הסיסמאות על פתקיות בקרבת המחשב.

3.7.6. ככלל, תוחלפנה סיסמאות אחת לשלושה חודשים. המערכת תכפה את החלפת הסיסמא על המשתמש. המשתמש יקבל התראה על מסך המחשב על סיום תוקף הסיסמא לפחות 7 ימים טרם פקיעתה.

3.7.7. במקרה של הקלדת סיסמא שגויה, תחסם התקשורת ותוצג על כך הודעה במסך. המערכת תאפשר שלושה ניסיונות כניסה, לאחר מכן תחסם התקשורת לחלוטין. חידוש הגישה של המשתמש אל המערכת יתאפשר רק אחרי קיומו של בירור ובקשת חידוש באמצעות מנהל המאגר. במקרה הצורך יועבר המקרה לידיעת הממונים הרלוונטיים.

3.7.8. עם כניסת נוהל זה לתוקף, תבוצע החלפה יזומה של סיסמאות כל המשתמשים, זאת על מנת להבטיח שלכל המשתמשים קיימות סיסמאות העונות להנחיות נוהל זה.

3.7.9. כל חריגה מהוראות נוהל זה, תתאפשר אך ורק לאחר פניה מנומקת בכתב ואישור בחתימה של ממונה אבטחת מידע ושל מנהל המאגר. כל המסמכים הללו יתויקו וישמרו בתיק מיוחד שיהיה אצל ממונה אבטחת מידע.

3.7.10. המשתמש יבחר סיסמא שתענה על הדרישות הבאות:

3.7.10.1. ככלל, הסיסמא תהיה קשה לניחוש.

3.7.10.2. הסיסמא תהיה מורכבת מ10 תווים (לכל הפחות) של אותיות, ספרות וסימנים.

3.7.10.3. תו זהה לא יופיע בסיסמא יותר מפעמיים.

3.7.10.4. לא יהיו תווים עוקבים שיופיעו בסדר הרציף שלהם (א'-ב', ספרות, סדר המקשים במקלדת וכו').

3.7.10.5. אין להשתמש בסיסמא בעלת משמעות הקשורה באופן אישי למשתמש כגון: שם העובד, שם בן/בת זוג, מחלקתו, תאריכים בעלי משמעות וכדומה.

3.7.10.6. אין לעשות שימוש במקשים פונקציונליים לאחסנת סיסמאות והפעלתן.

3.7.10.7. אין לחזור על סיסמאות קודמות במשך 3ה"דורות" האחרונים.

3.7.10.8. אין להשתמש בסיסמא שהנה מילה המופיעה במילון, בכל שפה שהיא.

3.7.10.9. על מנת לאפשר תיקוני טעות בשלב קביעת הסיסמא, יש לאפשר הקלדה פעמיים.

3.7.10.10. חל איסור מוחלט על מסירת סיסמאות. משתמש יתודרך על שמירת הסיסמא, אבטחתה ועל החובה שלא להעבירה לאחר. משתמש יתודרך להודיע מיידית על חשד של חשיפת סיסמתו.

3.7.10.11. עלה החשד לחשיפת הסיסמא, יש להודיע על כך מיד לממונה אבטחת מידע ואו למנהל המאגרים. במקרה זה תיעשה פעולה מיידית להחלפתה של הסיסמא, וכן תיעשה בדיקה אודות האפשרות לשימוש בלתי מורשה בסיסמא.

3.8. **הנחיות ביחס למשתמשי המאגרים**:

3.8.1. מטרה - ניהול שוטף של ההרשאות במאגרי המידע בצורה מרכזית, תוך הפעלת שיקול דעת של מנהל המאגרים וממונה אבטחת מידע.

3.8.2. כדי לכלול משתמש ברשימת משתמשי המאגרים, על ממונה אבטחת המידע להחתים את המשתמש על טופס "הצהרה והתחייבות שמירת סודיות", בו מתחייב המשתמש שלא להעביר לאנשים בלתי מורשים מידע שיקבל, או שימצא בידיו במסגרת עבודתו.

3.8.3. מנהל המאגר ירשום את המאגרים שאליהם יהיה המשתמש מורשה לגשת, יפרט אם המשתמש מורשה לעדכן את הנתונים או רק להציגם ויאשר בחתימתו על גבי הטופס את מתן הסיסמא והרשות לכניסה למאגר.

3.8.4. כל משתמש יוגדר בטבלאות ההרשאה של המאגר. מנהל המאגר יעדכן את ההרשאות על פי טופס ההצהרה על שמירת סודיות.

3.8.5. ממונה אבטחת המידע יעדכן את טופס ההצהרה ברשימת ההרשאות וישמור אצלו את המסמך למעקב. כמו כן, יהיה ממונה אבטחת מידע מוסמך להפעיל את שיקול דעתו לגבי ההרשאה המתבקשת, ובתאום עם מנהל המאגר, תשונה ההרשאה במידת הצורך.

3.8.6. ממונה אבטחת מידע יהיה מוסמך לבטל הרשאות למשתמשים שסיימו את עבודתם/התקשרותם עם המועצה, וכן לבטל הרשאה למשתמשים (בהתאם לנתונים המתעדכנים במערכות ההרשאות) ו/או במידה ונעשה שימוש לרעה בהרשאות שניתנו להם, וזאת ללא צורך במתן התראה מראש למשתמש.

3.8.7. מידי שישה חודשים תתבצע בדיקה של ההרשאות, ע"י ממונה אבטחת מידע. תוך תאום עם הנוגעים בדבר, ישונו או יבוטלו ההרשאות, במידת הצורך. הממונה יעביר לסגן הגזבר דיווח בדוא"ל על תוצאות הבדיקה.

3.8.8. באחריות המשתמשים עצמם וכן מנהלי כלל המחלקות במועצה, להודיע לממונה אבטחת מידע במועצה על כל שינוי תפקיד, פרישה, סיום התקשרות ו/או כל שינוי אחר, המחייב עדכון הרשאות של המשתמש.

3.8.9. לא ייגש עובד למידע שאין הוא מורשה לגשת אליו. עיון או שימוש במידע שלא על פי ההרשאה מהווה עבירה, וינקטו כנגד העובד צעדים משמעתיים.

3.8.10. משתמש שהורשה לגשת למאגרי מידע, חייב לשמור את סיסמתו בסוד ולא לאפשר לאדם אחר להשתמש בה. אם יתברר כי נעשה שימוש שלא כדין במידע תחת הסיסמא של משתמש מסוים, יישא המשתמש עצמו באחריות לכך.

3.8.11. משתמש שהורשה לגשת למאגרי מידע, חייב לנקוט בצעדים הדרושים כדי למנוע מאנשים אחרים גישה למאגר בעת שמוצג בו מידע. אין להשאיר את מאגר המידע פתוח ללא השגחת המשתמש.

3.8.12. ניהול הרשאות הגישה וניהול תחום ההצפנה ייעשו על ידי מנהל המאגר וממונה אבטחת מידע בלבד.

3.9. **קביעת סדרי בקרה לגילוי פגיעות בשלמות המידע ותיקון ליקויים**:

3.9.1. בשרתים עליהם מותקנים מאגרי המידע, יישמר LOG של כל הפעילויות באמצעות תוכנה ייעודית, לתקופה של שלושה חודשים אחרונים, לכל הפחות (להלן: "**מערכת הלוגים**").

3.9.2. ממונה אבטחת המידע יוודא פעילותה התקינה של מערכת הלוגים בשרתים עליהם מותקנים מאגרי המידע.

3.9.3. ממונה אבטחת המידע יטפל באירועים חריגים המטופלים באמצעות מערכת הלוגים.

3.9.4. ממונה אבטחת המידע יגדיר אירועים ופעולות חריגות או רגישות, בתיאום עם מנהל המאגרים, ובתאום עם כל הנוגעים בדבר. ההגדרה הנ"ל תכלול ניסיונות סרק לכניסה למאגרים וכן ניסיונות לבצע פעולות בלתי מורשות אחרות.

3.9.5. לממונה אבטחת המידע תינתן גישה לבחינת דוחות המערכת בהתאם לצורך. ייבדקו ניסיונות כושלים להציב סיסמא, שמות משתמשים לא פעילים שנעשה בהם שימוש וכדומה.

3.9.6. בבדיקה תהיה גם התייחסות לשעות ולמספר הכניסות של כל משתמש.

3.9.7. הגדרת הפעילויות החריגות תיבדק ותתעדכן לפחות פעם בשנה.

3.9.8. ממונה אבטחת מידע יבדוק וינתח את הלוגים באמצעות כלים ממוכנים אחת לשבוע ויעביר הממצאים החריגים באופן מיידי למנהל המאגרים.

3.9.9. ממונה אבטחת מידע, בתיאום עם מנהל המאגרים ומנכ"לית המועצה, יערוך בירור מיידי ודחוף לגבי הממצאים החריגים שאותרו ויישם פעילויות נגזרות כנדרש.

3.9.10. ממצאים המעידים על פעילויות חריגות שבוצעו בכוונת תחילה על ידי משתמשים, יועברו בדחיפות ובדיסקרטיות למנכ"ל המועצה ויובילו לטיפול משפטי בהתאם.

3.10. **הגנה הפיסית על אחסון הנתונים במאגרים** :

3.10.1. מטרה – הנחיות להגנה פיזית על אחסון הנתונים ומערכות עיבוד הנתונים האוטומטית ועל תשתיתה לרבות מבנה, אמצעי תקשורת, מסופים ותשתית חשמל מפני סיכונים סביבתיים ופגיעות חיצוניות.

3.10.2. ממונה אבטחת מידע יוודא פעילותן התקינות של מערכת המצלמות ומערכת האזעקה המותקנות בחדרי השרתים של המועצה בהם מותקנים מאגרי המידע של המועצה. במידה והמאגרים מותקנים בענן ספקי מערכות המידע – יוודא תקינות עם ספקי מערכות המידע באמצעות שאלון ו/או תצהיר חתום מטעם הספק.

3.10.3. ממונה אבטחת המידע ינחה את עובדי ספק המחשוב בנעילת חדרי השרתים, ארונות התקשורת וכל מתקן בו תתאפשר גישה למערכות התקשורת, המחשוב או השרתים של המועצה.

3.10.4. ממונה אבטחת המידע ינחה את חב' השמירה על משרדי המועצה לבדוק את חדרי השרתים וארונות התקשורת כחלק משגרת הסיורים במשרדי המועצה הנערכת לאחר שעות הפעילות של המועצה. חב' השמירה תדווח על כל פעילות חשודה לרבות גורמים שאינם מוכרים העובדים על עמדות מחשבים של המועצה או עובדים עם מחשבים ניידים במשרדי המועצה לאחר שעות הפעילות.

3.10.5. מנהל המאגרים ינהל יומן רישום ומעקב בו תפורט מצבת התוכנה והחומרה הקיימת במועצה וממונה אבטחת המידע ינהל יומן רישום בנושא מצבת החומרה.

3.10.6. כל שינוי במצבת התוכנה והחומרה, לרבות גריעת ציוד, משלוחו לתיקון או הוספת ציוד חדש, יתועדו ביומן. כמו כן, יידרש לציין את מיקומו במשרד.

3.10.7. אין לרכוש חומרה או תוכנה ללא אישור מפרט טכני של ציוד החומרה ובדיקת רמת האבטחה על ידי ממונה אבטחת מידע.

3.11. **ניהול מאגר באמצעות מיקור חוץ** :

3.11.1. מאגרי המידע של המועצה מנוהלים באמצעות ספקי מערכות מידע המספקים פלטפורמה יישומית ומחשובית לניהול המאגר.

3.11.2. ניהול המאגרים לעיל **שגיאה! מקור ההפניה לא נמצא.** מתבצע באמצעות מערכות המידע השונות במועצה ופועלים כמחזיקי המאגר .

3.11.3. ספקי מערכות המידע מחויבים לספק למועצה את המידע ביחס לאופן ביצוע התחייבויותיו לפי תקנות הגנת הפרטיות לרבות אך לא רק: אמצעי הגנה על מערכות המידע, מבדקי חדירה ובדיקות שנתיות. כל זאת, בהתאם לדרישות תקנות הגנת הפרטיות כמחזיקים במאגרי המידע. באחריות מנמ"ר המועצה לדרוש לקבל תוצאות מבדקים אלו אחת לשנה.

3.11.4. כמו כן עליהם לקבל דיווח ועדכון שוטף ממנהלי המחלקות במועצה המפעילים את מערכות המידע על כל עובד שעזב או שברצונם לחסום לשירותים כאלו ואחרים במערכת המידע, באופן מיידי באמצעות משלוח הודעת מייל לספק מערכות המידע. על ספקי מערכות המידע למנוע גישה לכל עובד אשר התקבלה לגביו הודעה כאמור ולבצע את החסימה בתוך פרק זמן של עד יום עבודה מיום הדרישה. באחריות מנהל המחלקה לוודא ביצוע הדרישה.

4. אירוע אבטחה

בהתאם לתקנות אבטחת הפרטיות תשע"ז 2017 ,המגדיר כהפרת חוק במקרה של גילוי פרטים רגישים ממאגרי מידע השונים שבבעלות המועצה כדוגמת פרטים אישיים על לקוחות, תושבים , מספרי ת.ז. וכיו"ב, אירוע זה מוגדר כאירוע אבטחת מידע. על חובת המועצה לפעול בהתאם להנחיות כפי שצוין בנוהל הכלת אירוע אבטחת מידע של המועצה ,בהתאם לתרחישי האיום השונים .

4.1. **הנחיות התנהלות בזמן אירוע אבטחת מידע:**

התנהלות אירוע אבטחה כוללת 6 שלבים, הפעלתם היא טורית – הפעלת שלב הבא לאחר השלמת שלב קודם.

התכוננות – Preparation- המועצה תיידע את רשויות החוק או שמא תגיב בשקט ; האם יבוצע מיגור מיידי של האירוע או שמא תבוצע הכלת האירוע, לימוד מאפייניו, וניסיון ללקט ראיות.

זיהוי – Identification- עם זיהוי האירוע, גורם מיומן מטעם ספק המחשוב יבוצעו פעולות מנע מידיות : ניתוק מחשב או שרת מהאינטרנט ובידודו מרשת LAN מקומית. מנהל אבטחת מידע או מי מטעמו, יקבע את המשך הטיפול באירוע.

על יועץ המחשוב המועצה או מי מטעמו להורות על הפעלה מיידית של מערכי סריקה לזיהוי התפשטות הנוזקה ברשת ה LAN המקומית. הסריקה תתבצע בניסיון לאתר פגיעות בכונני רשת ושיתופים, תחנות עבודה וניסיונות גישה למערכות שרתי הקבצים ושרתי הדואר האלקטרוני.

אירוע זה ידווח להנהלת המועצה טלפונית ובדוא"ל לרבות הערכת נזקים ראשונית – אילו מערכים ניזוקו, הושבתו או יצאו מכלל פעולה.

הכלה – Containment- הטיפול בהכלה יכלול את הגורמים הבאים ויפעל כצוות לטיפול באירוע : על יועץ המחשוב של המועצה או מי מטעמו ועל פי צורך נציג של ספק מערכות המידע / ספק המערכות ההנדסיות.

היועץ המחשוב ו/או ספק המחשוב יפעל בכל הכלים האפשריים על מנת למנוע הפצה של הנוזקה, לרבות אך לא רק באמצעים הבאים : אבטחת סביבת האירוע (מחשב, סביבת עבודה, שרת וכיו"ב ; יצירת גיבוי ; ניתוק המערכת מרשת LAN ; שינוי סיסמאות של כל המשתמשים בעלי הרשאת מנהל מקומי ומעלה (local admin).

יועץ המחשוב ו/או ספק המחשוב ידאג שהפעולות להכלת האירוע לא יגרמו לנזקים למערכת המחשוב ולאובדן רחב מהנזק הראשוני שנגרם. על האחראי להפעיל שיקול דעת, בטרם קבלת החלטה שמשמעותה מחיקת מחשב, מערכת או שרת שאינו לצורך. במידה ונדרש.

אבטחת הסביבה : בכל אירוע נדרש לאבטח את הסביבה באמצעות גיבוי של כל המערכות המושפעות מהאירוע.

מיגור – Eradication- בטרם הפעלת המערכות מחדש, היועץ המחשוב ו/או ספק המחשוב יפעל לתקן ולפתור את הבעיה שגרמה לפרצה באבטחת המידע.

אמצעים למיגור פריצות הינם : החלפת כתובת ה-IP ושינוי שם המערכת ; סורקי חולשות, (כגון כלים Nessus, Nmap) המסוגלים לזהות חולשות - הן ברשת הפנימית והן ברשת האינטרנט ; בנוסף קיימות אפליקציות המעניקות יכולת זיהוי חולשות באופן מעמיק ביותר. בסיום ההליך יופק דוח ממצאים של אותה מערכת המצביע על ווקטור הפריצה.

התאוששות – Recovery- שחזור מערכת : נדרש לוודא כי בעת שחזור מערכת לא משוחזרים גם קבצים שהושתלו עוד לפני זיהוי האירוע. במטרה לקבוע האם השחזור תקין נדרש לבצע בדיקה .יועץ המחשוב יכין דוח בו יוצגו הרכיבים הבאים : מועדי תחילת האירוע וסיומו, הגורמים המעורבים, מערכות המחשוב המעורבות באירוע, אופן זיהוי האירוע, הפעולות שננקטו, מחוללי האירוע (הפרצה), הנזקים שנגרמו והבדיקות שבוצעו לאחר התאוששות.

באחריות מנכ"ל המועצה, לקיים ישיבת ועדת היגוי לתחקור את הסיבות שהביאו לאירוע והפקת לקחים בעקבות האירוע לעתיד.

5. בקרות לתהליך

בדיקות מדגמיות ליישום הנדרש על פי התהליך אחת ל-6 חודשים על ידי ממונה אבטחת המידע של המועצה.

6. נספחים

טופס הצהרה והתחייבות שמירת סודיות.

7. . אחריות ,סמכות ותוקף

7.1. נוהל זה אינו מחליף את דרכי ההתערבות והטיפול הקיימים במקרים המובאים לעיל, אלא בא להוסיף עליהם.

7.2. האחריות והסמכות לביצוע נוהל זה הנה מנמ״ר המועצה ומי מטעמו בהתאם לאמור לעיל.

7.3. נוהל זה ייכנס לתוקפו ויפורסם לאחר אישורו ע״י המועצה .

נספח

טופס הצהרה והתחייבות שמירת סודיות

אני הח"מ מר / גב' _____, נושא/ת ת.ז. מספר _____, מרח' _____ יישוב _____ מתחייב/ת ומצהיר/ה בזאת מועצה אזורית הגלבוע (להלן: "**המועצה**") כדלקמן:

1. המועצה תציג ו/או תלמד ו/או תחשוף בפניי מידע, מסמכים, שיטות עבודה וטכנולוגיות הקשורים לתחום העיסוק, מסמכי המועצה, לקוחות, למערכות מידע ו/או כל מידע אחר הקשור בלקוחות ו/או שותפים עסקיים במועצה (להלן: "**מידע חסוי**").
2. הצגת המידע החסוי נועדה אך ורק לצרכי עבודה והריני מתחייבת כי לא אעשה במידע החסוי שיועבר לי כל שימוש, אלא לצורך עבודתי במועצה באמון מלא.
3. כמו כן הריני מתחייב, לשמור בסודיות, לא לגלות, לא להעביר ולא למסור בכל דרך שהיא ובשום זמן שהוא, לרבות בטרם קשריי עם המועצה, במשך תקופת קשריי עם המועצה והן לאחר מכן ולתקופה של 5 שנים, ולרבות במידה ולא אתקשר כלל בקשרים כלשהם עם המועצה, כל מידע הקשור למידע חסוי וכן כל מידע הקשור במועצה, לשירותיה, לספקיה, לשותפיה העסקיים, ללקוחותיה, לתכוניותיה, לסודותיה המקצועיים, העסקיים והמסחריים או לעסקיה, אשר הגיע או יגיע לידיעתי ו/או לידיעת שלוחיי בכל דרך שהיא ובלבד שמידע זה אינו נחלת הכלל, אלא שאם הפך המידע לנחלת הכלל עקב הפרת התחייבות כלשהי שלי ו/או מי מטעמי ו/או שלוחיי ו/או מי מעובדיי, יישאר אף אז המידע בבחינת מידע חסוי ולמעט מידע שהיה ברשותי בטרם חתימת כתב זה. המידע האמור יכול שיהיה, מבלי לגרוע מכלליות האמור לעיל, מידע בעל פה או מידע בכתב, לרבות בצורת דו"חות, רשימות, מסמכים, מפות, תיאור הליכי שיווק, הפצה, פיתוח ו/או אחרים ו/או בכל צורה אחרת.
4. לא להעתיק ו/או להרשות לצד שלישי כלשהו ו/או לגרום לצד שלישי כלשהו לבצע במידע החסוי שכפול, העתקה, צילום, תדפיס וכל צורת העתקה אחרת ולהחזיר כל מסמך ו/או חומר אחר שיועבר אלי למציג.
5. לשמור בהקפדה את המידע החסוי ולנקוט בכל אמצעי הזהירות הנדרשים לשם מניעת אובדנו ו/או הגעתו לידי צד שלישי כלשהו.
6. לא לפרסם ולא לעשות כל שימוש בכל צורה שהיא בין בעצמי ובין באמצעות אחרים במידע החסוי שיועבר אלי ו/או שיוצג בפני /ואו שייודע לי במהלך עבודתי.
7. ידוע לי שאצטרך לפצות עם המועצה בגין כל הנזקים שיגרמו לו בגין הפרת התחייבויותיי לפי כתב התחייבות זה.
8. תוקפו של כתב התחייבות זה הינו לכל תקופת היות המידע חסוי וסודי ובטרם הפך לנחלת הכלל.
9. התחייבויותיי לפי כתב התחייבות זה הינן בלתי חוזרות.
10. בחתימתי שלהלן הנני מאשר כי קראתי והבנתי את כל האמור בכתב התחייבות זה.

	אגף מנכ״ל	נוהל מס׳ :	32
	שם הנוהל : נוהל מאגרי מידע	ת. תחולה :	16/10/18
		מס׳ מהדורה :	1.0
		עמוד : 15 מתוך 15	

תאריך : _____ חתימה : _____