שם הנוהל: נוהל אבטחת מידע		**מס' הנוהל: 8.01**	**עדכון מס':** 0
תאריך נוהל קודם:	**תאריך עדכון: 25/8/20**	**דף מס':** 1	**מתוך:** 7

1. מטרת הנוהל

להתוות ולהגדיר מדיניות אבטחת מידע במועצה מקומית שוהם.

2. הגדרות

2.1 "מידע" - כל נתון הנוגע ו/או הקשור לפעילותו, תפעולו או תפקודה של המועצה, לרבות מידע הנוגע לצנעת הפרט ומידע ציבורי רגיש, הקיים על-גבי אמצעי אחסון ממוחשבים, מגנטיים או אלקטרוניים, על-גבי מצעי מידע פיזיים.

2.2 "אבטחת מידע" - מכלול הפעולות והאמצעים הננקטים והמיושמים במועצה, שמטרתם להביא לכך שהמידע ופריטי הציוד היוצרים אותו והמטפלים בו, יוגנו מפני פגיעה, חשיפה, מחיקה או שינוי, במזיד או בשוגג, הן מתוך המועצה והן מחוצה לה.

2.3 "ועדת ההיגוי לנושא מחשוב" - פורום ניהולי שמונה ע"י מנכ"ל המועצה ובראשו יושבים מנכ"ל המועצה או מי מטעמו ונועד לאשרר ולתקף את מדיניות המועצה בתחום אבטחת המידע, להתוות אסטרטגיות לפעילות, לפקח אחר תכניות העבודה השנתיות, לקיים הערכת נזקים בעקבות תקלות ולגבש המלצות לטיפול.

2.4 "מנהל אבטחת המידע" - מי שמונה בכתב ע"י מנכ"ל המועצה לשמש כממונה על אבטחת המידע של המועצה ומאגריה בהתאם לסעיף 12ב' לחוק הגנת הפרטיות (מסמך ישים 1).

2.5 "עובד" - עובד מועצה, לרבות עובד השמה ועובד מיקור חוץ.

2.6 "מנהל מאגר" - גורם אשר הוסמך מטעם מנכ"ל המועצה בו הינו מועסק, לנהל מאגר מידע מסוים ואשר נרשם במשרד המשפטים כמנהלו של המאגר.

2.7 "מועצה" – מועצה מקומית שוהם.

3. תוכן הנוהל

כללי

3.1 המועצה בהיותה גוף ציבורי, מחזיקה במערכות מידע ממוחשבות התומכות בפעילותה הציבורית והארגונית, כאשר במערכות אלו אגור מידע אישי, ארגוני וכלכלי רב.

3.2 מרבית המידע האישי הקיים והמעובד במערכות המידע של המועצה, הינו רגיש ומסווג כהגדרתו בחוק הגנת הפרטיות.

3.3 המערכות המנהלות אותו, האמצעים והציוד עליו הוא מושתת, מהווים נכס מרכזי וחיוני של המועצה ויש להגן עליהם כעל משאבים אחרים בעלי ערך במועצה.

3.4. פגיעה במידע תוביל לנזקים העלולים לתת אותותיהם בהיבטים תפעוליים ,טכנולוגיים וכספיים וכן להוביל לפגיעה בביטחון הפיסי, בשירותים ובצנעת הפרט של תושבים, עובדים וגורמים נוספים, שפרטיהם אגורים במערכות המועצה, וזאת מעבר לפגיעה במוניטין ובתדמית המועצה ונקיטת אמצעים משפטיים.

3.5. **התחייבויות עובד**

3.5.1. כל עובד חדש הנקלט לעבודה במועצה יחתום על "כתב התחייבות עובד לשמירה סודיות" (ראה נספח 1).

3.5.2. חל איסור לשתף גורם שאינו מורשה במידע סודי הקשור לעבודה במועצת שוהם, בדגש על פרטים אישיים ועסקיים של ספקים ותושבים.

3.5.3. העובד מתחייב שלא למסור כל מידע, רגיל וממוחשב, שהגיע אליו בתוקף תפקידו, לכל גורם, אלא אם כן הורשה לכך או שהדבר נעשה במסגרת תפקידו.

3.5.4. על העובד לשמור על סודיות המידע והנתונים אליהם הוא נחשף במהלך עבודתו.

3.5.5. הוראה זו חלה על העובד גם לאחר שסיים את עבודתו במועצה.

3.6. **ניהול הרשאות וסיסמאות:**

3.6.1. שם המשתמש והסיסמא הם אישיים, ונועדו אך ורק לשימושו האישי של העובד ולצורך ביצוע עבודתו.

3.6.2. חל איסור למסור את שם המשתמש והסיסמא האישיים לאדם אחר או להשתמש בשם משתמש וסיסמא של עובד אחר במהלך העבודה.

3.6.3. יש להימנע משמירת הסיסמא במקום בו היא עלולה להיחשף (תיקיות ציבוריות, הדבקת פתק באזור העבודה וכו'). בכל מקרה של חשיפת הסיסמא או חשד לחשיפתה, יש להחליף את הסיסמא מידית ולדווח למנהל אבטחת המידע על המקרה.

3.6.4. בכל מקרה של עזיבת עובד או איתור פעילות חריגה/ לא מורשית/ לא חוקית ע"י עובד מוסרות ההרשאות באופן מיידי.

3.7. **אבטחת סביבת העבודה**:

3.7.1. כל עובד/ת אחראי/ת לאבטחת סביבת העבודה האישית שלו. אבטחת סביבת העבודה תתבסס על מדיניות שולחן נקי. מסמכים רגישים לא יותרו חשופים על השולחן כאשר העובד עוזב את סביבת העבודה בסוף או במהלך יום העבודה.

3.7.2. בעת עזיבת סביבת העבודה, ינעל העובד את המסמכים הרגישים בארון נעול.

3.7.3 ניירת רגישה תושם בפח ייעודי אשר תכולתו מיועדת לגריסה. יש לגרוס כל ניירת משרדית, שאין בה עוד צורך ובפרט ניירת המכילה מידע "סודי" , במידה ולא קיים פח מעין זה בסביבת העבודה של המשתמשים באחריות המשתמש לגרוס את הנייר.

3.7.4 מדיניות מסך נקי - אין להותיר את המחשב פתוח (במצב של חיבור לרשת), כאשר עוזבים את סביבת העבודה.

3.7.4.1 על העובד לצאת באופן מסודר מהרשת (off log) ולכבות את המחשב .

3.7.4.2 בכל מקרה של "נטישת" עמדת המחשב, יפעיל המשתמש את שומר המסך באופן ייזום באמצעות לחיצה על המקשים Delete+Ctrl+Alt.

3.7.4.3 מידע תפעולי של המועצה ישמר בכונן הרשת בלבד ולא על עמדות מחשב.

3.7.5 הגישה למידע תתאפשר בהתאם לרמת ההרשאות שניתנה לעובד ובהתאם לעקרון "הצורך לדעת".

3.8 **התקנת והסרת תוכנות ומחשבים** :

3.8.1 מועצת שוהם מייחסת חשיבות רבה להתקנת תוכנות חוקיות בלבד על כל המחשבים במועצה, ולכן חל איסור שימוש בתוכנות בלתי חוקיות.

3.8.2 חל איסור מוחלט להתקין במחשבי המועצה תוכנות ללא אישור בכתב ממחלקת מחשוב.

3.8.3 מחשבים ניידים : המחשב הינו אישי ולשימושו של העובד בלבד.

3.8.4 חל איסור לבצע תחזוקה של המחשב הנייד ע"י גורם מחוץ למועצה.

3.8.5 כאשר העובד מנייד את המחשב (הנייד או הנייח) מחוץ למועצה, המחשב יהיה תמיד תחת השגחתו.

3.8.6 אם הלפטופ אבד או נגנב, יש לדווח מיידית למחלקת מחשוב.

3.8.7 יש להימנע משימוש לצרכים פרטיים בציוד המחשוב של המועצה.

3.8.8 חל איסור להפסיק את פעולת המערכות לאבטחת מידע, כגון אנטי וירוס.

3.8.9 חל איסור לשנות את הגדרות המערכת של המחשב.

3.8.10 חל איסור על התקנה, הורדה או אחסון של מידע המוגן בזכויות יוצרים.

3.8.11 טרם סילוק רשומות או ציוד מחשובי יש לוודא שלא מאוחסן בתוכו מידע רגיש וזאת באמצעות פירמוט דיסק קשיח טרם סילוקו וכד'.

3.9. ניהול מצעים ניידים:

3.9.1. חל איסור מוחלט לחבר במחשבי המועצה או לרשת הארגונית רכיבי ציוד תוכנה וחומרה באביזרים נלווים כגון דיסקים ניידים, key on Disk טלפונים ניידים וכדומה ללא אישור של מנכ"ל המועצה או מנהל המחשוב.

3.9.2. חל איסור להוציא מידע על כל מצע, ממשקי, USB דיסקים ניידים key on , Disk ונתיקים, וכו' ללא אישור מראש ובכתב של מנהלי היחידות.

3.9.3. כאשר שומרים מידע חסוי על גבי מדיה נתיקה, יש לאחסן אותו על גבי on Disk key מוצפן אשר יסופק ע"י המועצה בלבד ולא במדיה אחרת, ניירת או מצע מידע אחר דיסקים/ דיסקים ניידים/ נתיקים (Key On Disk ,) יאוחסנו במקום מאובטח כגון מגירות או ארונות נעולים.

3.9.4. חל איסור להוציא מידע מהמועצה, למעט במקרים שאושרו ע"י המנהל הישיר ולפי צרכי העבודה. מידע המכיל ריכוז פרטים לגבי אנשים ומסווג כמידע רגיש עפ"י הוראות חוק הגנת הפרטיות וכן כל מידע אחר של המועצה, יימצא תחת משמורת המחזיק בו בכל זמן.

3.10. שימוש באינטרנט :

3.10.1. חל איסור לשתף מידע של המועצה באמצעות היישומים השונים באינטרנט.

3.10.2. יש להימנע ממסירת פרטים אישיים של העובד, וחל איסור למסור את כתובת הדואר האלקטרוני של המועצה בעת רישום לאתרי אינטרנט, למעט רישום לאתרים הקשורים לעבודתו של העובד.

3.10.3. חל איסור לגלוש באתרים זדוניים לרבות אתרי הימורים, אתרים מיניים ו/או בעלי תוכן פוגעני. אין להפיץ תכנים נושאי אופי מיני או מידע אחר העלול להוות עלבון ליחיד או לקבוצה או כל חומר המפר את הנחיות המועצה בנושא הטרדה מינית.

3.11. שימוש בדואר אלקטרוני :

3.11.1. תיבת הדואר האלקטרונית במועצה הינה תיבה מעורבת, ויחד עם זאת יש להמעיט השימוש בה לצרכים אישיים.

3.11.2. חל איסור לשלוח מכתבי שרשרת, מיילים והודעות בעלי תוכן פוגעני או כאלה ,אשר עלולים לפגוע במהלך התקין של העבודה או בתדמיתה של המועצה.

3.11.3. אין לפתוח הודעות דואר אלקטרוני או קבצים מצורפים אשר מקורם אינו מוכר או אינו סביר.

3.11.4. עובד שקיבל מייל חשוד בתיבת המייל שסופקה לו לצורך עבודתו, ידווח במיידית למחשוב .

3.12. **רשתות חברתיות**:

3.12.1. בזמן שימוש ברשתות חברתיות, חלים כל הכללים בנוהלי המועצה, בקשר להוצאת מידע ושמירת סודיות.

3.12.2. אין לפרסם תכנים של המועצה המוגדרים בחיסיון מטעמי אבטחת מידע או הגנת הפרטיות.

3.12.3. אם עובד במועצה בחר לציין את עובדת היותו עובד במועצה, מחובתו להבהיר שדבריו נאמרים על דעת עצמו ולא מטעם המועצה.

3.13. **דיווח על אירועי אבטחת מידע:**

3.13.1. חלה חובה על המשתמש לדווח על אירועים/בעיות אבטחת מידע בהם הוא נתקל במהלך עבודתו ובהם: חשד לפרצות אבטחת מידע במערכות השונות ובמחשב האישי. חשד כלשהו כי המידע האגור במערכות נפגע / נמחק, שונה או נחשף.

3.13.2. חשד לקבלת מייל הונאה (Phishing) - חשד של המשתמש כי נעשה שימוש לא מורשה בזיהוי המשתמש שלו.

3.13.3. הדיווח יעשה במייל למרכז התמיכה עם העתק למנהל המחשוב יש לצרף את מירב הפרטים ככל שניתן.

3.14. **אבטחה פיזית חדר שרתים**

3.14.1. חדר השרתים נעול לאורך כל שעות היממה.

3.14.2. לא תתבצע כניסה לחדר השרתים ללא ליווי של מורשה גישה.

3.14.3. חדר השרתים יהיה ממוזג בכל עת.

3.15. **גיבוי נתונים:**

3.15.1. למועצה מערכת גיבוי מקיפה ועדכנית. נתונים הנשמרים בקבצי מערכות המידע או במחשבים האישיים יגובו, ויאובטחו כך, שהשימוש בהם יהיה מבוקר וע"י המורשים לכך בלבד.

3.15.2. באחריות כל עובד לשמור את המסמכים עליהם הוא עובד ברשת המקומית ולא במחשב האישי, על מנת להבטיח גיבוי מלא של המידע.

3.15.3. נציגי מחלקת מחשוב יבדקו באופן תדיר את תקינות הגיבויים וביצוע שחזורים יזומים אקראיים על מנת לבחון האם המידע נשמר כראוי.

שם הנוהל: נוהל אבטחת מידע		**מס' הנוהל: 8.01**	**עדכון מס':** 0
תאריך נוהל קודם:	**תאריך עדכון: 25/8/20**	**דף מס':** 6	**מתוך:** 7

4. **אחריות ביצוע:**

4.1. מנכ"לית המועצה

4.2. מנהל אבטחת מידע

4.3. מחלקת מחשוב ומערכות מידע

4.4. כלל עובדי המועצה

5. **מסמכים ישימים:**

5.1. חוק הגנת הפרטיות, התשמ"א – 1981.

5.2. תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017

6. **נספחים:**

6.1. נספח 1 - כתב התחייבות עובד לשמירת סודיות

7. **תפוצה:**

7.1. מנכ"לית המועצה

7.2. מנהל אבטחת מידע

7.3. מחלקת מחשוב ומערכות מידע

7.4. כלל עובדי המועצה

7.5. קובץ נהלי המועצה

כותב הנוהל: גב' דליה בסן מר אורן חכם	**תפקיד:** מנהלת משאבי אנוש מנהל מחשוב
מאשר הנוהל: גב' דינה פרומוביץ	**תפקיד:** מנכ"ל
תאריך:	**חתימה:**

שם הנוהל: נוהל אבטחת מידע		**מס' הנוהל: 8.01**	**עדכון מס':** 0
תאריך נוהל קודם:	**תאריך עדכון: 25/8/20**	**דף מס':** 7	**מתוך:** 7

נספח 1
התחייבות לסודיות – עובד/ת

1. הנני מתחייב/ת לשמור בסודיות מלאה על כל המידע שיימסר לי על-ידי מועצה מקומית שוהם ועבור מועצה מקומית שוהם (להלן: "המועצה") ולא להעבירו ו/או לא למסור את תוכנו לכל אדם ו/או תאגיד, ולהשתמש בו לפי הנחיות המועצה בלבד, וכן להשמידו עם גמר העבודה, במידה שנדרש לכך ע"י המועצה.

2. הנני מתחייב/ת שלא לעשות שימוש כלשהו שלא לצרכי עבודתי במועצה, בין במישרין ובין באמצעות צד שלישי, בכל מאגר מידע ו/או חלק ממנו ו/או כל מידע אחר שהועבר או יועבר בעתיד על-ידי המועצה ועבור המועצה.

3. הנני מתחייב/ת בזה שלא לגלות כל ידיעה שתגיע אלי בתוקף תפקידי במועצה בעבודתי עם מערכות עיבוד נתונים הממוחשבות, אלא לצורך עבודתי.

4. הנני מתחייב/ת שלא לפגוע בפרטיות זולתי ע"י שימוש בידיעה על ענייניו הפרטיים של אדם או מסירתם לאחר שלא למטרה שלשמה נמסרה, ושלא להעתיק או להשתמש בתוכנו של מסמך שלא נועד לפרסום ושלא להפר חובת סודיות שנקבעה בדין לגבי ענייניו הפרטיים של אדם. לקיים ולשמור על כל הוראה ו/או חוק בנושא שמירת ו/או אבטחת מידע ובכלל זה חוק הגנת הפרטיות, התשמ"א- 1981 ותקנותיו.

5. הסיסמאות הינן אישיות וסודיות ללא משמעות לוגית כלשהי, ואינן ניתנות להעברה.

6. הנני מתחייב/ת בעת סיום העסקתי לאפשר למועצה להיכנס לתיבת הדואר האלקטרונית האישית שלי מטעם המועצה, לצורך שליפת מידע רלוונטי לצרכי העבודה שקיים במייל/ שיתקבל בעתיד.

בכבוד רב,

שם פרטי +משפחה	תפקיד	חתימה	תאריך