מועצה אזורית הגלבוע

נהלי מחשוב ואבטחת מידע
נוהל אבטחת מידע לקליטת עובד חדש, שינוי תפקיד וסיום העסקה

1. <u>כללי</u>:

א. המועצה האזורית הגלבוע (להלן: "**המועצה**") עושה שימוש במערך מחשוב לטובת העבודה השוטפת, בו נאגרת מסה אדירה של מידע רגיש הכולל פרטים אישיים של תושבי המועצה ונתונים עסקיים- ציבוריים ונתונים תפעוליים.

ב. מערך המחשוב מבוסס על תשתית האינטרנט ועל כן חשוף לאירועי אבטחת מידע אשר יכולים להיגרם כתוצאה מהתממשות איומים מסוגים שונים, ועלולים להוביל לפגיעה בתפקוד המועצה על ידי השבתת המערכות התפעוליות והארגוניות ו/או חשיפת המידע האגור בהן.

ג. אי לכך, עולה הצורך הבלתי מתפשר למזער ככל הניתן את הסיכוי הממשי להתרחשותם של אירועי אבטחת מידע ובכך גם את הסיכוי להתממשותה של פגיעה בפעילות המועצה ותושביה.

ד. נוהל זה יפרט את הנחיות אבטחת המידע הנדרשות למימוש במסגרת התהליכים הארגוניים הנוגעים לתהום משאבי האנוש לרבות קליטת עובד חדש, שינוי תפקיד וסיום העסקה.

2. <u>מטרות וייעוד הנוהל</u>:

א. לפרט את תהליכי העבודה הנדרשים לביצוע על ידי בעלי התפקידים המפורטים בנוהל זה, בעת קליטת עובד חדש, שינוי תפקיד וסיום העסקה כנלווה לנהלי משאבי אנוש של המועצה.

ב. הנוהל מיועד לעובדי המועצה, לקבלן המחשוב של המועצה (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.

3. <u>הגדרות</u>:

3.1. <u>"אירוע סייבר"</u>:

מקרה בו עובד או מערכת ניטור הקיימת ברשות המועצה או 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.

3.2. <u>"מערך המחשוב"</u>:

כלל התשתיות והמערכות הממוחשבות המשמשות את בעלי התפקידים במועצה לטובת פעילותם לרבות ציוד ממוכן, תשתיות טכנולוגיות, שרתים, מחשבים נייחים וניידים, ציוד תקשורת וכו'.

3.3. "אירוע אבטחת מידע": כל מקרה אשר עלול להוביל לפגיעה בסודיות, אמינות או זמינות של מערכות המועצה והמידע האגור והמעובד בהן.

3.4. אירוע מסוג "איום פנימי": אירוע אבטחת מידע שמקורו בגורם פנים ארגוני המבצע פעולות שמהוות איום על מערכות המחשוב, כגון: חריגה מנהלים, מעילה, שימוש בחומר רגיש שלא על פי ההנחיות, עקיפת הרשאות, העברת מידע אל גורמים בלתי מורשים, פגיעה בפעילות התפעולית וכדומה.

3.5. אירוע מסוג "איום חיצוני": אירוע אבטחת מידע שמקורו בגורם חיצוני לארגון המבצע פעולות שמטרתן להשיג נגישות אל מערך המחשוב של המועצה במטרה להשיג מידע רגיש (אישי-פרטי או עסקי-ציבורי) ו/או לבצע השחתה או שינויים במערכות ניהול המידע הארגוניות ו/או לפגוע בפעילות התפעולית של מערכות המועצה.

3.6. מנהל מערכות מידע ראשי (מנמ"ר): בעל התפקיד האחראי במועצה על מימוש תהליכי העבודה המבוצעים באמצעות מערך המחשוב, באופן שימזער את הסיכוי להתממשות אירועי אבטחת מידע.

4. תיאור התהליך:

4.1. אחראי אבטחת המידע או מי מטעמו יתדרך את העובד בהתאם לדגשים הרלוונטיים לכל אחד מן התהליכים הארגוניים השונים.

4.2. קליטת עובד חדש - העובד הנקלט יתודרך בנוגע לנהלי אבטחת המידע המוגדרים ב

4.3. מועצה, תוך הצגת הנהלים הארגוניים וכן הדגשת נהלי מפתח.

4.4. מטרת התדרוך הינה להבהיר את אחריותו של העובד לעניין מימוש הנחיות אבטחת המידע ולמזער את הסיכוי להתממשות אירוע אבטחת מידע שמקורו ב"איום חיצוני" או "איום פנימי".

4.5. כל עובד חדש יעבור תדרוך לשימוש נאות במערכות המידע הרלוונטיות לתפקידו. התדרוך יגדיר את תחומי האחריות וכללי השימוש במערכות המידע הארגוניות והתפעוליות שבשימוש המועצה.

4.6. שינוי תפקיד - העובד יתודרך בנוגע למתאר ההרשאות הרלוונטי לתפקידו החדש במטרה להבהיר את אחריותו של העובד לעניין חשיבות השמירה על נהלי המידור המוגדרים במועצה.

4.7. סיום העסקה - עובד המסיים את תפקידו במועצה יתודרך בנוגע לאיסור העברת המידע אליו נחשף במסגרת מילוי תפקידו אל גורמים בלתי מורשים וכן איסור השימוש במידע זה לטובת כל פעילות אחרת שיבצע בעתיד, מחוץ למועצה.

4.8. בסיום התדריך יידרש עובד חדש / עובד המשנה את תפקידו לחתום על מסמך רשמי שיונפק מטעם המועצה, המתעד את ביצוע התדריך ואת הסכמתו לעניין הבנת משמעותן של ההנחיות שהוצגו בפניו וכן את התחייבותו לעמוד בנהלי העבודה והגישה למערך המחשוב של המועצה.

4.9. במקרה של סיום העסקה, מנהל מערכות המידע הראשי ינטרל לחלוטין את הרשאותיו של העובד היוצא על ידי מחיקת כל המשתמשים האישיים באמצעותם ניגש אל הפלטפורמות השונות הקיימות במערך המחשוב של המועצה. (יש לוודא כי המחיקה מבוצעת באופן פרטני בכל אחד מממשקי הניהול של הפלטפורמות השונות - AD, מערכת ERP וכדומה).

4.10. ה

תנהלות עם מידע ארגוני ותפעולי

4.10.1. עובד המועצה מיועד להיחשף במסגרת תפקידו למידע אישי רגיש ולמידע פנים ארגוני שאינו ראוי להיחשף לעיני כל. במסגרת חתימתו על הצהרת סודיות, מתחייב העובד שלא למסור מידע לגורמים בלתי מורשים.

4.10.2. מידור - עובדי המועצה ייגשו רק למידע חיוני לצורך עבודתם השוטפת ויימנעו ככל הניתן מחשיפה למידע שאינו רלוונטי למילוי תפקידם, גם אם מערכת ההרשאות הטכנולוגית מאפשרת בפועל גישה אליו.

4.10.3. הגישה למערך המחשוב, למערכות ניהול המידע ולמערכות התפעוליות של המועצה תתאפשר באמצעות הזנת שם משתמש וסיסמא אישיים. חל איסור להעביר את פרטי המשתמש של עובד אחד לאחר. כמו כן, אין לאפשר גישה של עובד אל המערכות באמצעות משתמש שאינו ייעודי לו.

4.10.4. אבטחת מידע פיסית - מסמכים המתעדים מידע רגיש יאוחסנו באופן שימנע את הגישה אליהם ע"י גורמים בלתי מורשים, באמצעות כספת ו/או מנעול.

4.11. ש

ימוש בתיבת דוא"ל

4.11.1. אין לפתוח הודעות דוא"ל מכתובות שולח לא מוכרות. יש לוודא בעת פתיחת ההודעה כי זו נשלחה מכתובת שולח לגיטימית ומוכרת למשתמש הקצה.

4.11.2. אין לפתוח קבצים ו/או ללחוץ על קישורים שנשלחו מכתובות לא מוכרות.

4.11.3. אין למסור פרטי משתמש אישיים ו/או פרטי הגישה לתיבת הדוא"ל לגורמים שאינם מוכרים בוודאות. תוקפים רבים מתחזים לגורמים לגיטימיים אשר דורשים את פרטי המשתמש. לרבות הסיסמה לתיבת הדוא"ל.

4.11.4. באחריות המשתמש לדווח לאחראי אבטחת המידע על כל מקרה בו התקבלה בחשבונו הודעת דוא"ל בלתי מזוהה המעלה חשד.

4.12. שימוש בעמדת הקצה

4.12.1. אין לחבר התקנים חיצוניים לעמדת הקצה. בכלל זה - התקני מדיה נתיקה (dok), מכשירים סלולריים ומחשבי לוח (טאבלטים).

4.12.2. גם בהיעדר אכיפה טכנולוגית במערכות הארגון, משתמש ישאף להגדרת סיסמא חזקה בעבור כל משתמש אישי שברשותו; סיסמה המכילה לפחות 12 תווים ומורכבת מסימנים, אותיות גדולות, אותיות קטנות ומספרים.

4.12.3. הסיסמא היא אישית וחל איסור לשתפה עם עובדים אחרים. כמו כן, הסיסמא ושם המשתמש לא יישמרו באופן גלוי (לדוג' - פתק על שולחן העובד).

4.12.4. אין לבצע הורדה של קבצים מרשת האינטרנט שאינם משמשים לצרכים ארגוניים מוגדרים. כאשר עולה צורך לבצע הורדה של קבצים, המשתמש נדרש לוודא כי מקור הקבצים הינו מקור מזוהה ומהימן. במקרים של ספק - אין לבצע הורדה לעמדת הקצה.

4.12.5. אין לבצע שימוש ברשתות חברתיות כלל ו/או בשירותי דוא"ל שאינם במסגרת שרת הדוא"ל האירגוני.

4.12.6. על המשתמש מוטלת האחריות לדווח לאחראי אבטחת המידע אודות כל פעילות חריגה או חשודה המתרחשת כעמדת הקצה.

<u>קבלת הודעה ודיווח</u>:

כל עובד/ת המועצה, אשר על פי המידע והכלים המקצועיים העומדים לרשותו, מעריך כי לפניו אירוע סייבר יפעל כדלקמן:

4.13. ידווח מיידית למנמ"ר המועצה למר רונן בגים והוא יעדכן במידת הצורך את מוקד השירות של ספק המחשוב למספר 0525656080: או לכתובת המייל: ciso911@ladpc.co.il

א. במקרה של וירוס כופר אין לנהל מו"מ עם החוטף או ליצור קשר טלפוני עמו ו/או לענות לו על דוא"ל ובו דרישת כופר. כלל התכתובת של האקר תועבר מיידית לדוא"ל של ספק המחשוב לכתובת: ciso911@ladpc.co.il

לו"ז: מיידי.

<u>אחריות: מקבל המידע</u>.

4.14. במידה והאירוע תוייג כאירוע סייבר – מנהל ספק המחשוב יודיע מיידית הן טלפונית והן בדוא"ל למנמ"ר המועצה וזאת תודיע במידת הצורך ליועץ אבטחת המידע של המועצה.

לו"ז : מיידי.

אחריות : ספק המחשוב / מנמ"ר המועצה

4.15. יועץ אבטחת המידע של המועצה ינתח את האירוע ועל פי חומרתו ינחה את ספק המחשוב ליישום הפעולות הבאות עד לרמת השבתת פעילות : ניתוק עמדת עבודה מהרשת, בידוד מערכת מידע נגועה, טיפול במערכת הנחשדת כמפיץ הווירוס או ממנה קיימת חדירה, עד לרמת השבתת מערכת המחשוב של המועצה או מערכות המידע של המועצה.

לו"ז : מיידי.

אחריות : יועץ אבטחת המידע.

4.16. במקרה של "אירוע סייבר" מהותי המשפיע על מערכות המחשוב של המועצה ברמת השבתת מערכת מחשוב או מערכת מידע, יועבר דיווח למנכ"לית המועצה.

לו"ז : מיידי.

אחריות : יועץ אבטחת המידע.

4.17. יועץ אבטחת המידע ו/או מנכ"לית המועצה יעביר דיווח מסודר למשרד הפנים אגף הסייבר, למטה הסייבר הלאומי ויקבל הנחיות מהם לפעולות נדרשות במקביל לפעולות המבוצעות על ידי ספק המחשוב.

לו"ז : 24 שעות מקבלת ההודעה.

אחריות : יועץ אבטחת המידע ו/או מנכ"לית המועצה.

5. אחריות, סמכות ותוקף:

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

5.2. האחריות והסמכות לביצוע נוהל זה הינה על מנמ"ר המועצה ובהתאם לאמור לעיל.

5.3. נוהל זה ייכנס לתוקפו החל מיום פרסומו.

נהלי מחשוב ואבטחת מידע
נוהל אבטחת מידע לקליטת עובד חדש, שינוי תפקיד וסיום העסקה

ספח התחייבות עובד לשמירת ולעמידה בדרישות אבטחת מידע של המועצה

1. הנני מצהיר על כך שהובאו לידיעתי המשמעויות הנוגעות לשימוש שלא לצורך במידע פנים-אירגוני.
2. לתשומת ליבך, הפרת הנוהל עלולה להיחשב כעבירת משמעת על פי חוק הרשויות לעבירות משמעת.
3. כמו כן הובאו לידיעתי הסיכונים הנוגעים לשימוש בעמדת הקצה הארגונית (המחוברת לרשת האינטרנט), באופן שחורג מנהלי אבטחת המידע המוגדרים.
4. הנני מצהיר בזאת בי הובאו לידיעתי נהלי אבטחת המידע האירגוניים הבאים(סמן 1-0) :

- התנהלות עם מידע רגיש
  - במסגרת תפקידי איחשף למידע אישי רגיש של תושבים ולמידע פנים אירגוני שאינו ראוי להיחשף לעיני כל. בחתימתי על הצהרת הסודיות והצהרה זו, הנני מתחייב שלא למסור מידע לגורמים בלתי מורשים.
  - במסגרת תפקידי במועצה איחשף אך ורק למידע הרלוונטי למילוי התפקיד ואמנע ככל הניתן מחשיפה למידע שאינו רלוונטי למילוי התפקיד, גם אם מערכת ההרשאות הטכנולוגית תאפשר בפועל גישה אליו.
  - גישתי אל מערכות המידע בארגון תבוצע ע״י הזנת שם משתמש וסיסמא הידועים לי בלבד ומיועדים אך ורק לשימוש שלי. לא אאפשר גישה ו/או שימוש של עובד אחר במשתמש האישי שלי וכן לא אסכים לבצע את עבודתי באמצעות משתמש אחר. כמו כן, אתחייב שלא לחשוף את פרטי המשתמש האישי שלי, בדגש על סיסמת הגישה למערכות ולא אתעד את פרטי המשתמש במקום חשוף לעיני כל.
  - במסגרת עבודתי, אשמור ואאחסן מסמכים המתעדים מידע רגיש בכפוף לנוהל האירגוני, באופן שימנע גישה של גורמים בלתי מורשים.
- שימוש בתיבת דוא״ל
  - לא אפתח הודעות דוא״ל מכתובות שולח שאינן מוכרות לי. אוודא בעת פתיחת ההודעה כי זו נשלחה מכתובת שולח לגיטימית ומוכרת.
  - לא אפתח קבצים ו/או אלחץ על קישורים שצורפו להודעות דוא״ל אשר נשלחו מכתובות שאינן מוכרות לי.

נהלי מחשוב ואבטחת מידע
נוהל אבטחת מידע לקליטת עובד חדש, שינוי תפקיד וסיום העסקה

- לא אמסור את פרטי המשתמש האישיים שניתנו לי ו/או את פרטי הגישה לתיבת הדוא"ל שברשותי, לגורמים שאינם מוכרים בוודאות.
- הנני מתחייב לדווח לאחראי אבטחת המידע בכל מקרה בו אקבל הודעת דוא"ל חשודה ו/או שהתקבלה מכתובת שולח בלתי מזוהה.

- שימוש בעמדת הלבנה
  - לא אחבר התקנים חיצוניים לעמדת הקצה. בכלל זה - התקני מדיה נתיקה (dok), מכשירים סלולריים ומחשבי לוח (טאבלטים).
  - לא אשתף את פרטי המשתמש האישי שלי עם אף גורם אחר (מלבד אחראי המחשוב) ולא אתעד אותם באופן גלוי.
  - לא אבצע הורדה של קבצים מרשת האינטרנט שלא לצרכים ארגוניים ובכל מקרה אוודא כי מקור הקבצים הינו מקור מזוהה ומהימן. במקרים של ספק - לא אבצע את הורדת הקבצים ללא אישור אחראי המחשוב.
  - לא אעשה שימוש ברשתות חברתיות כלל ו/או בשירותי דוא"ל שאינם במסגרת שרת הדוא"ל האירגוני.
  - הנני מתחייב לדווח לאחראי המחשוב אודות כל פעילות חריגה או חשודה המתרחשת בעמדת הקצה.

5. הנני מצהיר שהובא לידיעתי כי במקרה של שינוי תפקיד במועצה, מתאר ההרשאות שהוקצו לי לטובת מילוי תפקידי הקודם ישתנה, בהתאם לנהלי המידור המוגדרים.

6. הנני מצהיר שהובא לידיעתי כי במקרה של סיום העסקה במועצה, חל עליי האיסור לעשות כל שימוש במידע אליו נחשפתי במסגרת פעילותי במועצה, לרבות העברה לגורמים בלתי מורשים.

תאריך	שם מלא	אגף/ מחלקה	תפקיד	מספר זהות
_____	_____	_____	_____	_____

חתימת העובד

_____

חתימת מנמ"ר
המועצה

_____

נהלי מחשוב ואבטחת מידע

נוהל אבטחת מידע לקליטת עובד חדש, שינוי תפקיד וסיום העסקה