	שם המסמך: שימוש נאות בנכסי מידע (הנחיות אבטחת מידע לעובד)	עמוד 1 מתוך 19
	מספר הנוהל: **2.01**	תאריך תחולה: **01.01.2023**
	גרסה: **6.0**	תאריך עדכון: **15.07.2026**

שימוש נאות בנכסי מידע (הנחיות אבטחת מידע לעובד)

[2.01]

	שם המסמך: שימוש נאות בנכסי מידע (הנחיות אבטחת מידע לעובד)	עמוד 2 מתוך 19
	מספר הנוהל: **2.01**	תאריך תחולה: **01.01.2023**
	גרסה: **6.0**	תאריך עדכון: **15.07.2026**

<u>טבלת ניהול שינויים:</u>

כותב	מאשר	גרסה	תאריך אישור	מהות השינוי
יוסי קולטון	רותם רשטיק עינב	1.0	02/12/2022	כתיבת הנוהל
רותם רשטיק עינב	רותם רשטיק עינב	2.0	12/02/2023	תיקוף ואישור הנוהל
רותם רשטיק עינב	רותם רשטיק עינב	2.1	1/8/24	שינוי לוגו
רותם רשטיק עינב	רותם רשטיק עינב	2.3	13/8/24	שינוי ל-מנכ"ל העירייה
עמית ארד	רותם רשטיק עינב	3.0	27/1/25	הוספת חלק AI
עמית ארד	רותם רשטיק עינב	4.0	20/10/25	הוספת נספחים
אסף כלאף	יגאל מרזון	5.0	01/03/2026	עדכון
תני שפירא	יגאל מרזון	6.0	15/07/2026	הערות DPO

	שם המסמך: שימוש נאות בנכסי מידע (הנחיות אבטחת מידע לעובד)	עמוד 3 מתוך 19
	מספר הנוהל: **2.01**	תאריך תחולה: **01.01.2023**
	גרסה: **6.0**	תאריך עדכון: **15.07.2026**

תוכן עניינים:

1.כללי: **4**
2.מסמכים ישימים: **4**
3.מטרה: **4**
4.תחולה: **4**
5.הגדרות ומושגים: **5**
6.שיטה: **5**
7.אחריות וסמכות: **12**
8.בקרה ומעקב: **13**
9.נהלים קשורים: **13**
נספח א' – הנחיות אבטחת המידע לעובד רשות: **14**
נספח ב' – התחייבות לשמירת סודיות ואבטחת מידע: **15**
נספח ג' – ניטור רשת הרשות: **16**
נספח ד' – הצהרת אבטחת מידע למחזיק מחשב נייד: **17**
נספח ה' – התחייבות לשמירת סודיות לאחר העסקה: ..... שגיאה! הסימניה אינה מוגדרת.
נספח ו' – הסכמה לשמירת המידע: **19**

	שם המסמך: שימוש נאות בנכסי מידע (הנחיות אבטחת מידע לעובד)	עמוד 4 מתוך 19
	מספר הנוהל: **2.01**	תאריך תחולה: **01.01.2023**
	גרסה: **6.0**	תאריך עדכון: **15.07.2026**

1. כללי:

1.1. מערכות המחשוב העומדות לרשות עובדי העירייה לשם ניהול העשייה ומתן שירות לתושב, על כל מרכיביהן הן נדבך חשוב ומרכזי.

1.2. במערכת המחשוב נשמר מידע רב, מוניציפאלי, אישי ורגיש.

1.3. המידע נגיש לעובדי העירייה במסגרת פעילותם המקצועית.

1.4. כללי השימוש ואבטחת המידע המפורטים בנוהל הינם הבסיס להתנהלות ארגונית נכונה ומטרתם לסייע לעובדים בעבודתם ולמנוע חשיפת מידע או שימוש בלתי מורשה במידע, תוך עמידה בדרישות חוק ותקנות שונות.

2. מסמכים ישימים:

2.1. מדיניות אבטחת מידע וסייבר.

2.2. תקן ISO/IEC 27001: 2022, בקרות A.6.2,A.6.6 ,A5.10.

2.3. תקנות הגנת הפרטיות - תקנות 5 (א), 5 (ב).

2.4. תוה"ג- 10.1.

3. מטרה:

3.1. הגדרת ההנחיות לשימוש במערכות המחשוב הארגוניות במטרה לצמצם את סיכוני אבטחת המידע.

4. תחולה:

4.1. נוהל זה חל על השימוש בכלל אמצעי והתקני המחשוב, הרשת והתקשורת ברשות.

4.2. כל עובדי הרשות, עובדי צד ג', ספקים, יועצים וכו', אחראים להפעיל שיקול דעת באשר לשימוש נאות בידע, התקני אלקטרוניים ומשאבי מחשוב, וזאת, בהתאם לנהלי ומדיניות הרשות.

	שם המסמך: שימוש נאות בנכסי מידע (הנחיות אבטחת מידע לעובד)	עמוד 5 מתוך 19
	מספר הנוהל: **2.01**	תאריך תחולה: **01.01.2023**
	גרסה: **6.0**	תאריך עדכון: **15.07.2026**

5. הגדרות ומושגים:

5.1. אבטחת מידע - כלל האמצעים הטכנולוגיים והארגוניים הננקטים לשם צמצום סיכוני השימוש במערכות טכנולוגיית המידע בתחומי סודיות המידע, אמינותו, שלמותו ,זמינותו ושרידותו.

5.2. סייבר - משמש ככינוי למרחב הקיברנטי. מרחב ה"סייבר" משלב מידע, מערכות ואנשים.

5.3. אירוע אבטחת מידע וסייבר - אירוע המהווה סטייה מהפעילות התקינה של המערכת, פעילות חשודה, שינוי, אובדן או חשיפה לא מורשית של מידע. מצב אשר עלול לגרום לפגיעה בסודיות, בזמינות ובשלמות של מערכות המידע כולל פעולות שנעשות בזדון או בשגגה מתקיים על פי הגדרה מראש של תנאים לקיומו על ידי מערכת ממוחשבת או באופן מנהלי.

5.4. עובד – כל עובד עירייה או עובד תאגיד שמועסק בכל צורת העסקה (קבוע, זמני, מיקור חוץ, חוזה אישי וכד'). בנוסף נכללים בהגדרת העובדים כל מי שמקבל מחשב או כל אמצעי תקשובי טכנולוגי לצרכי עבודתו מהעירייה ואינם עובדי עירייה כגון, יועצים, עובדים במערכת החינוך וכד'.

5.5. מידע – נתונים בעלי ערך או הקשר פרטי או מוניציפאלי שחשיפתם יכולה לגרום נזק לעירייה או לפגיעה בפרטיות.

5.6. מערכות מידע – כלל מערכות המידע המשמשות את העובד ככלי עזר טכנולוגי לשיפור ותמיכה בעבודתו השוטפת: מערכת הפעלה במחשב המשרדי, תיבת מייל, יוזר והרשאה למערכות גבייה, פיננסים, רישום למוסדות החינוך, שכר, נתוני משרד החינוך ועוד.

5.7. מחלקת מערכות המידע והמחשוב - יחידת המחשוב של העירייה (תחת אגף חדשנות, אסטרטגיה ודיגיטל).

6. שיטה:

6.1. <u>תקלות מחשוב</u>

6.1.1. במקרים של תקלה במערכות המחשב, העובד יפנה למוקד העירייה שיעביר את הפנייה למחלקת מערכות מידע ומחשוב.

6.1.2. תיקון וטיפול בתקלות ייעשה אך ורק באמצעות גוף המחשוב של העירייה – מחלקת מערכות מידע.

6.2. <u>שמירת סודיות והגנה על פרטיות</u>

6.2.1. העובד מתחייב, עם קבלתו בעירייה ותחילת העסקתו, על שמירת סודיות, אבטחת המידע והגנת הפרטיות (עם חתימתו על חוזה העסקה , יקרא ויחתום על מדיניות שימוש נאות במערכות מחשוב וכן על הסכם סודיות -**NDA**).

6.2.2. מסמך להחתמת עובד עירייה- https://www.ganeytikva.org.il/smartforms/466/

6.2.3. מסמך להחתמת ספק (עובד מיקור חוץ)- https://www.ganeytikva.org.il/smartforms/410/

6.2.4. העובד מתחייב שלא למסור כל מידע, בכל דרך: ממוחשב ,בעל פה או אחר , שהגיע אליו מתוקף תפקידו, לכל גורם אלא בסמכות וברשות מנכ"לית העירייה. את הסכמת המנכ"לית להעברת מידע יש לקבל בכתב בלבד (מייל, וואסטאפ, הצהרה וכו').

6.2.5. העברת מידע לספקים וגופים (גורמים חיצוניים) שעובדים עם העירייה תאושר רק לאחר שחתם הגורם החיצוני על מסמך אבטחת סודיות אל מול יועמ"ש העירייה.

6.2.6. הוראה זו חלה על העובד גם לאחר שסיים את עבודתו בעירייה.

6.2.7. על העובד חלה החובה לפעול על פי הוראות חוק הגנת הפרטיות ותקנותיו ולא לחשוף מידע אישי, רגיש או מידע העלול להוות פגיעה בעירייה, אלא בסמכות וברשות מנכ"לית העירייה.

6.2.8. במסגרת העבודה במערכות המידע, ישנו שיח והעברת נתונים אל מול ספקי נותני שירותים שונים – חל איסור להעביר מידע, בעל פה או בקובץ לגורם חיצוני.

6.2.9. במידה ונדרש להעביר מידע לגורם חיצוני, הנ"ל יבוצע לאחר קבלת אישור ממנהלת מערכות המידע, תוך צמצום המידע למינימום הנדרש ותוך שימוש באמצעי הגנה רלוונטיים (הצפנת המידע).

6.2.10. ספקים אשר במסגרת עבודתם נחשפים ונדרשים למידע מתוך מערכות המידע, יאושרו לאחר חתימתם על הסכם שמירת סודיות ואבטחת המידע על פי חוק הגנת הפרטיות.

6.3. <u>הזדהות והרשאות</u>

6.3.1. פרטי ההזדהות למערכות המחשוב של המשתמש הינם אישיים ואינם ניתנים להעברה.

6.3.2. חל איסור לעשות שימוש בפרטי הזדהות של משתמש אחר.

6.3.3. אין להעביר/למסור סיסמא אישית לעובד אחר, באותה מחלקה או במחלקה אחרת במסגרת התפקיד, כולל בסיום תפקידו בעירייה. עובד אחר שייקלט לאותו תפקיד יקבל סיסמא ושם משתמש חדשים.

6.3.4. הרשאות הגישה למערכות הינם בהתאם לתפקיד העובד.

6.3.5. חל איסור לגשת לתיקיות/קבצים/מערכות שאינם חלק מהגדרת התפקיד.

6.3.6. במידה וקיימות למשתמש הרשאות עודפות- נדרש לפנות לצוות המחשוב להסרתם.

6.3.7. אין להתיר למשתמש מורשה אחר לעבוד על תוכנה הדורשת הזדהות באמצעות שם המשתמש שאינו שלו.

6.4. <u>סיסמאות</u>

6.4.1. הסיסמה למערכות המחשוב הינה אישית ואינה ניתנת להעברה.

6.4.2. יש לעשות שימוש במחשב אך ורק בסיסמאות הגישה שניתנו לעובד כמפורט לעיל.

6.4.3. במקרים חריגים שבהם נמסרה הסיסמא על רקע אילוץ תפעולי, העובד יפעל בהקדם להחלפתה בעזרת מחלקת מערכות המידע והמחשוב. אישור להעברת הסיסמא לעובד אחר יהיה אך ורק על ידי מנהלי האגפים של העירייה או מנכ"לית העירייה.

6.4.4. הסיסמה תורכב מ-8 תווים לפחות הכוללים אותיות גדולות, אותיות קטנות, ספרות ותווים מיוחדים(@!#).

6.4.5. חל איסור לשמור את הסיסמה בסמוך לעמדת הקצה (מתחת למקלדת, על המסך, במגירה לא נעולה) או לכרטיס החכם.

6.4.6. אחת ל 3 חודשים יידרש העובד להחליף סיסמה.

6.4.7. שישה ניסיונות כושלים של גישה לעמדה תביא לנעילת העמדה עבור אותו משתמש ל-6 שעות.

6.4.8. במקרה של נעילת עמדת משתמש נדרש לפנות לצוות המחשוב לשחרור נעילת המשתמש בתוך 6 השעות מהניסיון הכושל, לאחר מכן ישתחרר לבד.

6.5. <u>אבטחת סביבת העבודה</u>

6.5.1. הגנה על המידע המצוי בסביבת העבודה האישית של כל עובד מפני גישה פיזית של גורמים לא מורשים יכולה למנוע חשיפה, גניבה, שינוי או נזק של המידע. כל עובד אחראי לאבטחת סביבת העבודה האישית שלו .אבטחת סביבת העבודה תתבסס על שני עקרונות מרכזיים:

6.5.1.1. מדיניות שולחן נקי - מסמכים רגישים לא יוותרו חשופים על השולחן כאשר העובד עוזב את סביבת העבודה בסוף יום העבודה. בעת עזיבת סביבת העבודה ינעל העובד את המסמכים הרגישים בתוך ארון / מגירה נעולה. העקרונות הנ"ל תקפים גם לגבי מדיה מגנטית/אופטית.

6.5.1.2. מדיניות מסך נקי - אין להותיר את המחשב נגיש לצפייה ושינוי נתונים כאשר עוזבים את סביבת העבודה- נדרש לנעול את המחשב. בסוף יום עבודה נדרש לבצע שמירה של המסמכים הפתוחים, או כיבוי של תחנת העבודה. הכיבוי יעשה בדרך הנכונה בלבד ("התחל" או start + "כיבוי"). מעת לעת לצורך החלת עדכונים לתוכנות השונות מחלק המחשוב תבצע ריסטרט או כיבוי יזום לתחנות העבודה בהתראה מראש.

6.6. <u>אבטחת קבצים ברשת העירייה</u>

6.6.1. הנתונים בתיבות הדואר האלקטרוני ובכונן האישי של העובדים יישמרו על פי הכללים בעירייה, אך ורק בשרתי האחסון המרכזיים אשר מגובים מידי יום במלואם באחריות מחלקת מערכות מידע ומחשוב.

6.6.2. שרתי האחסון מיועדים לאחסן חומר הקשור בצרכי העבודה בלבד ואין לשמור בהם מידע אישי או אחר, אשר אינו שייך לעבודה השוטפת של העירייה.

6.6.3. המידע המאוחסן בתחנת העבודה האישית איננו מגובה וזוכה לרמת אבטחה נמוכה יותר מאשר בשרתים המרכזיים. בכדי להסיר ספק, יודגש כי האחריות על הנתונים אשר יישארו בכונן המקומי הינה על המשתמש בלבד!

6.6.4. בשום מקרה אין לשמור קבצים רגישים באופן מקומי על המחשב.

6.6.5. מסמכים בעלי חשיבות גבוהה (מכרזים, הצעות מחיר וכיוב') ישמרו אך ורק בתיקיות המיועדות לכך.

6.6.6. חל איסור להעתיק קבצים מרשת העירייה לכוננים חיצוניים ללא אישור מחלקת מערכות מידע ומחשוב.

6.6.7. קובץ המכיל מידע רגיש יוצפן בסיסמה טרם שמירתו / העברתו.

6.6.8. יש לבחון עם מי משתפים את המידע, ולצמצם ככל הניתן את המידע שמעבירים (לדוגמה אם אין הכרח בכל השדות בטבלה מסוימת- יש לצמצם למינימום ההכרחי).

6.7. <u>שימוש בדואר אלקטרוני</u>

6.7.1. השימוש בדוא"ל נועד לצרכי עבודה והתפקיד ולא לצרכים פרטיים (רישום לאתרי אינטרנט, רשתות חברתיות, מסעדות, קופונים, מועדונים וכו'). הדוא"ל וכל המידע המצוי בו מיועדים לצורכי עבודה בלבד ומהווים אמצעי עבודה של הארגון.

6.7.2. בכפוף להוראות הדין, הארגון רשאי לנטר, לעיין, לאחזר ולגשת לתיבת הדואר ולתוכנה, ככל שהדבר נדרש לצרכים תפעוליים, אבטחת מידע, המשכיות עסקית, בירור חשד להפרת דין או נהלי הארגון, או לכל צורך ארגוני לגיטימי אחר.

6.7.3. חל איסור לעשות שימוש בתיבות דוא"ל פרטיות לצרכי עבודה (כגון **walla**,**gmail** וכו').

6.7.4. נהלי סיווג מסמכים חלים גם על מסמכים המועברים בדואר האלקטרוני, משמע אין להעביר מידע רגיש ארגוני או אישי לגורם חיצוני ללא אישור ובאמצעים לא מאובטחים.

6.7.5. חל איסור לשלוח דוא"ל בעלי תוכן פוגעני.

6.7.6. חל איסור לשלוח דואר זבל, מכתבי שרשרת, חומר פוגע או משמיץ או חומר העלול לפגוע בעירייה, עובדיה או תושביה וכן דוא"ל המפריעים למהלך התקין של העבודה.

6.7.7. תיבת הדוא"ל מנוהלת בשרת מרכזי ומנוטרת לטובת מניעת ביצוע עבירה פלילית ו/או משמעתית וכן איתור מקרים בהם קיים חשש שבוצעה עבירה כל זאת בכפוף לשמירה על צנעת הפרט...

6.7.8. יש להימנע מפתיחת דואל שהתקבל מאיש קשר שאינו מוכר תוך שימת לב לצרופות במייל, קישורים לאתרים, ונוסח המצביע על דחיפות מסויימת – במידה וזוהה מייל חשוד, כאמור, ידווח העובד על כך למחלקת מערכות מידע לצורך חסימת השולח יש להקפיד לא ללחוץ על לינקים או צרופות במייל החשוד.

6.7.9. במידה ונעשה שימוש בדוא"ל המשרדי בטלפון הנייד- נדרש לקבוע סיסמת כניסה לטלפון הנייד.

6.7.10. הפצת מסרים בתפוצה רחבה תיעשה במערכות ייעודיות ולא בתיבת הדוא"ל, ככל הינתן. לצד זאת, שליחת דוא"ל למספר נמענים רחב יתבצע באמצעות "עותק מוסתר" (**BCC**) בלבד וזאת על מנת למנוע חשיפת הכתובות.

6.7.11. הארגון רשאי להעביר את תיבת הדוא"ל או תוכנו לעובד אחר, לממונה, למחליף זמני או לכל גורם מוסמך אחר בארגון, בין היתר בעת היעדרות, סיום העסקה, שינוי תפקיד או כל צורך ארגוני אחר.

6.7.12. להלן הפרמטרים לקבלה ושליחה של דוא"ל:

6.7.12.1. הגודל המקסימלי המותר לשליחה או לקבלה של דוא"ל בודד לא יעלה על 50MB.

6.7.12.2. מספר הנמענים המקסימלי לשליחה או קבלה של הודעת דוא"ל מחוץ לעירייה לא יעלה על 250 נמענים.

6.7.12.3. מספר הנמענים המקסימלי לשליחה או קבלה של הודעת דוא"ל בתוך העירייה לא יעלה על 300 נמענים.

6.7.12.4. הודעות ופרסומים מאתרי שיתוף ואתרי רשתות חברתיות ייחסמו(spam).

6.8. <u>שימוש באינטרנט וברשתות חברתיות</u>

6.8.1. חל איסור לעשות שימוש בלתי נאות באינטרנט אשר עלול לפגוע בתדמית העירייה לרבות:

6.8.2. ביצוע פעולות בלתי חוקיות כגון הימורים, **BIT-COIN** וכו'.

6.8.3. גלישה לאתרים בלתי ראויים- כגון אתרים למבוגרים.

6.8.4. גלישה לאתרים שאינם מאושרים כגון אתרים לצפייה ישירה בסרטים.

6.8.5. גילוי וחשיפת מידע רגיש אודות העירייה.

6.8.6. הצגת דעות אישיות כמייצגות את העירייה.

6.8.7. חל איסור כניסה ושימוש ברשתות חברתיות ממחשבי העירייה לצרכי עבודה אלא אם במסגרת העבודה העובד משתמש במערכות אלה לעבודתו (כגון שיווק ופרסום) (**TWITER** ,**FACEBOOK** וכו').

6.8.8. חל איסור לפרסם מידע רגיש ברשתות החברתיות.

6.8.9. חל איסור להוריד למחשבי העירייה קבצים/סרטים/תמונות אשר אינן מיועדים לצרכי העבודה של העירייה.

6.8.10. נדרש לשים לב להנחיות גלישה בטוחה הבאים:

6.8.11. גלישה לאתרים שכתובת האתר מתחילה בכיתוב **HTTPS** ולצידו סימן מנעול- מעיד על אתר מאובטח.

6.8.12. גלישה לאתרים עם סיומות מוכרות כגון **il**, **us**, **gov**, **com**- נדרש להימנע לגלישה באתרים עם סיומות כגון **ru**, **ch**,**exe**.

6.8.13. מניעה מגלישה לאתר לא מוכר שמעוצב בצורה לא מקצועית ולא ניתן להפיק מידע על האתר(אין פרטי קשר, אין תקנון, אין מדיניות פרטיות).

6.9. <u>שימוש בפלטפורמות **AI**</u>:

6.9.1. טרם שימוש בפלטפורמות **AI** ציבוריות מרשת העירייה יש לקבל אישור ממנהלת אגף חדשנות אסטרטגיה ודיגיטל. בחירת פלטפורמות **AI** תביא בחשבון היבטי אבטחה, אמינות ופרטיות – ככלל יבוצע שימוש ב-**AI** בגרסאות העסקיות שלהן (רישיון בתשלום) שכן הן מספקות יכולות מהימנות יותר ופרטיות יותר.

6.9.2. חל איסור להזין בפלטפורמת **AI** מידע רגיש, מסווג או אישי, בנוסף רישום של מנוי פרטי יבוצע על ידי יצירת חשבון שאינו מזוהה עם העירייה וזאת על מנת להקשות על אפשרות הקישור בין השאילתות המגיעות למערכת לבין מקור השאילתה - צרכים חריגים יעלו לאישור של מנהלת אגף אסטרטגיה, חדשנות ודיגיטל והיועמ"ש לשיקול התממת/השחרת פרטים מזהים.

6.9.3. יש לנסח שאילתות ל-**AI** בצורה שלא תחשוף מידע עסקי, רגיש ו/או פרטים מזהים של העירייה, עובדיה ותושביה. לדוגמה, אין צורך לציין עיריית גני תקווה, מספיק לציין עירייה.

6.9.4. חל איסור להעלות קבצים המכילים מידע אישי של תושבים, עובדים, נכסים, עסקים, תלמידים וכיו"ב לפלטפורמות **AI** ציבוריות. חריגים לכך ידרשו אישור והנחיות ייעודיות של מנהלת אגף אסטרטגיה, חדשנות ודיגיטל. כך לדוגמה, יש לשים לב לא לשתף קבצי אקסל עם מידע רגיש, קורות חיים וכדומה.

6.9.5. במקרים בהם מערכות **AI** מעבדות מידע אישי ממאגרי המידע – הנ"ל יהיה כפוף לאישור מנהל המאגר ולאישור התהליך המלא בוועדה להעברת מידע בין גופים ציבוריים.

6.9.6. יש לבדוק על ידי אדם כל תוצר המתקבל על ידי כלי בינה מלאכותית ולבצע אימות נכונות המידע שהתקבל.

6.9.7. בעת ייצור תמונות באמצעות **AI** יש לשים לב לשים לתנאי השימוש. ככלל, בעת פרסום של תוצר יש לכתוב מקור / קרדיט לתמונה ולציין את שם הכלי שבו נעשתה. בחלק מכלי יצירה ב**AI** כגון תמונות / מצגות, יש לוודא כי קיים סימן מים עם שם הכלי באופן דיפולטיבי על התמונה.

6.10. <u>עמדת עבודה</u>

6.10.1. חיבורי החומרה (מחשב, מסך, מדפסת, סורק, מכונת צלום) לשקעי התקשורת יתבצעו ע"י אגף המחשוב בלבד.

6.10.2. בעת תקלה באחד ממרכיבי החומרה של משתמש הקצה נדרש לפנות ל אגף המחשוב בלבד.

6.10.3. בעת מעבר משרדים נדרש לעדכן את אגף המחשוב לטובת העברת תחנות העבודה.

6.10.4. משתמש הקצה נדרש לאסוף את החומר מהמדפסת לאחר שליחתה להדפסה, על מנת לוודא כי החומר במודפס לא יילקח ע"י גורם לא מורשה.

6.10.5. כל חומרה שאינה בשימוש ו/או תקולה לרבות מדיה מגנטית ,שסופקו ע"י העירייה, יועברו לאגף המחשוב.

6.10.6. חל איסור לחבר חומרה פרטית כלשהי לרשת/מחשבי העירייה ללא אישור מחלקת מחשוב.

6.10.7. באחריות העובד לשמור על ציוד העירייה וניקיונו ככל הניתן.

6.11. <u>מחשבים ניידים</u>

6.11.1. בעלי מחשב נייד אחראים באופן אישי על שלמותו הפיזית של המחשב שברשותם ועל המידע האגור עליו.

6.11.2. מחשבים ניידים עלולים להיגנב, אין להשאיר מחשב נייד מחוץ לתחומי משרדי העירייה או מחוץ לביתו של המשתמש (ובפרט ברכב) בלא השגחה.

6.11.3. כל נהלי אבטחת המידע חלים על עובדי העירייה גם בשימוש במחשב מחוץ לרשת העירייה.

6.11.4. יש להקפיד על נהלי האבטחה בעת שימוש בדואר האלקטרוני או בעת גלישה מרשתות חיצוניות לרשת העירייה.

6.11.5. אין לשמור קבצים רגישים על המחשב הנייד.

6.11.6. חל איסור להעביר מחשב נייד למשתמש אחר בלא אישור בכתב או בדואר האלקטרוני ממחלקת המחשוב.

6.11.7. מחשב נייד מחויב בסיסמה לצורך כניסה.

6.12. <u>שימוש באמצעי זיכרון</u>

6.12.1. בכלל מחשבי הארגון קיימת חסימת התקנים ניידים.

6.12.2. עובד אשר נדרש לצורך עבודתו להתקן זכרון נייד, יפנה למחלקת המחשוב לקבלת אישור.

6.12.3. חל איסור שימוש בהתקן זכרון נייד אשר לא אושר והוחרג במחלקת המחשוב.

6.12.4. בעת תקלה או סיום הצורך בהתקן זכרון יש להעבירו למחלקת המחשוב למחיקה או גריטה.

6.13. <u>התקנת תוכנות</u>

6.13.1. האפשרות להתקנת תוכנה חסומה על ידי המשתמש בעמדת קצה ברשת העירייה.

6.13.2. הוספת/הסרת תוכנה או עדכונים והתקנות ייעשה ע"י מחלקת המחשוב בלבד.

6.14. <u>ארונות תקשורת</u>

6.14.1. חל איסור מוחלט לגעת בכבילת הרשת, ארונות וציוד התקשורת. טיפול בארונות הללו יתבצע על ידי מחלקת המחשוב בלבד.

6.14.2. חל איסור מוחלט לחבר לרשת הארגונית ציוד ללא אישור מחלקת המחשוב, לרבות מחשבים ניידים.

6.15. <u>מכשירים סלולריים</u>

6.15.1. במידה וחשבון הדואר הארגוני מוגדר במכשיר הסלולרי חובה להגדיר סיסמת גישה למכשיר.

6.15.2. יש לדווח מיידית על אבדן או גניבת מכשיר סלולרי לצוות המחשוב לצורך החלפת סיסמת המכשיר או ניתוקו מהמידע הארגוני.

6.15.3. חל איסור לצלם מידע רגיש ממערכות המידע באמצעות הטלפון הנייד.

6.15.4. באחריות בעל מכשיר לוודא ביצוע כל בקשת עדכון של תכנת האנטיוירוס ללא דיחוי.

6.16. <u>עדכוני אבטחה</u>

6.16.1. עדכוני מערכות הפעלה מתבצעים על מחשבי העירייה באופן אוטומטי בחיבור לרשת.

6.16.2. באחריות בעל מחשב לוודא ביצוע כל בקשת עדכון של תכנת האנטיוירוס ללא דיחוי.

6.17. <u>תוכנות</u>

6.17.1. השימוש במערך המחשוב של העירייה ייעשה אך ורק בתוכנות מורשות שהותקנו על ידי מחלקת מערכות המידע והמחשוב.

6.17.2. חל איסור מוחלט לעשות כל שימוש בתוכנות פרטיות או תוכנות שהורדו באמצעות האינטרנט.

6.17.3. אין לעשות שימוש במחשבי העירייה בתוכנות שאין לגביהן רישיון חוקי. העובר על הוראה זו יהיה אחראי אישית בפני החוק.

6.17.4. בסמכות מחלקת מערכות המידע והמחשוב להסיר כל תוכנה שהותקנה ללא רשות עם זיהוייה.

6.17.5. אין להעתיק תכנות שבשימוש העובד לצרכים פרטיים.

6.17.6. על העובדים לציית לחוקי זכויות יוצרים והגבלות היצרנים.

6.18. <u>דיווח על אירועי אבטחה</u>

6.18.1. משתמש המזהה אירוע/ בעיית אבטחה ידווח עליה באופן מידי למחלקת המחשוב.

6.18.2. להלן סוגי האירועים הנדרשים בדיווח:

6.18.3. אובדן/גניבה/היעלמות של מידע רגיש.

6.18.4. אובדן/ גניבה של התקנים ניידים ומדיה מגנטית.

6.18.5. משתמש החושד כי נעשה שימוש בשם המשתמש או הסיסמה שלו, שלא על ידו.

6.18.6. חשד לחשיפה של מידע רגיש לגורם לא מורשה.

6.18.7. המצאות גורם לא מורשה במתחמים הקריטיים כפי שהוגדרו ע"י מחלקת המחשוב.

6.19. <u>ביקורות</u>

6.19.1. במסגרת הפעילות של מחלקת המחשוב יבוצעו ביקורות אבטחה פיזיות, ניהוליות וטכניות לבחינת יישום ההנחיות במשרדים השונים.

6.19.2. דו"ח ביקרות וחריגה מנהלים יועברו למנהל האגף בו התבצעה הביקורת.

6.20. <u>הפרה של הנחיות אבטחת מידע</u>

6.20.1. במידה ויתעורר חשש לביצוע עבירה ע"י משתמש קצה, תהיה הנהלת העירייה רשאית לבצע פעולת מעקב של נתוני התקשורת, נתוני הגלישה ונתוני תיבת הדוא"ל של אותו עובד וכן לחדור לתכתובות הדוא"ל המקצועיות שניהל העובד.

6.20.2. הנהלת העירייה תהיה רשאית להשתמש במידע אשר יושג על ידה לשם הגשת תלונה במשטרה ו/או לצורך עריכת חקירת משמעת כנגד העובד.

6.20.3. הנהלת העירייה תהיה רשאית להשתמש במידע לצורך נקיטת אמצעי משמעת כנגד העובד.

6.21. <u>סיום העסקת עובד</u>

6.21.1. בעת סיום העסקת עובד, מכל סיבה, על העובד להחזיר את כל הציוד אשר סופק לו על ידי העירייה, לרבות ציוד מחשוב, סלולאר, אחסון.

6.21.2. עובד המסיים את תפקידו תחסם המשתמש והגישה למערכות העירייה.

7. אחריות וסמכות:

<u>מנכ"ל העירייה</u> – הינו בעל אחריות כוללת לכל התהליכים בארגון. טיפול בנושאים מערכתיים ומסירת מידע לגורמים חיצוניים אם נדרש.

<u>מחלקת משאבי אנוש</u> – הינה אחראית להחתים כל עובד בעירייה, כולל עובדים חדשים שנקלטים על הצהרת סודיות (והתחייבות שימוש נאות במערכות מחשב).

<u>מנהלת מערכות מידע</u> – הינה בעלת אחריות כוללת לכל נושאי המחשוב, כולל תפעול ובקרה, תכנון מערכתי, ציוד ותוכנות לאורך מחזור חיי המוצר.

<u>כלל העובדים</u> אחראים ליישום נוהל זה.

	שם המסמך: שימוש נאות בנכסי מידע (הנחיות אבטחת מידע לעובד)	עמוד 13 מתוך 19
	מספר הנוהל: **2.01**	תאריך תחולה: **01.01.2023**
	גרסה: **6.0**	תאריך עדכון: **15.07.2026**

8. בקרה ומעקב:

8.1. מנמ"ר הרשות ומנהל אבטחת מידע וסייבר.

9. נהלים קשורים:

9.1. נוהל בקרת גישה.

9.2. נוהל אבטחת מידע במשאבי אנוש.

	שם המסמך: שימוש נאות בנכסי מידע (הנחיות אבטחת מידע לעובד)	עמוד 14 מתוך 19
	מספר הנוהל: **2.01**	תאריך תחולה: **01.01.2023**
	גרסה: **6.0**	תאריך עדכון: **15.07.2026**

נספח א' – הנחיות אבטחת המידע לעובד רשות:

1. הנני מאשר כי קראתי את הנחיות אבטחת מידע כאמור לעיל וכי הבנתי את תוכנן ומשמעותן ואת חובותיי.
2. חתימה על נספח זה מהווה הצהרה מצידי, כי אני מקבל על עצמי את כל החובות המוטלות עליי לפי הנחיות אלו.
3. ידוע לי כי הפרת התחייבויותיי תאפשר לרשות לנקוט כלפי בכל הצעדים על פי כל דין ועל פי נהלי הרשות.

	שם המסמך: שימוש נאות בנכסי מידע (הנחיות אבטחת מידע לעובד)	עמוד 15 מתוך 19
	מספר הנוהל: **2.01**	תאריך תחולה: **01.01.2023**
	גרסה: **6.0**	תאריך עדכון: **15.07.2026**

נספח ב' – התחייבות לשמירת סודיות ואבטחת מידע:

הסכם התחייבות זה אינו מבטל נהלים/הוראות קודמות, והוא מהווה חלק בלתי נפרד מתהליך קליטת עובדים חדשים ברשות, שמטרתו להדגיש ולהבהיר את הוראות אבטחת המידע והסייבר.

1. הנני מצהיר כי קראתי את נהלי אבטחת המידע והסייבר הרלוונטיים, והובהר לי על-ידי הגורמים המוסמכים כי חלה עליי החובה לשמור בסוד מוחלט כל מידע אליו איחשף במישרין או בעקיפין בעת עבודתי.

2. הובא לידיעתי כי המידע המצוי במאגרי המידע של הרשות ו/או מאגרים אחרים אשר שותפו עימי במסגרת עבודתי, הינו חסוי ומשמש לצרכי עבודה בלבד ואין לעשות בו שימוש לצרכים אישיים.

3. מבלי לפגוע בכלליות האמור בסעיף 1, הנני מתחייב שלא לעיין או לשלוף כל מידע ממאגרי הרשות ו\או ממאגרים אחרים אשר שותפו עימי במסגרת עבודתי, למטרות שאינן קשורות לעבודתי, כמו כן, לא אפרסם ולא אוציא מחזקתי מידע, בין אם במישרין ובין אם בעקיפין.

4. אני מתחייב לפעול בהתאם להוראות חוק הגנת הפרטיות, התשמ"א-1981 והוראות כל דין הנוגע לעניין.

5. אני מתחייב כי לאחר סיום עבודתי ברשות, מכל סיבה שהיא, לא אשאיר ברשותי כל מסמך ו/או חומר שנמסרו לי או הגיעו לרשותי בעקבות ו/או כתוצאה מעבודתי ברשות ולהחזיר מיד כל מסמך, מכשיר, חפץ או חומר כאמור עם סיום עבודתי ברשות ו/או להשמיד בתיאום מראש כל מידע שנאסף ו/או נשאר ברשותי ושלא הועבר לרשות המעסיק.

	שם המסמך: שימוש נאות בנכסי מידע (הנחיות אבטחת מידע לעובד)	עמוד 16 מתוך 19
	מספר הנוהל: **2.01**	תאריך תחולה: **01.01.2023**
	גרסה: **6.0**	תאריך עדכון: **15.07.2026**

נספח ג' – ניטור רשת הרשות:

הסכם התחייבות זה אינו מבטל נהלים/הוראות קודמות, והוא מהווה חלק בלתי נפרד מתהליך קליטת עובדים חדשים ברשות, שמטרתו להדגיש ולהבהיר את הוראות אבטחת המידע והסייבר.

1. המרחב הווירטואלי אשר הוקצה לך כולל: שטח זיכרון לאחסון ההודעות המתקבלות והנשלחות בדוא"ל, שטח זיכרון לאחסון תיקיות ומסמכים וכן, שטח לתיקיות משותפות שהשימוש בהן נעשה בהתאם להרשאות כניסה שנקבעות בתיאום מנהלי המחלקות.
2. במסגרת התמיכה המחשובית בשל תקלה או צורך בקבלת הדרכה לביצוע פעולות במחשב קיימת האפשרות להשתלטות מרחוק של גורמי המחשוב לתיקון תקלות, בהסכמתך ובנוכחותך.
3. לידיעתך, הרשות סורקת באמצעות EDR את כלל אמצעי הקצה והמשאבים אשר מחוברים אליו בכל שעות העבודה ולאחריה וכן את המידע השמור בתיקיות לזיהוי התנהגות חריגה ומניעת וירוסים. הרשות אינה רואה בהסכמתך לניטור אוטומטי מחשש לווירוסים, והפרת מדיניות - הסכמה למעקב ספציפי לאיסוף נתונים אישיים והסכמה לקריאת תוכן תכתובת האי-מייל האישית באותן תיבות.
4. תשומת ליבך כי "משאבי מחשוב אישיים" נשמרים, וזאת לצורכי גיבוי וניטור בלבד.
5. עם סיום יחסי העבודה בינך לבין הרשות, ועל מנת שניתן יהיה לעשות שימוש ב"משאבי המחשוב של הרשות" לצרכי עבודה וצרכים מקצועיים בלבד, יש לוודא מחיקה של תכתובת אישיות, קבצים אישיים והפעלת שליחת הודעה אוטומטית המפנה את הפונים אליך לגורם האחראי ובה דרכי התקשרות עמו.
6. הרשות אינה מקיימת מעקב בחומרים הנמצאים ב"משאבי המחשוב האישיים" שהנך מקיים לצרכיך האישיים למעט בהתקיים נסיבות חריגות המצדיקות זאת. וכן, שננקטו אמצעים טכנולוגיים חודרניים המעידים על שימוש בלתי ראוי שלך כעובד בטכנולוגיות שהועמדו לרשותך לצרכי עבודה.
7. מעקב אחר חומרים הנמצאים ב"משאבי המחשוב האישיים" תתאפשר רק לאחר קביעת סיבה ברורה אשר לה זיקה לאינטרסים הלגיטימיים של הרשות כמקום עבודה.

הנני מסכים מדעת ומרצון לביצוע מעקב ב- "משאבי המחשוב האישיים" אשר מחוברים על ידי לסביבת העבודה ברשות ותיבת המייל שניתנה לצורכי עבודה, בהתקיים נסיבות חריגות המצדיקות זאת. וכן, שננקטו אמצעים טכנולוגיים חודרניים המעידים על שימוש בלתי ראוי שלי כעובד בטכנולוגיות שהועמדו לרשותי לצרכי עבודה. עם סיום יחסי עובד/ מעביד הנני מסכים מדעת ומרצון שהרשות תהיה רשאית לעשות שימוש ב- "משאבי המחשוב האישיים" לצרכי עבודה וצרכים מקצועיים בלבד.

	שם המסמך: שימוש נאות בנכסי מידע (הנחיות אבטחת מידע לעובד)	עמוד 17 מתוך 19
	מספר הנוהל: **2.01**	תאריך תחולה: **01.01.2023**
	גרסה: **6.0**	תאריך עדכון: **15.07.2026**

נספח ד' – הצהרת אבטחת מידע למחזיק מחשב נייד:

הסכם התחייבות זה אינו מבטל נהלים/הוראות קודמות, והוא מהווה חלק בלתי נפרד מתהליך קליטת עובדים חדשים ברשות, שמטרתו להדגיש ולהבהיר את הוראות אבטחת המידע והסייבר.

1. השימוש במחשב הנייד יתבצע לצורך ביצוע עבודתי בלבד ולא לצרכים פרטיים.
2. אין להעביר את המחשב הנייד לשימוש אף גורם אחר ללא אישור בכתב של מנהל אבטחת מידע וסייבר ברשות.
3. בסיום העבודה עם מחשב הנייד, יש לבצע נעילה\כיבוי של המחשב.
4. המחשב הנייד יהיה בפיקוח העובד בכל עת. אין להשאיר את המחשב ללא השגחה במקומות ציבוריים, ברכב, או בכל מקום בו קיים חשש לפריצה\גניבה.
5. אין לשמור מידע רגיש בתצורה מקומית על המחשב.
6. אין לחבר את המחשב הנייד לרשת אלחוטית ללא סיסמא או לרשת ציבורית בעלת סיסמא (לדוגמא: בתי קפה וחנויות).
7. מחזיק המחשב הנייד ידווח מיידית למנהל אבטחת מידע וסייבר ברשות בכל מקרה של גניבה/אובדן או חשד לגניבה/אובדן של מחשב נייד שהועמד לרשותו ע"י הרשות.
8. ידוע לי כי התחייבות זו מהווה חלק בלתי נפרד מהתקשרותי עם הרשות ומהווה חלק מהסכם ההתקשרות עליו חתמתי עם הרשות. אני מודע/ת לכך כי הפרת תוכן הצהרה זו יכולה להיגרם עקב מעשה מכוון ו/או רשלנות ו/או מחדל, והאחריות בגינן, זהה היא.
9. בסיום העסקתי ברשות, אני מתחייב/ת למסור לאגף אסטרטגיה, חדשנות ודיגיטל את מחשב הנייד שקיבלתי מהרשות.

	שם המסמך: שימוש נאות בנכסי מידע (הנחיות אבטחת מידע לעובד)	עמוד 18 מתוך 19
	מספר הנוהל: **2.01**	תאריך תחולה: **01.01.2023**
	גרסה: **6.0**	תאריך עדכון: **15.07.2026**

1. אני מצהיר בזאת שהובהר לי ע"י אגף משאבי אנוש, כי חובה עלי לשמור בסוד מוחלט כל מידע מסווג, פרטי, עסקי או מוגן, אליו נחשפתי במישרין או בעקיפין בעת עבודתי.

2. אני מתחייב/ת בזאת שלא אמסור דבר לאדם שאינו מוסמך באשר למידע זה בין בכתב, בין בעל פה, בין ברמז או במפורש או כל דרך אחרת, לאחר סיום העסקתי ברשות.

3. הובהר לי היטב כי שמירת הסודיות כאמור לעיל, הכרחית מטעמים של הגנת הפרטיות, וכי גילוי מידע זה לכל גורם, לרבות בני משפחה, שאינם מורשים לקבלו מתוקף תפקידם, מהווה עבירה על החוק.

	שם המסמך: שימוש נאות בנכסי מידע (הנחיות אבטחת מידע לעובד)	עמוד 19 מתוך 19
	מספר הנוהל: **2.01**	תאריך תחולה: **01.01.2023**
	גרסה: **6.0**	תאריך עדכון: **15.07.2026**

נספח ו' – הסכמה לשמירת המידע:

1. הנני מאשר שבמהלך העסקתי ברשות יועבר מידע הנוגע למצבי הכלכלי (הכנסות, אישורי מחלה וכדומה) לרשות לצורך בחינת תנאי העסקתי ותשלום שכרי.
2. חתימה על נספח זה מהווה הצהרה מצידי, כי הסכמה זו ניתנה מרצוני ובהסכמתי בלבד.
3. ידוע לי כי העברת המידע מבוצעת לטובת שימוש הרשות בלבד ומידע זה לא יועבר לגורם צד שלישי לאורך תקופת זמן העסקתי ברשות או לאחריה וזאת למעט במקרים של צו משפטי מחייב.
4. ידוע לי כי אי-הסכמה למסירת המידע הנדרש בנספח זה עלולה לפגוע ביכולת הרשות לשלם את שכרי במועד, לבחון את תנאי העסקתי באופן מיטבי, ועשויה להשפיע על המשך העסקתי ברשות.