	שם המסמך: נוהל שימוש בכלי בינה מלאכותית (AI)	עמוד 1 מתוך 7
	מספר הנוהל: -	תאריך תחולה: 11/08/2025
	גרסה: **2.0**	תאריך עדכון: 25/11/2025

נוהל שימוש בכלי בינה מלאכותית (AI)

	שם המסמך : נוהל שימוש בכלי בינה מלאכותית (AI)	עמוד 2 מתוך 7
	מספר הנוהל : -	תאריך תחולה : 11/08/2025
	גרסה : **2.0**	תאריך עדכון : 25/11/2025

טבלת עדכונים:

כותב	מאשר	גרסה	תאריך אישור	מהות השינוי
ICTBIT	יגאל מרזון	1.0	11/08/2025	כתיבה
ICTBIT	יגאל מרזון	2.0	25/11/2025	עדכון ע"פ הערות מנכ"ל

	שם המסמך: נוהל שימוש בכלי בינה מלאכותית (AI)	עמוד 3 מתוך 7
	מספר הנוהל: **-**	תאריך תחולה: 11/08/2025
	גרסה: **2.0**	תאריך עדכון: 25/11/2025

תוכן עניינים:

1. כללי:..... 4

2. מטרה ויעדים:..... 4

3. מסמכים ישימים:..... 4

4. תחולה:..... 4

5. הגדרות ומושגים:..... 4

6. עקרונות השימוש:..... 4

7. פעולות מותרות:..... 5

8. פעולות אסורות:..... 5

9. דרישות אבטחה:..... 5

10. הדרכה ומודעות:..... 5

11. אחריות וסמכות:..... 6

12. הפרת הנוהל:..... 6

נספח א' – הצהרת עובד על שימוש בכלי בינה מלאכותית (AI)..... 7

	שם המסמך: נוהל שימוש בכלי בינה מלאכותית (AI)	עמוד 4 מתוך 7
	מספר הנוהל: -	תאריך תחולה: 11/08/2025
	גרסה: **2.0**	תאריך עדכון: 25/11/2025

1. כללי:

1.1. הטכנולוגיות של בינה מלאכותית (AI) הן כלי עבודה משמעותי, אך השימוש בהן עלול לחשוף את הארגון לסיכונים חמורים – דליפת מידע, פגיעה בפרטיות, פגיעה בזכויות יוצרים, ואף טעויות חמורות בתוכן המתקבל.

1.2. נוהל זה נועד להגדיר את השימוש בכלים אלו, זאת בהתאם לדרישות תקנות הגנת הפרטיות (אבטחת מידע), חוק הגנת הפרטיות, והמדיניות הארגונית (מדיניות אבטחת מידע וסייבר בשימוש בבינה מלאכותית – 006).

2. מטרה ויעדים:

2.1. להבטיח שכל שימוש ב-AI יתבצע באופן מאובטח, חוקי ואתי.

2.2. למנוע חשיפת מידע רגיש או אישי לכלי AI חיצוניים.

2.3. לייצר אחידות בנהלי העבודה ולמנוע פרשנויות שגויות לגבי מה מותר ומה אסור.

2.4. לשמור על אמון הציבור והעובדים בכך שהמידע מנוהל בצורה אחראית.

3. מסמכים ישימים:

3.1. מדיניות אבטחת מידע וסייבר בשימוש בבינה מלאכותית – 006.

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

3.3. חוק הגנת הפרטיות, התשמ"א – 1981.

4. תחולה:

4.1. הנוהל חל על:

4.1.1. כלל העובדים, יועצים, ספקים וקבלני משנה שיש להם גישה למערכות הארגון.

4.2. כל סוגי כלי ה-AI:

4.2.1. פלטפורמות ציבוריות – כגון ChatGPT, Claude, Copilot, Gemini ועוד.

4.2.2. מערכות פנימיות – שנבנו או הותאמו עבור הארגון.

4.2.3. שירותי צד שלישי – המוטמעים במערכות הארגון.

4.2.4. כלי פיתוח מבוססי AI – כולל כאלה לכתיבת קוד או לניתוח נתונים.

5. הגדרות ומושגים:

5.1. **מידע רגיש** – כל מידע אישי, רפואי, פיננסי, ביומטרי, משפטי, או מידע על מערכות הארגון וקוד מקור.

5.2. **מידע מזהה** – כל פרט שמאפשר זיהוי ישיר או עקיף של אדם (שם, מספר זהות, כתובת, טלפון וכו').

5.3. **פלטפורמות AI ציבוריות** – שירותי AI פתוחים לציבור, הפועלים בשרתים חיצוניים שאינם בשליטת הארגון.

6. עקרונות השימוש:

6.1. **אבטחה כברירת מחדל (Security by Design & Privacy by Default)** – ההגנה על המידע והפרטיות חייבת להיות משולבת בכל שלב השימוש בכלי AI.

6.2. **פיקוח אנושי** – אין להסתמך על תוצר AI ללא בדיקה ואישור אנושי.

6.3. **שקיפות** – כל שימוש בכלי AI יהיה מתועד וידוע לממונה על אבטחת המידע.

6.4. **הגבלת גישה** – רק מי שקיבל אישור רשאי להשתמש בכלי AI לצורכי עבודה.

7. פעולות מותרות:

7.1. **שימוש במידע כללי בלבד** – חיפוש והפקת מידע שאינו כולל פרטים מזהים או סודיים.

7.2. **סיוע ניסוח ותוכן** – כתיבת טקסטים, תמצות מסמכים, רעיונות לכתיבה – ללא הזנת מידע רגיש.

7.3. **שימוש בפלטפורמות מאושרות** – גרסאות עסקיות עם חשבון ארגוני בלבד.

7.4. **סיוע בפיתוח** – קבלת הצעות לקוד או פתרונות טכניים, אך רק עבור קוד שאינו מכיל לוגיקה עסקית רגישה או פרטי מערכת פנימית.

7.5. **בדיקות רעיוניות** – שימוש ב-AI לבדיקת רעיונות, מיתוג, חוויית משתמש – אך לא לקבלת החלטות סופיות ללא בקרה.

8. פעולות אסורות:

8.1. **הזנת מידע רגיש** – פרטים אישיים, מידע רפואי, פיננסי, משפטי, נתוני אבטחה, סיסמאות, מפתחות API, כתובות IP פנימיות.

8.2. **שימוש בגרסאות חינמיות/פרטיות** – כל שימוש מקצועי יתבצע רק בגרסאות מאושרות ומאובטחות.

8.3. **העלאת קבצים או מסמכים** – אלא אם קיבלו אישור מיוחד ועברו תהליך ניקוי מידע מזהה ומטא-דאטה.

8.4. **הפקת תוכן מטעה או פוגעני** – אסור לייצר או לשתף תוכן שיש בו הטעיה, פגיעה באדם, או אי עמידה בערכי הארגון.

8.5. **עקיפת מנגנוני אבטחה** – אין לנסות לשנות או לעקוף הגדרות אבטחה של הכלי או המערכת.

9. דרישות אבטחה:

9.1. התחברות עם אימות דו-שלבי (2FA).

9.2. ביטול שמירת היסטוריית השיחות ואיסור שימוש בתוכן לשיפור המודלים.

9.3. שימוש בחיבורים מוצפנים (HTTPS/TLS) בלבד.

9.4. שמירת תיעוד לשימושים שאושרו – למעקב ובקרה.

10. הדרכה ומודעות:

כחלק מדרישות תקנות הגנת הפרטיות (אבטחת מידע) והמדיניות הארגונית, כל עובד בעל גישה לכלי AI מחויב לעבור הדרכה מסודרת לפני קבלת ההרשאה.

10.1. ההדרכה תכלול:

	שם המסמך: נוהל שימוש בכלי בינה מלאכותית (AI)	עמוד 6 מתוך 7
	מספר הנוהל: **-**	תאריך תחולה: 11/08/2025
	גרסה: **2.0**	תאריך עדכון: 25/11/2025

10.1.1. **היכרות עם הסיכונים** – הסבר על סיכוני פרטיות, אבטחת מידע, ודוגמאות למקרי דליפה או שימוש לרעה בכלי AI.

10.1.2. **מה מותר ומה אסור** – פירוט גבולות השימוש לפי סעיף 7 ו-8 בנוהל, כולל דוגמאות מהשטח.

10.1.3. **הנחיות טכניות** – איך להתחבר בצורה מאובטחת, איך להשבית שמירת היסטוריה, ואיך לוודא שמידע לא משמש לאימון המודלים.

10.1.4. **זיהוי ודיווח אירועים** – איך לזהות חשש לדליפת מידע או שימוש לא תקין, ולאן לפנות במקרה של חשד.

10.1.5. **תרחישי סימולציה** – תרגול מצבים אמיתיים (למשל, עובד שנדרש להזין נתונים לקבלת דוח, או מפתח שמעוניין בקוד ל"דיבוג" – זו טעות במילה?).

10.2. חובת ריענון:

10.2.1. תתקיים הדרכת ריענון ומודעות שנתית לכל המשתמשים המאושרים.

10.2.2. במקרה של שינוי מהותי במדיניות, בתקנות, או במערכות ה-AI – תינתן הדרכה ייעודית נוספת.

11. אחריות וסמכות:

11.1. **מנהל אבטחת מידע וסייבר** – מאשר שימושים חריגים, מפקח על עמידה בנוהל, ומטפל באירועי אבטחה.

11.2. **מנהלים ישירים** – מוודאים שהעובדים מבינים ופועלים לפי הנוהל.

11.3. **העובדים** – מחויבים להכיר את הנוהל, להשתתף בהדרכות, ולדווח מיידית על חשד לדליפת מידע.

12. הפרת הנוהל:

12.1. הפרת הנוהל עלולה להוות:

12.1.1. עבירת משמעת בארגון.

12.1.2. עבירה על חוק הגנת הפרטיות ותקנות אבטחת המידע.

12.1.3. עילה לנקיטת צעדים משפטיים ומשמעתיים.