מדיניות שימוש אחראי בבינה מלאכותית

קבוצת ASTER

מסמך מדיניות · CAIO · יולי 2026

מדיניות קבוצת ASTER לשימוש אחראי בבינה מלאכותית

AI Usage Policy — AI Service Co-Pilot

גרסה 1.0 · יולי 2026 · מאושר: ועדת היגוי AI וההנהלה הבכירה · בעל המסמך: CAIO

בקרת מסמך. כניסה לתוקף: מועד העלייה לאוויר (תחילת הפיילוט), וממשיכה כמדיניות קבועה בפרודקשן · **תדירות תיקוף: לפחות אחת לשנה + אחרי שינוי רגולטורי/אירוע מהותי** (ISO 27001 / DORA / תקנות אבטחת מידע). *אירוע מהותי = אירוע AI בחומרה משמעותית/חמורה, הפרת אבטחה/פרטיות, או שינוי רגולטורי משמעותי.* · הפצה: הנהלה, ועדת היגוי AI, מנהלי מחלקות · יומן שינויים: נספח ד'.

יחס למדיניות קיימת. מדיניות זו **משלימה ואינה גוברת** על מדיניות הפרטיות, אבטחת המידע, ה-HR והרכש הקיימות; בסתירה — הדין והמדיניות המחמירה גוברים.

מחוץ לתחום. שימושי AI שאינם בתהליכי שירות הלקוחות אינם מכוסים בשלב זה ויידונו בנפרד.

חלק 1 — תשתית המדיניות, הגדרות ועקרונות יסוד

1.1 מטרה. מדיניות זו קובעת את הכללים לשימוש אחראי, מבוקר וחוקי בבינה מלאכותית בקבוצת ASTER, החל מפרויקט ה-AI Service Co-Pilot. מטרתה לאפשר מהירות עסקית תוך שליטה מלאה בסיכון המשפטי, הרגולטורי, הפרטי והתפעולי.

1.2 תחולה. המדיניות חלה על כל עובדי הקבוצה, נציגי השירות, צוות תפעול ה-AI, וכל ספק או צד ג' המעורב במערכות AI בתהליכי השירות. שלב הפיילוט מוגבל למוקד שירות יחיד ולמידע סטטי בלבד.

1.3 הגדרות.

- **מערכת AI** — מערכת מבוססת-מכונה הפועלת בדרגות אוטונומיה ומייצרת פלטים (תחזיות, תוכן, המלצות) המשפיעים על סביבתה (הגדרת הנציבות האירופית).
- **Co-Pilot** — כלי סיוע לנציג השירות בזמן אמת. **אינו מחליף** את שיקול הדעת האנושי.
- **מידע סטטי** — "מידע ברזל" שאינו משתנה ואינו מבוסס שיקול דעת (עמלות, מדיניות, שעות פעילות, נהלים).
- **מידע דינמי** — זכאויות, החזרים, סטטוס תביעה, מידע פרסונלי על לקוח.
- **שלב סטטי (פיילוט)** — ההפעלה הראשונית, המטפלת במידע סטטי/ציבורי בלבד. **שלב דינמי** — הרחבה מאוחרת שבה המערכת ניגשת למידע אישי של הלקוח (זכאות/סטטוס תביעה), בכפוף לאישורי FRIA/DPIA וועדת היגוי AI.
- **ועדת היגוי AI** — הגוף המפקח והמאשר הבכיר.
- **צוות תפעול ה-AI** — היחידה המקצועית תחת ה-CAIO המבצעת: בונה, מריצה ומנטרת את המערכת.
- **בעל נוהל (Owner)** — הגורם ה-Accountable לתוכן נוהל, לעדכונו ולאכיפתו.
- **סמכות פרטיות (DPO)** — הגורם המכריע במרכיבי המידע האישי בנוהל שבעליו אינו ה-DPO.
- **Deployer / Provider** — מפעיל מערכת מול יצרן המערכת. **Deployer** = ASTER.
- **RAG** — אחזור מידע ממאגר מאומת סגור. **מיסוך (Anonymization)** — הסרת פרטים מזהים לפני עיבוד חיצוני. **Human-in-the-loop** — אישור אנושי לפני שימוש בפלט.

1.4 עקרונות יסוד.

1. **סיוע ולא תחליף** — הנציג הוא מקבל ההחלטה ובעל האחריות לתשובה.
2. **אדם בלולאה** — אוטומציה אינה מחליפה שיקול דעת אנושי בנקודות רגישות.
3. **פרטיות ואבטחה מובנות** (Privacy & Security by Design).
4. **שקיפות והסברתיות** — גילוי שמדובר ב-AI, וכל פלט מציין את מקורו.
5. **הוגנות ומניעת הטיה** — איסור אפליה אלגוריתמית.
6. **אחריותיות** — הארגון אינו מתחמק מאחריות לתוצאות המערכת.
7. **מידתיות** — לא מפעילים AI היכן שפתרון דטרמיניסטי מספיק.

כללי הברזל (Non-Negotiable). שבעה כללים שאין לחרוג מהם בשום שלב:

1. **הנציג מכריע** — המערכת אינה מחליפה שיקול דעת אנושי.

2. **אין התחייבות כספית אוטונומית** (החזר/ביטול/פיצוי) — חסום ומוסלם למנהל.

3. **אין PII לספק ללא מיסוך.**

4. **כל פלט הוא טיוטה עם ציון מקור, הנבדקת ע"י נציג** — תשובה ללא מקור נחסמת.

5. **אין שימוש ב-AI לא מאושר (Shadow AI).**

6. **אין מדידה, דירוג או משמעת של עובדים** באמצעות המערכת.

7. **מידע רגיש — של לקוח או של הארגון — אינו נכנס למערכת ואינו נפלט ממנה.**

1.5 גישת סיכון. סיווג כל שימוש לפי פירמידת EU AI Act (אסור / גבוה / מוגבל / מינימלי) וטבלת החומרה הארגונית (נספח ג').

1.6 גבולות הפיילוט — מה לא עולה לאוויר בשלב א'. אינם נכללים בפיילוט: פניות דינמיות (זכאות/החזר/תביעה), שליחת PII לספק, הקמת סוכנים ע"י נציגים, יכולת KYC/OCR/Liveness, וכל פעולת כתיבה אוטונומית. הרחבה אליהם מותנית באישור נפרד של ועדת היגוי AI.

1.7 תלות ביישום. סעיפי מדיניות זו המתבססים על בקרות טכניות (מיסוך, RBAC, Prompt Filter, DLP) ועל הנהלים (נ-01..נ-05) מותנים ב**יישומם ואימותם בפועל כתנאי סף לעלייה לאוויר** — המדיניות אינה מסמך הצהרתי אלא כללים אכיפים.

חלק 2 — ממשל תאגידי (Governance)

2.1 ועדת היגוי AI. יו"ר: מנהל הסיכונים הראשי (CRO). חברים: CISO, DPO, CAIO (Executive Sponsor), היועמ"ש, קצין הציות, מנהלת השירות, מנהל טכנולוגיות המידע. משתתפים לפי עניין: CFO (תקציב ו-ROI), משאבי אנוש (השפעה על עובדים). ה-CAIO מנוע מהשתתפות בדיון ובהצבעה על עליית פרויקט לאוויר; זכות עצירה (Veto) ל-CISO ול-DPO בנושאי אבטחה ופרטיות. סמכות: לאשר, להגביל או **לעצור** פרויקטי AI, לאשר חריגים ולהכריע מקרי גבול רגולטוריים. מעוגנת בצ'ארטר (Charter) רשמי. מתכנסת חודשית בפיילוט, רבעונית לאחריה, ובכל אירוע מהותי.

2.2 זכות עצירה (Veto). ל-CISO ול-DPO זכות עצירה על השלב הדינמי; כל אחד רשאי לעכב עלייה לאוויר עד לסגירת סיכון פתוח.

2.3 צוות תפעול ה-AI. מבצע ומריץ את המערכת ומדווח לוועדת היגוי AI. כלל: **הוועדה מפקחת ומאשרת · צוות התפעול מבצע**.

2.4 חלוקת אחריות (RACI). ראה נספח ב'. עקרון: ל-CAIO אחריות תיאום כוללת; לכל שומר סף תחום הכרעה מוגדר.

2.5 פיקוח דירקטוריון. דיווח תקופתי לדירקטוריון על סטטוס, סיכונים ואירועים, על בסיס שמונה שאלות הפיקוח (מדיניות מאושרת, אחריות, שימושים קריטיים, נאותות ספקים, סיכון תקינות, תגובת אירוע, דיווח, אכיפה).

2.6 יישוב מחלוקות. בהתנגשות בין מהירות עסקית לסיכון — ההכרעה בוועדת היגוי AI; בנושאי פרטיות/אבטחה גוברת זכות ה-Veto.

חלק 3 — תהליכי אישור ובחינה (Intake & Approval)

3.1 שאלון הערכת סיכון (AI Intake Form). כל כלי או שימוש AI חדש נבחן בשאלון הערכת סיכון הבוחן ארבעה היבטים: (1) **פרטי היוזמה** — זהות ה-Business Owner, הצורך העסקי ומשתמשי הקצה; (2) **טכנולוגיה** — סוג המערכת (גנרטיבי/אחזור), אופן ההתקשרות (SaaS/API/On-Prem) ותדירות עדכון המודל; (3) **נתונים ופרטיות** — היקף עיבוד מידע אישי, יציאת מידע מגבולות הארגון וחשיפת סודות מסחריים; (4) **השפעה וסיכון** — קיום החלטות אוטומטיות, פוטנציאל הנזק והצורך בפיקוח אנושי.

3.2 שער הקמת סוכנים. אין הקמת סוכנים ע"י נציגים — קיים רק ה-Co-Pilot המרכזי המאושר. כל בקשה עוברת שער חוסם הבוחן: קיום כלי חלופי ב-Whitelist, פגיעה באחידות המידע, רמת הסיכון, והצורך האמיתי בסוכן. ראה נ-04.

3.3 מחזור חיים (Lifecycle). יזום ותכנון (Secure by Design) ← פיתוח (Dev/Stage, Whitelist) ← בדיקות QA/Sec (Bias testing, red-teaming, לוגים) ← אישור והפצה (אישור ועדה + סקירה משפטית).

3.4 רשימת כלים מאושרים (Whitelist). שימוש מותר אך ורק בכלים שאושרו ונרשמו ב-AI Inventory. ראה נ-04.

3.5 בדיקות הוגנות. לפני עלייה ובאופן תקופתי — בדיקות הטיה על פני קבוצות לקוחות, תיעוד התוצאות והצגתן לוועדת היגוי AI.

3.6 ניהול שינויי מודל/גרסה. עדכון מהותי של המודל או של גרסת הספק מחייב **בדיקה מחדש** (איכות, הטיה, רגרסיה) ואישור לפני הטמעה — שינוי במודל עלול לשנות התנהגות גם ללא שינוי בשימוש.

חלק 4 — הוראות שימוש ופרומפטים

4.1 מסנן AI / לא-AI. קודם נבחן אם נדרש (1) :AI דטרמיניסטי/ייעודי (לא AI, מחוץ להגדרה); (2) אחזור/RAG (סיכון נמוך); (3) גנרטיבי (סיכון hallucination, נדרש HITL). **מידע ציבורי בסיסי — שעות פעילות, מספר טלפון של שירות הלקוחות וכתובת — אינו נכנס ל-RAG ואינו מאונדקס**; הוא מוצג כתשובה גנרית/דטרמיניסטית קבועה (דרגה 1), שכן זהו מידע פומבי בסיכון הזיה נמוך. **תנאי שירות ופוליסה כללית** (תנאי ביטול, אחריות) מטופלים כמידע סטטי בדרגה 2 (RAG ממאגר מאומת + בדיקת נציג); תנאי פוליסה ספציפיים ללקוח הם דינמיים.

4.2 גבולות גזרה. לכל שימוש מוגדר: מה אסור למערכת לעשות, באילו הקשרים אסור להשתמש בה, אילו החלטות אסור לקבל על בסיס הפלט, ואילו אוכלוסיות אסור להחיל עליה.

4.3 מה מותר ואסור להזין. אסור להדביק רשומת לקוח מלאה; אסור להזין prompt המכוון לפעולה כלפי פרט מזוהה; אסור להזין מידע רגיש (בריאותי, פיננסי, שכר/הערכות עובדים).

4.4 קווים אדומים (שימושים אסורים). המערכת חסומה מ: (1) התחייבות/החזר/ביטול/פיצוי אוטונומי; (2) שליחת PII לספק ללא מיסוך; (3) מדידה/דירוג עובדים; (4) יצירת מצג/(5) ;Deepfake עיבוד קטגוריה מיוחדת ללא בסיס חוקי; (6) החלטה מול לקוח ללא אדם בלולאה מעל רמת "מוגבל"; (7) אימון מודל הספק על הדאטה שלנו.

4.5 שימוש בפלט. הפלט הוא **טיוטה בלבד**, מסומן כהצעת AI, מציין את מקורו, ונבדק ע"י הנציג לפני שליחה. בסיכון גבוה — מוצג גם המקור המילולי לצד הטיוטה.

4.6 סינון והסלמה. Prompt Filter בזמן אמת חוסם מילים רגישות ("מתחייבים להחזר", "פיצוי") ומחייב אישור מנהל. נוהל תשובה שגויה והסלמה — ראה נ-01.

4.7 עמידה בהוראות היצרן. השימוש במערכת יתבצע בהתאם ל-Instructions for Use של הספק (EU AI Act סע' 26(1)); חריגה מהן אסורה.

4.8 אותות אמינות וניתוב. מהימנות תשובה אינה נמדדת לפי "ביטחון" שהמודל מדווח על עצמו, אלא לפי אותות נמדדים: ציון האחזור/הדמיון ב-RAG, בדיקת עיגון (האם התשובה מופיעה במקור שנשלף), עקביות בין הרצות, והסתברויות הפלט. אות אמינות נמוך מפעיל **ניתוב אוטומטי לבדיקה אנושית או ל-Fallback**. האותות מנוטרים ע"י צוות תפעול ה-AI (ראה 7.3).

4.9 חיווי איכות ופידבק נציג (בפיתוח). בממשק ה-Co-Pilot ישולב **כפתור חיווי** לדירוג איכות תשובת הבוט, לצד **שדה הערות חופשי**. הפידבק מוזן למדדי הבקרה (override/correction rate — ראה 7.3) ומשמש לבקרת איכות, לתיקון בסיס הידע ולאימון המערכת. הדיווח הוא חלק מתפקיד הנציג ו**אינו מדד לדירוגו** (ראה נ-01 ס' 10). **שדה ההערות לא יכיל מידע אישי או רגיש של לקוח** (בהלימה לס' 4.3 ולכללי הברזל).

חלק 5 — ספקי AI וצדדים שלישיים

5.1 בדיקת נאותות (Due Diligence). דרישת הסמכות ISO 27001 ו-SOC 2 Type II, עמידה מהותית ב-NIST AI RMF, וחתימה/עמידה ב-GPAI Code of Practice (שקיפות + זכויות יוצרים). מעורבות CISO/DPO מוקדם. בחינת הספק נערכת מחדש **תקופתית (אחת לשנה) ובכל שינוי מהותי**. התקנים ISO/NIST/GPAI הם **תקנים בינלאומיים וולונטריים** שאנו מאמצים כ-best practice ודורשים מהספק — אינם דין זר החל על ASTER; הרגולציה **המחייבת** היא האירופית (EU) והישראלית.

5.2 סעיפי חובה בחוזה. No-Training (איסור אימון על קלט/פלט של הלקוח); **Super-Cap** לתביעות קניין רוחני ופרטיות; שיפוי עם החרגות מוגדרות; בעלות ASTER על התוצרים; זכויות ביקורת (Audit) ודרישות DORA לספק ICT ; יצוא מידע ומחיקה בסיום.

5.3 דאטה "מלוכלך". הספק יגביל אחריות אם המודל אומן על מידע לא מורשה. תגובת ASTER: העדפת מודלים נקיים/מורשים, Super-Cap, סינון תוכן בשכבת המוצר, ובהירות נטל הבדיקה.

5.4 מודל ההתקשרות. שלב סטטי — SaaS/API בענן ציבורי (מידע ברזל בלבד); שלב דינמי — פריסה פרטית (VPC On-Prem/) או API תחת שכבת מיסוך והסמכות. אם ספק אינו מסכים ל-No-Training — ספק Enterprise חלופי או פריסה פרטית (קוד-פתוח פנימי הוא נקודה להתייעצות והכרעת החברה, לא ברירת מחדל).

5.5 יציאה ותלות. מניעת Vendor Lock-in, אסטרטגיית יציאה, ו-data portability. הכרעה: ללא No-Training, Super-Cap ויציאה — לא חותמים. ראה נ-03.

5.6 קבלני משנה (Sub-processors). על הספק לגלות ולאשר מראש שימוש בקבלני משנה ובמודלי צד ג'; מודלים ממקורות בסיכון גבוה (למשל מסין) טעונים בחינה מיוחדת.

חלק 6 — פרטיות ואבטחת מידע

6.1 מזעור ומיסוך. עיבוד מידע מינימלי הכרחי. שכבת מיסוך פנימית (Anonymization Layer): הספק מקבל קוד אנונימי בלבד ולעולם אינו רואה PII.

6.2 הרשאות (RBAC). עקרון least-privilege ו-need-to-know; לכל תפקיד פרופיל מוגדר (צפייה/עריכה/גישה לקבצים). מפת "אין-גישה": חסום לחלוטין — כתיבה ל-CRM, מערכות HR ונתוני עובדים, מערכות תשלום (PCI), דאטה של חברות בנות, מנועי החלטת תביעות. ראה נ-02.

6.3 הגנת זליגה. שכבת DLP בזמן אמת (חוסמת egress ו-jailbreak), הגנה מפני prompt injection, סביבה סגורה (Sandbox), No-Training + Zero Data Retention, וניטרול connectors/agents כברירת מחדל.

6.4 לוגים ושמירה. תיעוד מלא (prompt + מקור + פלט + החלטת נציג). שמירת לוגים ≤6 חודשים (חובת Deployer), וארוך יותר לפי DORA ותקנות אבטחת מידע; לרשומות פיננסיות — בהתאם לחובות השמירה הסקטוריאליות. מדיניות שמירה ומחיקה מוגדרת.

6.5 תסקירי השפעה. DPIA (זרימות מידע, בסיס חוקי, מזעור, סיכוני פרטיות) ו-FRIA (זכויות יסוד מושפעות, חומרה, הפחתה, פיקוח) נדרשים ל**שלב הדינמי** — השלב שבו ה-Co-Pilot מתחיל לטפל בפניות דינמיות (זכאות, החזר, סטטוס תביעה) ולגשת למידע אישי של הלקוח, בשונה מהפיילוט הסטטי. חובה לפי EU AI Act למפעיל שירות פיננסי/ביטוחי. **אישור ה-FRIA וה-DPIA ע"י DPO וועדת היגוי AI הוא תנאי סף להפעלת הטיפול בפניות דינמיות בפרודקשן.**

6.6 מניעת פליטת מידע רגיש. המערכת לעולם אינה שולפת/פולטת מידע רגיש — צד לקוח (בריאותי, אשראי, קטגוריות מיוחדות, מידע על לקוחות אחרים) וצד חברה (שכר/הערכות עובדים, סודות מסחריים, מסמכים בהליך). אכיפה: הדרה מהאינדוקס + DLP + allow-list. **תנאי לאכיפה: סיווג מקורות המידע (רגיש/לא-רגיש) לפני האינדוקס** — ללא סיווג, ההדרה אינה אמינה.

6.7 בסיס חוקי לעיבוד. עיבוד מידע אישי מחייב בסיס חוקי מוגדר (הסכמה / אינטרס לגיטימי / חוזה) והסכם עיבוד נתונים (DPA) עם הספק.

6.8 זכויות נושא מידע. בקשות נושא מידע (עיון, תיקון, מחיקה, והתנגדות להחלטה אוטומטית לפי סע' 22 GDPR) יטופלו גם כאשר מעורב AI. המערכת אינה מקבלת החלטה אוטומטית בעלת השפעה משפטית/משמעותית ללא אדם בלולאה.

6.9 העברות בין-לאומיות. העברת מידע מחוץ לאיחוד/ישראל מחייבת מנגנון חוקי (SCCs / החלטת נאותות); עדיפות לאחסון בתחום השיפוט הרלוונטי.

6.10 סימון תוכן AI. סיכומי שיחה ותכנים שנוצרו ע"י המערכת מתויגים כ-AI-generated ברשומת ה-CRM. השמירה ל-CRM נעשית בידי הנציג או המערכת התפעולית, לא בידי הבוט — שאין לו הרשאת כתיבה (ס' 6.2).

חלק 7 — הטמעה, דיווח ואכיפה

7.1 הדרכה והטמעה. הדרכת נציגים (Onboarding, Role-based, עדכונים שוטפים) על גבולות המערכת; דגש על **Automation Bias** — אין להסתמך על הפלט "בעיניים עצומות", ומתי חובה לסטות מהמלצת המערכת. ההדרכה מקיימת גם את **חובת אוריינות ה-AI (EU AI Act סע' 4)** — הבטחת רמת הבנה מספקת אצל המשתמשים והמפעילים. ראה נ-05.

7.2 יידוע ועד העובדים. חובה חוקית לפי **EU AI Act סע' 26(7)** ליידע את נציגות העובדים לפני הפעלת מערכת high-risk; בישראל חובת היוועצות בדיני עבודה קיבוציים. מחויבות אי-פיטורים בתקופת הפיילוט + תוכנית הסבה.

7.3 ניטור ובקרה. ניטור לוגים, שיעור override/correction rate, חיווי הנציג (ראה 4.9), וביקורת מדגמית על אישורים. מדדי הצלחה (KPIs) ב-4 קטגוריות: ערך עסקי, אימוץ, איכות, ובקרת סיכון — כל אחד עם baseline /יעד/לו"ז. **מדד ה-AHT לא ייקבע באופן שמעניש בדיקה אנושית קפדנית**, כדי למנוע אישור אוטומטי ("חותמת גומי"); ה-override/correction rate משמש כאיתות איכות הבדיקה. ראה נ-04.

7.4 דיווח אירועים. סיווג חומרה (קל/משמעותי/חמור), לוחות זמני דיווח לשלושה משטרים (EU AI Act סע' 26(5)/73 , תיקון 13, DORA), יכולת **Kill Switch**, וקישור ל-FRIA. **בהפרה הפוגעת בנושאי מידע — יידוע הנפגעים והרשות להגנת הפרטיות בהתאם לתיקון 13 ול-GDPR (דיווח לרשות תוך 72 שעות לפי GDPR).** ראה נ-02.

7.5 אכיפה. הפרת המדיניות (למשל שימוש ב-Shadow AI לא מאושר) כפופה לסנקציות משמעתיות בהתאם לחומרה.

7.6 עדכון תקופתי. המדיניות **והנהלים** (נ-01..נ-05) נבחנים ומתעדכנים **לפחות אחת לשנה, ובכל שינוי רגולטורי או אירוע מהותי** — בהלימה לחובת הסקירה בדין **האירופי** (DORA שנתי, ISO 27001 ס' 9.3) וב**ישראלי** (תקנות אבטחת מידע 2017 — סקר/הדרכה תקופתיים). החובה חלה **גם על מדיניויות ונהלים קיימים הכוללים היבטי AI** (ניהול סיכונים, אבטחה, פרטיות) — לא רק על מסמכי ה-AI. Lessons Learned שנתי. שינוי ייעוד של רכיב סטטי לשימוש דינמי מחייב סיווג רגולטורי מחדש.

7.7 המשכיות עסקית. בכשל או אי-זמינות של ה-Co-Pilot, הנציג ממשיך לעבוד ללא המערכת (סיוע ולא תלות); ניתוב אוטומטי לחיפוש פנימי פשוט מונע חוויית ניתוק.

7.8 נגישות. ממשק הנציג ותכני השירות יעמדו בדרישות הנגישות הרלוונטיות (תקנות נגישות השירות).

נספח א' — מפת נהלים

נוהל	תחום	בעלים
נ-01	שירות ותפעול נציג: שימוש · הסלמה · תשובה שגויה	מנהלת שירות + צוות תפעול ה-AI
נ-02	אבטחה ופרטיות: הרשאות/RBAC · מיסוך/אינדוקס · דיווח אירועים	DPO · CISO (Owner) (סמכות פרטיות)
נ-03	התקשרות ספקי AI: due diligence · חוזה · exit	רכש + יועמ"ש
נ-04	ממשל ובקרת AI: אישור כלי/סוכן · ניטור/QA	ועדת היגוי AI (מאשרת) · צוות תפעול ה-AI (מבצע)
נ-05	הון אנושי: הדרכה והטמעה · automation bias	HR

סטטוס נהלים: נ-01 הופק. נ-02..נ-05 **בפיתוח** (מתוכננים) — ההפניות אליהם משקפות את מבנה היעד ואינן טענה למסמך קיים.

נספח ב' — מטריצת אחריות (RACI) — תמצית

נושא	מאשר	מייעץ	מבצע	Veto
עלייה לפיילוט	ועדת היגוי AI	יועמ"ש/CFO	צוות תפעול ה-AI	CISO/DPO
פרטיות ומיסוך	DPO	CISO	צוות תפעול ה-AI	DPO
אבטחה והרשאות	CISO	DPO	צוות תפעול ה-AI	CISO
חוזה ספק	יועמ"ש	CISO/DPO	רכש	—
ROI ומדדים	CFO	מנהלת שירות	CAIO	—

נספח ג' — טבלת חומרה / פירמידת סיכון

פירמידת EU AI Act: □ אסור · □ גבוה · □ מוגבל · □ מינימלי.

חומרה	דוגמה ב-Co-Pilot	אינדיקטור	אחראי	מיתון
□ קריטי	מצג כספי מחייב ללקוח (החזר/ביטול)	תלונה · פער AI↔מדיניות	יועמ"ש + CAIO	Hard Block · human review · incident
□ גבוה	PII לספק ללא מיסוך	DLP / anomaly	DPO + CISO	containment · הערכת חובת דיווח
□ גבוה	תשובה דינמית שגויה שהנציג מעביר	feedback / inconsistency	מנהלת שירות + CAIO	fallback אנושי · תיקון מקור
□ בינוני	Shadow AI לא מאושר	accounts לא מזוהים	HR + CAIO	allow-list · הכשרה

חומרה	דוגמה ב-Co-Pilot	אינדיקטור	אחראי	מיתון
□ בינוני	תלות בספק / חוזה חלש	אין export	רכש + legal	renegotiation · exit
□ נמוך	שליפת מידע סטטי	low risk · אין PII	יחידת שירות	בדיקת נציג · no sensitive data

נספח ד' — יומן שינויים

גרסה	תאריך	שינוי
1.0	יולי 2026	גרסה ראשונה — אושרה בוועדת היגוי AI