בינה מלאכותית בגובה העיניים בע"מ
EYE LEVEL AI LTD · ח.פ. 517180931

חיבור העוזר האישי של מועדון AI פרקטי אל Microsoft 365

מסמך הסבר עבור מחלקת טכנולוגיות המידע בארגון

על מה המסמך הזה

העוזר האישי של **מועדון AI פרקטי** יכול להתחבר ליומן Outlook, לדואר, לאנשי הקשר, למשימות, לקבצים ב-OneDrive ול-Microsoft Teams של המשתמש, כדי לנהל עבורו את יומו: לקבוע פגישות, לנסח ולשלוח מיילים, לאתר אנשי קשר, לנהל משימות, למצוא ולערוך קבצים וגיליונות Excel, ולקרוא ולשלוח הודעות ב-Teams.

בארגונים רבים חיבור כזה מחייב **אישור חד-פעמי של מנהל מערכת**. המסמך מסביר מה האפליקציה מבקשת, מה היא רואה ומה היא אינה רואה, וכיצד לאשר או לבטל את החיבור.

חלק א': לעובד או לעובדת שמבקשים להתחבר

אם ניסיתם לחבר את חשבון Microsoft הארגוני שלכם ונתקלתם בחסימה או בהודעת שגיאה, דעו שזה תקין ואין זו תקלה. ארגונים מגדירים כברירת מחדל שרק מנהל מערכת מאשר חיבור של יישומים חיצוניים.

1. **העבירו את המסמך הזה למנהל המערכת או לאיש ה-IT בארגון.** כל המידע שהוא צריך נמצא בחלק ב'.
2. **המתינו לאישור.** הפעולה אורכת דקות ספורות ומבוצעת פעם אחת עבור כל הארגון.
3. **התחברו שוב** מתוך העוזר האישי. לאחר האישור החיבור יעבור ללא חסימה וללא בקשת הרשאה נוספת.

לפני שתעבירו, דבר אחד שכדאי לדעת

במסך האישור תופיע הודעה שהאפליקציה "**לא מאומתת**". זהו סימון טכני של Microsoft שמשמעותו שהליך רישום היצרן שלנו מול Microsoft טרם הושלם. **אין זו אזהרת אבטחה ואין זה ממצא על האפליקציה.** ההסבר המלא מופיע בחלק ב' והוא נכתב במיוחד עבור איש ה-IT.

חלק ב': למנהל המערכת בארגון

1. פרטי היישום והיצרן

שם היישום	Practice AI Assistant
מזהה יישום (Client ID)	6db47650-1fe7-4b0a-b893-a802c925d272
דומיין היצרן	practice-ai.co.il
שם היצרן	בינה מלאכותית בגובה העיניים בע"מ · EYE LEVEL AI LTD
מספר חברה	ח.פ. 517180931 · חברה פעילה הרשומה ברשם החברות בישראל
סוג ההרשאות	**Delegated** בלבד (ראו סעיף 4)

מומלץ לאמת את מזהה היישום מול מה שמוצג במסך האישור לפני מתן ההרשאה.

2. מה היישום עושה

מועדון AI פרקטי מפעיל עוזר אישי מבוסס בינה מלאכותית עבור משתמשים רשומים. לאחר שמשתמש מחבר את חשבון Microsoft שלו, העוזר יכול לבצע עבורו פעולות **בחשבונו האישי בלבד**: לקרוא ולקבוע אירועים ביומן, לאתר ולנסח מיילים ולשלוח אותם בשמו, לאתר ולעדכן אנשי קשר, לנהל משימות ב-Microsoft To Do, למצוא קבצים ב-OneDrive ולעבוד עם גיליונות Excel, ולקרוא ולשלוח הודעות ב-Microsoft Teams.

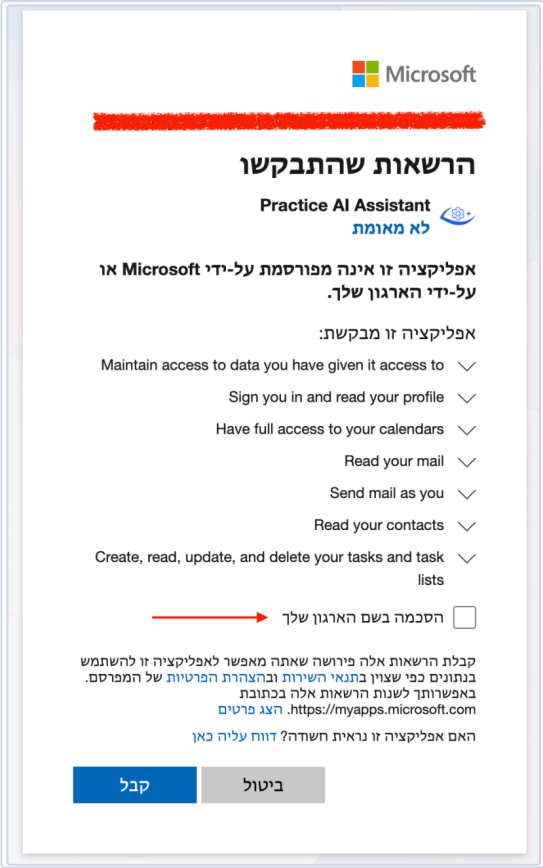
היקף הגישה נגזר מההרשאות של המשתמש עצמו. כל קריאה ל-Microsoft Graph נעשית באסימון המשתמש המחובר, ולכן העוזר רואה בדיוק את מה שאותו עובד רואה בדפדפן — לא יותר. ערוץ שאין לו גישה אליו, קובץ שלא שותף איתו וצ'אט שאינו משתתף בו אינם נגישים לעוזר.

כל פעולה נעשית ביוזמת המשתמש ובהקשר של בקשה שהוא ניסח. היישום אינו פועל באופן עצמאי ברקע על תיבות דואר של משתמשים אחרים.

3. ההודעה "לא מאומת": מה משמעותה

במסך האישור תוצג ליד שם היישום התווית "**לא מאומת**", ולצידה הטקסט:

> **"אפליקציה זו אינה מפורסמת על-ידי Microsoft או על-ידי הארגון שלך."**



מסך האישור כפי שהוא מוצג בפועל, עם התווית "לא מאומת" ועם תיבת הסימון "הסכמה בשם הארגון שלך" (מסומנת בחץ). **רשימת ההרשאות בצילום היא לדוגמה בלבד** — הרשימה המלאה והעדכנית מופיעה בטבלה שבסעיף 4. בפורטל המוגדר באנגלית יופיע אותו מסך עצמו, עם התווית `Unverified` והטקסט `This app is not published by Microsoft or your organization`.

משמעות התווית

התווית "יצרן מאומת" מוענקת על ידי Microsoft ליישומים שהיצרן שלהם רשום בתוכנית השותפים שלה, *Microsoft AI Cloud Partner Program*. **מדובר בהליך רישום מנהלי של החברה מול Microsoft.**

ההליך נמצא בעיצומו ואורך זמן. עם השלמתו התווית תוסר מאליה, ללא צורך בפעולה כלשהי מצד הארגון וללא השפעה על חיבורים שכבר אושרו.

מה התווית אינה מעידה עליו

- **אין זו אזהרת אבטחה** ואין זה ממצא של סריקה או של בדיקת קוד.
- **Microsoft לא בחנה את היישום ולא מצאה בו ליקוי.** התווית מציינת היעדר הליך רישום מנהלי שהושלם, ותו לא.
- **אין לכך כל השפעה על ההרשאות** שהיישום מבקש או על היקף הגישה שלו. ההרשאות המפורטות בסעיף 4 הן מלוא מה שהיישום יכול לבצע, עם התג או בלעדיו.

4. ההרשאות המבוקשות

כל ההרשאות הן **Delegated** מול Microsoft Graph. שימו לב שבמסך האישור שמות ההרשאות מוצגים באנגלית גם בממשק בעברית. להלן התרגום המלא:

שם ההרשאה	כפי שמוצג במסך	המשמעות בפועל
User.Read	Sign in and read user profile	התחברות וקריאת פרופיל בסיסי: שם וכתובת דואר אלקטרוני
offline_access	Maintain access to data you have given it access to	שמירת החיבור פעיל, כדי שהמשתמש לא יידרש להתחבר מחדש בכל שימוש
Calendars.ReadWrite	Have full access to user calendars	יומן Outlook של המשתמש: קריאה, יצירה, עריכה ומחיקה של אירועים
Mail.Read	Read user mail	**קריאה בלבד** של תיבת הדואר של המשתמש
Mail.Send	Send mail as a user	שליחת הודעות דואר בשם המשתמש
Mail.ReadWrite	Read and write access to user mail	ארכוב, סימון כנקרא, העברה בין תיקיות, כתיבת טיוטות ומחיקה של הודעות בתיבת המשתמש
Contacts.ReadWrite	Have full access to user contacts	אנשי הקשר של המשתמש: קריאה, יצירה ועדכון
People.Read	Read users' relevant people lists	**קריאה בלבד** של אנשים שהמשתמש עובד איתם, לצורך השלמת כתובת לפי שם
Tasks.ReadWrite	Create, read, update, and delete user's tasks and task lists	ניהול משימות ורשימות משימות ב-Microsoft To Do
Files.ReadWrite.All	Have full access to all files user can access	קבצים ב-OneDrive וחוברות Excel: חיפוש, קריאה, יצירה והעלאה. הסיומת .All פירושה **כל הקבצים שלמשתמש עצמו כבר יש גישה אליהם**, כולל קבצים ששותפו איתו — הגרסה הצרה (Files.ReadWrite) אינה מאפשרת גישה לקבצים משותפים
Chat.ReadWrite	Read and write user chat messages	צ'אטים ב-Teams של המשתמש: קריאה וכתיבה
ChatMessage.Send	Send user chat messages	שליחת הודעה בצ'אט בשם המשתמש
Team.ReadBasic.All	Read the names and descriptions of teams	**שמות בלבד** של הצוותים שהמשתמש חבר בהם. אינה מאפשרת קריאת תוכן
Channel.ReadBasic.All	Read the names and descriptions of channels	**שמות בלבד** של ערוצים. אינה מאפשרת קריאת תוכן
ChannelMessage.Send	Send channel messages	שליחת הודעה לערוץ בשם המשתמש
ChannelMessage.Read.All	Read user channel messages	**דורשת אישור מנהל מפורש.** קריאת הודעות שנכתבו בערוצים שהמשתמש חבר בהם
Channel.Create	Create channels	**דורשת אישור מנהל מפורש.** פתיחת ערוץ חדש בצוות
Schedule.Read.All	Read user schedule items	**דורשת אישור מנהל מפורש.** צפייה במשמרות של המשתמש ב-Teams Shifts

OnlineMeetings.Read	Read user's online meetings	איתור פגישה מקוונת לפי קישור ההצטרפות שלה. אינה קוראת תוכן
OnlineMeetingTranscript.Read.All	Read all transcripts of online meetings	**דורשת אישור מנהל מפורש.** קריאת תמלול של פגישה שהמשתמש השתתף בה, כדי לסכם אותה עבורו

שלוש ההרשאות המסומנות — אופציונליות לחלוטין

שלוש ההרשאות האחרונות בטבלה הן היחידות ש-Microsoft מסווגת כדורשות **אישור מנהל מערכת מפורש**. כל השאר מאושרות על ידי המשתמש עצמו.

הן מבודדות ביישום כיחידה נפרדת. עובד שיחבר את Teams מקבל צ'אטים, שמות צוותים וערוצים ושליחת הודעות — בלי שאף אחת מהשלוש תידרש. מי שלא יאשר אותן אינו מאבד דבר מלבד שלוש היכולות האלה עצמן, והשירות ממשיך לעבוד במלואו.

לפיכך אפשר לאשר את היישום **בלעדיהן**, ולחזור ולשקול אותן בנפרד אם וכאשר יתעורר צורך.

תמלולי פגישות: שני דברים שצריך להפעיל

כדי שהעוזר יוכל לסכם פגישה, התמלול שלה צריך להיות קיים ונגיש. שני הדברים האלה מוגדרים בארגון, ואינם חלק מאישור ההרשאות:

1. **תמלול בפגישות Teams.** שהמשתתפים יוכלו ללחוץ "התחל תמלול" בפגישה. נקבע במדיניות הפגישות של הארגון.

2. **גישה לתמלולים דרך Microsoft Graph.** מתג נפרד, כבוי כברירת מחדל: מרכז הניהול של Teams → *Meetings* → *Meeting settings* → *Transcript API access*. בלעדיו הבקשה נדחית גם כשההרשאה אושרה.

להצגת שמות הדוברים בתמלול נדרש גם -EnableAttributedTranscripts. הסיכום נעשה על ידי היישום מתוך הטקסט.

חשבון ארגוני מול חשבון Microsoft אישי

היישום עובד עם שני הסוגים, בהבדל אחד: **Teams אינו קיים בחשבון אישי** (Outlook.com, Hotmail, Live). אין לו שם ממשק Graph, ולכן שמונה ההרשאות של Teams נוגעות לארגונים בלבד ואינן מוצעות למשתמש פרטי. גם מציאת חלון פנוי משותף אינה קיימת שם.

יומן, דואר, אנשי קשר, משימות וקבצים עובדים בשני הסוגים באותה צורה. בחשבון אישי אין מנהל מערכת ואין חסימה ארגונית, והמסמך הזה אינו נדרש.

הנקודה המהותית: Delegated ולא Application

כל 20 ההרשאות הן מסוג **Delegated**. משמעות הדבר שהיישום פועל **אך ורק בהקשר של המשתמש שהתחבר, ורואה אך ורק את הנתונים שלו עצמו**, בכפוף להרשאות שכבר יש לאותו משתמש בארגון.

לשם השוואה, הרשאות מסוג *Application* היו מאפשרות ליישום לגשת לתיבות הדואר של כלל הארגון ללא משתמש מחובר. **היישום אינו מבקש ואינו מחזיק הרשאות מסוג זה.**

מתן אישור ארגוני **אינו מחבר אף משתמש באופן אוטומטי.** הוא מסיר את החסימה בלבד; כל עובד שיבחר להשתמש בשירות יתחבר בעצמו, ועבורו בלבד.

5. אבטחת מידע ושמירת נתונים

- **אין שמירה של עותק מתיבת הדואר או מהיומן.** תוכן נשלף מ-Microsoft Graph בזמן אמת לצורך הבקשה הספציפית ואינו נשמר במאגרי המידע שלנו. תוכן שהמשתמש בוחר לדון בו מול העוזר עשוי להופיע בהיסטוריית השיחה האישית שלו, הנגישה לו בלבד.
- **אסימוני הגישה נשמרים מוצפנים** במסד הנתונים, ולא בטקסט גלוי.
- **כל התקשורת מוצפנת** בתעבורה (HTTPS/TLS) מקצה לקצה.
- **הערכת אבטחה חיצונית שנתית.** המערכת נבדקת מדי שנה על ידי מעבדת אבטחה מוסמכת, בהליך CASA (Cloud Application Security Assessment). ההערכה כוללת בדיקת תצורה, ניהול הרשאות ואבטחת ממשקים.
- **הגישה הפיכה בכל רגע** ונשלטת במלואה על ידי הארגון (ראו סעיף 7).
- **המידע אינו משמש לאימון מודלים.** נתוני המשתמשים אינם משמשים לאימון או לשיפור של מודלי בינה מלאכותית, לא על ידינו ולא על ידי ספקי המודלים.
- **עבודה מול ספקים רשמיים בלבד.** המערכת פועלת מול OpenAI, Anthropic ו-Google Gemini, בממשקי ה-API העסקיים שלהם, שבהם הנתונים אינם משמשים לאימון מודלים.
- **אין העברת מידע לצדדים שלישיים** לצורכי פרסום או מכירה.
- **מדיניות פרטיות מלאה** זמינה בכתובת practice-ai.co.il/privacy-policy.

6. כיצד לאשר

קיימות שתי דרכים שוות ערך, ושתיהן מבוצעות פעם אחת בלבד עבור כלל הארגון.

לביצוע הפעולה נדרשת **אחת** מההרשאות הבאות: **Global Administrator**, **Privileged Role Administrator** או **Cloud Application Administrator**. מאחר שכל ההרשאות המבוקשות הן מסוג Delegated בלבד, אין הכרח דווקא במנהל-על של הארגון.

דרך א': קישור ישיר

פתיחת הקישור והתחברות עם חשבון מנהל המערכת. Microsoft תזהה את הארגון באופן אוטומטי ותציג את מסך האישור:

```
https://login.microsoftonline.com/organizations/v2.0/adminconsent?client_id=6db47650-1fe7-4b0a-b893-a802c925d272&scope=https%3A%2F%2Fgraph.microsoft.com%2F.default&redirect_uri=https%3A%2F%2Fpractice-ai.co.il%2Fassistant%2Fmicrosoft%2Fcallback%2F&state=org_consent
```

לאחר לחיצה על "**קבל**" תתבצע הפניה חזרה לאתר שלנו, והאישור נרשם.

דרך ב': מתוך פורטל Microsoft Entra

1. כניסה אל `entra.microsoft.com` בחשבון מנהל מערכת.
2. מעבר אל **Enterprise applications** ובחירת **Practice AI Assistant**.
   היישום מופיע ברשימה לאחר שמשתמש בארגון ניסה להתחבר לפחות פעם אחת.
3. בתפריט הצדדי: **Permissions**.
4. לחיצה על **Grant admin consent** ואישור רשימת ההרשאות.

חשוב: תיבת הסימון "הסכמה בשם הארגון שלך"

אם האישור ניתן מתוך **זרימת ההתחברות הרגילה** ולא מהקישור שבדרך א', יופיע במסך תיבת סימון בשם "**הסכמה בשם הארגון שלך**" (ראו צילום המסך בסעיף 3).

יש לסמן אותה. בלעדיה האישור חל על המשתמש המאשר בלבד, ושאר עובדי הארגון ימשיכו להיתקל בחסימה.

7. כיצד לבטל

ניתן לשלול את ההרשאה בכל עת, ללא תלות בנו וללא צורך לפנות אלינו:

`entra.microsoft.com` → **Enterprise applications** → **Practice AI Assistant** → **Properties** → **Delete**

הביטול מנתק את כל המשתמשים בארגון מהשירות באופן מיידי. בנוסף, כל משתמש יכול לנתק את החשבון שלו בכל רגע מתוך הממשק של מועדון AI פרקטי.

8. לשאלות נוספות

נשמח לענות על כל שאלה של מחלקת ה-IT, לרבות שאלות על ארכיטקטורה, שמירת נתונים או הליכי האבטחה, ולהעמיד מידע נוסף לפי הצורך.

בברכה,

אשר מורגנשטרן

סמנכ"ל טכנולוגיה וממונה הגנת מידע (DPO) · בינה מלאכותית בגובה העיניים בע"מ (EYE LEVEL AI LTD)

דואר אלקטרוני: **asher@practice-ai.co.il**

אתר: **practice-ai.co.il**

מסמך זה הופק על ידי בינה מלאכותית בגובה העיניים בע"מ (ח.פ. 517180931) ומיועד למחלקות טכנולוגיות המידע של ארגונים שעובדיהם משתמשים בשירותי מועדון AI פרקטי. הפרטים נכונים למועד העדכון המופיע בראש המסמך.