משרד החדשנות, המדע והטכנולוגיה
Ministry of Innovation, Science & Technology

אגף טכנולוגיות דיגיטליות ומידע

שיקולים טכנולוגיים לפתרון AI לסקירת הצעות מחקר

רקע ומטרת הפרויקט

- מטרת הפרויקט היא הקמת מערכת מבוססת בינה מלאכותית שתסייע למשרד החדשנות, המדע והטכנולוגיה לבצע סקירה ראשונית של הצעות מחקר המוגשות במסגרת קולות קוראים
- כיום תהליך הסקירה מבוסס על סוקרים אנושיים בלבד, דבר הדורש זמן ומשאבים לאיתור סוקרים, העברת ההצעות וקבלת חוות הדעת. שילוב כלי AI נועד לייעל את התהליך באמצעות ניתוח אוטומטי של ההצעות, הפקת תובנות ותמיכה בעבודת ועדות השיפוט.

יכולות פונקציונליות מבוקשות

- המערכת תקלוט הצעות מחקר בפורמטים נפוצים) כגון PDF ו ,(DOCX-תנתח את תוכנן באמצעות כלי AI, ותבצע דירוג של ההצעות לפי קריטריונים מוגדרים.
- בנוסף, המערכת תפיק דוחות סקירה אוטומטיים, תאפשר השוואה בין הצעות מחקר שונות ותספק דשבורד ייעודי למנהלי תוכניות ולוועדות השיפוט לצורך קבלת החלטות מושכלת.

פלט המערכת

יש לפרט את התהליך הכוללך קריטריוני הערכה והתוצרים:

- ציון מספרי לכל קריטריון
- סיכום חוזקות וחולשות
- המלצה ראשונית לוועדה
- דוח סקירה מפורט

סוג פתרון המבוקש

- פתרון טכנולוגי העונה על הנחיות ממשלתיות – מפורט בהמשך
- פתרון פשוט ליישום ולתחזוקה, אשר מבוסס על שירותי ענן קיימים ומודלים מוכנים
- מומלץ לבחור פתרון אשר עומד בקריטריונים הבאים:
  - פתרון **פשוט ומהיר ליישום**
  - **קל לתחזוקה לאורך זמן**
  - מבוסס **שירותי ענן מנוהלים (Managed Services) עדיפות לAWS**
  - שימוש בשירותי AI מנוהלים
  - אינו דורש צוות פיתוח לאורך זמן (רק ליישום והתאמות)
  - מאפשר הרחבה עתידית

משרד החדשנות, המדע והטכנולוגיה
Ministry of Innovation, Science & Technology

אגף טכנולוגיות דיגיטליות ומידע

תשתית הענן והעדפת פלטפורמה

- שימוש ב AWS במסגרת פרויקט נימבוס ובהתאם לשירותים המאושרים לרכש בממשלה.
- השימוש בענן צריך להיות תואם למדיניות הממשלתית, לדרישות אבטחת מידע ולמגבלות רכש.
- המשרד מפעיל את מערכותיו בענן AWS במסגרת פרויקט נימבוס ,ולכן קיימת העדפה לפתרון אשר ניתן למימוש ולהפעלה בסביבה זו. שימוש בתשתית AWS הקיימת צפוי לצמצם עלויות הקמה, תפעול ואינטגרציה, וכן להקל על שילוב הפתרון במערכות המשרד הקיימות.
- ככל שהפתרון המוצע מבוסס על תשתית ענן אחרת, על הספק לפרט במסגרת המענה את כלל המשאבים והעלויות הנדרשים לצורך הקמה ותפעול של הסביבה, לרבות:
  - הקמת תשתיות ענן נדרשות
  - עלויות תפעול שוטפות של הסביבה
  - ניהול פיננסי של משאבי הענן(FinOps)
  - משאבי תשתית, אחסון, עיבוד ורשת
  - מנגנוני ניהול, ניטור ואבטחת מידע
- בנוסף, על הספק להציג הערכת עלויות מלאה והשלכות תפעוליות של פתרון המבוסס על ענן שאינו AWS לרבות התאמה למדיניות הענן הממשלתית ולדרישות הרכש והאבטחה הרלוונטיות.

לוח זמנים משוער ליישום

- לו"ז למימוש עד חודשיים עבודה כולל כל השלבים – אפיון, יישום, התאמות, בדיקות וכו'.

מגבלות רכש ממשלתיות

הפתרון חייב לעמוד בהנחיות הרכש הממשלתיות בין היתר:

- שימוש בשירותים המאושרים במסגרת פרויקט נימבוס. ראו:
  https://www.gov.il/he/departments/topics/nimbus_cloud_strategy/govil-landing-page
  https://www.gov.il/he/departments/topics/takamnimbus/govil-landing-page
- אפשרות לרכש דרך השוק הדיגיטלי הממשלתי ככל שנדרש. ראו:
  https://takam.mof.gov.il/document/HM.16.12.1
  https://takam.mof.gov.il/document/HM.16.12.3

דרישות תשתיות, הגנת הפרטיות וסודיות

- הפתרון יכלול ארכיטקטורה תשתית הכולל את כלל הרכיבים הנדרשים.
- מניעת שימוש במידע לצורך אימון מודלים חיצוניים, אלא אם אושר במפורש ובהתאם למדיניות

- שמירה על הגנת הפרטיות וסודיות נתוני הצעות המחקר
- יש לפרט את תהליכי הגנת מידע, הצפנת מידע , ניהול הרשאות מבוסס תפקידים, רישום ובקרה על גישה למסמכים
- ניהול הרשאות - שמירה על הפרדת מידע בין משתמשים ותהליכים
- מנגנוני מחיקה ושימור בהתאם למדיניות

דרישות אבטחת מידע, פרטיות וריבונות נתונים

- **ריבונות** נתונים **ומיקום גיאוגרפי** כלל נתוני המערכת, לרבות מסמכי המקור, בסיסי הנתונים הווקטוריים (Vector DB) והייצוגים הווקטוריים (Embeddings) יאוחסנו אך ורק ב Region-הישראלי של ספק הענן הנבחר: במידה וייבחר שימוש ב AWS-הנתונים יאוחסנו ב `il-central-1` ובמידה וייבחר שימוש ב GCP-הנתונים יאוחסנו ב`me-west1`, עיבוד המידע (Inference) יבוצע בישראל, כאשר במידת הצורך ובכפוף לאישור, ניתן לבצע עיבוד זמני ב Regions-מאושרים באיחוד האירופי בלבד, ללא שמירת נתונים במנוחה מחוץ לגבולות המדינה .כמו כן, יש לוודא מחיקה אוטומטית של קובצי המקור והנתונים הגולמיים מיד לאחר השלמת תהליך יצירת הייצוג הווקטורי וטעינת הנתונים הסופיים.
- **הגנה על המידע ומניעת אימון מודלים** הספק מחויב להוכיח כי הופעל מנגנון "Opt-out" המבטיח כי המידע והתשובות לא ישמשו לאימון או שיפור מודלי השפה של יצרן המודל או צד שלישי .העבודה תתבצע אך ורק מול מודלים מנוהלים כגון Amazon Bedrock המבטיחים חוזית הפרדת נתונים מלאה ואי-שימוש במידע לצורך אימון.
- **אבטחת רשת ובידוד רכיבים** הפתרון יופעל בתוך סביבת ה VPC-של המשרד ,כאשר כלל התקשורת לשירותי ה AI-תתבצע בחיבור פרטי ומאובטח כגון AWS PrivateLink ללא חשיפה לאינטרנט הציבורי .הגישה למערכת תתבצע באמצעות אימות דו-שלבי (MFA) וניהול הרשאות לפי עקרון "מינימום הרשאות.(Least Privilege) "
- **בקרות תוכן ו DLP (Data Loss Prevention)-**המערכת תכלול שכבת הגנה אקטיבית לסינון תוכן רגיש ,(PII) מניעת מתקפות "הזרקת פקודות (Prompt Injection) "וחסימת תשובות מודל שאינן עומדות במדיניות האבטחה .יש להפעיל כלי DLP כגון Amazon Macie לזיהוי ומיסוך אוטומטי של פרטים אישיים מזוהים בטרם שליחתם לעיבוד במודל .בנוסף, תוגדר מגבלת כמות הודעות לשעה למשתמש לצמצום סיכוני דלף מידע ושימוש לרעה במשאבים.
- **ניטור, בקרה ומשילות** הפתרון יתמוך בהעברת לוגים מלאה (Audit Logs) בזמן אמת למערכות הניטור וה SOC-של המשרד .המודל יונחה לספק תשובות אך ורק על בסיס המידע המסופק בקונטקסט של הצעות המחקר, ללא הסתמכות על ידע חיצוני למניעת "הזיות" , והמערכת מחויבת לציין עבור כל תשובה את המקור המדויק (שם מסמך/פרק) ממנו נשלף המידע.

מדדי הצלחה לפיילוט

- התאמה בין ציוני המערכת לציוני סוקרים אנושיים
- איכות הסיכום האוטומטי
- זיהוי הצעות מצטיינות או חלשות

- קיצור זמן הטיפול בהצעה
- שביעות רצון משתמשים

תרשים ארכיטקטורה מוצע

יש להגיש ארכיטקטורה מפורטת לכל תהליך, לדוגמא:

1. קליטת הצעות מחקר
2. מנוע עיבוד מסמכים
3. מודל AI
4. מנוע דירוג והפקת דוחות
5. דשבורד ועדה

איכות ובשלות הפתרון המוצע

- על הספק להציג מידע מפורט בדבר איכות הכלי המוצע ורמת הבשלות שלו לשימוש מבצעי
- במסגרת זו יידרש הספק לפרט את אופן השימוש בכלי בארגונים אחרים, לרבות מספר המשתמשים הפעילים, סוגי הארגונים המשתמשים במערכת (לדוגמה: מוסדות מחקר, אוניברסיטאות, גופים ציבוריים או פרטיים), והיקפי השימוש בפועל
- בנוסף, על הספק להציג נתונים המעידים על יכולת המערכת לפעול בהיקפים משמעותיים, לרבות עמידה בעומסי עבודה, ביצועים, זמני תגובה, זמינות המערכת (SLA) וניסיון מוכח בהפעלת המערכת בסביבות ייצור.