2.6.26

הנדון: **<u>בקשה להצעת מחיר לשירותי פיתוח ותחזוקה שוטפת של אתר האינטרנט עבור המכללה האקדמית אחוה</u>**

<u>כללי:</u>

כחלק מפעילותה, המכללה האקדמית אחוה (ע"ר) (להלן: "המכללה") מבקשת להתקשר עם חברה מקצועית (להלן: "הספק") לצורך קבלת שירותי פיתוח, תחזוקה שוטפת ושדרוג מתמיד של אתר האינטרנט של המכללה. האתר כולל רכיבי הזדהות, מנוע חיפוש, רכיבי נגישות, חנות מקוונת ומערכות נלוות, והוא מהווה את הנכס הדיגיטלי המרכזי של המכללה מול סטודנטים, מרצים, בוגרים וקהל רחב.

מטרת ההתקשרות היא להבטיח זמינות, אבטחה, עדכונים שוטפים, ביצועים גבוהים והמשכיות עסקית — ובמקביל, לקדם חדשנות טכנולוגית פעילה. המכללה מבקשת ספק שיפעל לא רק כגורם תחזוקה, אלא כשותף טכנולוגי המוביל שיפור מתמיד של חוויית המשתמש, הנראות והרלוונטיות של האתר בסביבה דיגיטלית המשתנה ללא הרף.

הליך זה אינו מהווה מכרז ודיני המכרזים אינם חלים עליו

<u>אשת קשר במכללה:</u> עו"ד שני מור, shany.mor@achva.ac.il

<u>תכולת המסמך:</u>

1. בקשה להצעה ותנאים כללים
2. מפרט השירות
3. ניסיון המציע
4. נספח א' – הצעת והצהרות המציע
5. נספח ב'- כתב סודיות וניגוד עניינים- כללי
6. נספח ג'- נספח ביטוח
7. נספח ד'- שאלון ממליצים
8. נספח ה'- נספח סודיות, פרטיות ואבטחת מידע
9. נספח ו'- הסכם אבטחת מידע ושאלון ספק

<u>תנאים כלליים להצעה:</u>

1. המכללה אינה מתחייבת לקבל את ההצעה הזולה ביותר , או אף אחת מההצעות.
2. הצעת המחיר תוגש במטבע ישראלי בלבד לא כולל מע"מ.
3. המכללה תהיה רשאית לנהל משא ומתן עם החברה הזוכה.
4. המכללה האקדמית אחוה שומרת לעצמה את הזכות לבטל בכל עת את הזמנת העבודה בהתאם לשיקול דעתה ומכל סיבה שהיא תוך מתן הודעה בכתב או בדואר אלקטרוני בהתראה של 30 יום.

5. על הספק לחתום על כל דפי ההצעה הנ"ל כאישור להבנתו ולהסכמתו עימם.
6. מחלקת הרכש רשאית לפסול הצעה שיהיו בה שינויים או תיקונים.
7. תוקף הצעת המחיר תקף ל 90 יום מיום ההגשה.

לוח המועדים:

תיאור	המועד
מועד פרסום הבקשה	2.6.26
המועד האחרון לשאלות הבהרה	11.6.26 עד השעה 12:00
המועד האחרון להגשת ההצעות	18.6.26 עד השעה 12:00

תנאי תשלום: שוטף+30 מיום קבלת החשבונית בהנהלת החשבונות של המכללה.

תקופת ההתקשרות: למשך 60 חודשים (5 שנים). למכללה בלבד שמורה הזכות להביא חוזה זה, לידי סיום, לפי שיקול דעתה המוחלט והבלעדי, בכל עת במהלך תקופת ההתקשרות, בהודעה בכתב שתימסר ליועץ לפחות 30 יום מראש, ומבלי צורך לנמק.

נא להגיש את ההצעה, חתומה על כל דפיה עם חותמת חברה וחתימת בעל זכות חתימה, כולל כל הרישיונות/ נספחים/ פרופיל חברה למייל : shany.mor@achva.ac.il לא יאוחר מתאריך יום ה' 18.6.26 עד השעה 12:00.

תנאי סף נדרשים (נא לצרף להצעה):

1. אישור ניהול ספרים בתוקף
2. אישור על ניכוי מס במקור בתוקף
3. טופס התאגדות חברה/ תעודת עוסק מורשה/ פטור/ שותפות
4. למציע ניסיון מוכח של 5 שנים לפחות, באספקת שירותים הדומים בסוגן כנדרש בפלה"מ זה, עם גופים ציבוריים ו/או גופים פרטיים. לשם כך ימלא המציע את טבלת "ניסיון המציע".
5. למציע מחזור כספי של לפחות 2 מיליון בכל שנה, בין השנים 2022-2025, לשם כך ימלא המציע את "הצעת והצהרות המציע".
6. למציע ניסיון מוכח של לפחות 3 שנים, הן בפיתוח אתרים בעלי ממשקים (אינטגרציות), והן בחוויית משתמש, לשם כך ימלא המציע את "הצעת והצהרות המציע".

7. המציע מעסיק בהעסקה ישירה 5 עובדים לפחות, מהם לפחות 3 מפתחים, לשם כך ימלא המציע את ״הצעת
והצהרות המציע״.
8. למציע ניסיון מוכח בהנגשת אתרים ובפיתוח מונגש עם העדפה לשירותי הנגשה ברמת AA, לשם כך ימלא
המציע את ״הצעת והצהרות המציע״.

<u>בחירת ההצעה הזוכה: (ניקוד ההצעות)</u>

ההצעה הזוכה תיבחר באופן הבא:

1. בדיקת שלמות ההצעה ועמידה בתנאי הסף- מציע שלא יעמוד בתנאי הסף, הצעתו תיפסל.
2. בדיקת איכות: 60% מכלל הניקוד – ועדה פנימית מטעם המכללה תיבחן את המציעים בפרמטרים של:

- שיחות עם לקוחות עבורם בוצע שירות דומה (נא למלא את הטבלה בסעיף ״ניסיון המציע״)) 20%- המכללה ו/או מי מטעמה ייצרו קשר עם עד שלושה (3) לקוחות ותשאל אותם שאלות זהות באמצעות טופס הניקוד המצורף כנספח ד׳.
- ריאיון אישי (בזום) עם נציגי המכללה 40% – בראיון ייבחנו ניסיון מקצועי, פרו אקטיביות, שירותיות ותקשורתיות, מתן מענה UX UI, הבנת צרכי המכללה, ובחינת יכולות המציע לעמוד בדרישות המכללה.

3. בדיקת מחיר 40%: המציע בעל ההצעה הזולה ביותר יקבל את מירב הנקודות (40%) ולאחריו ינוקדו המציעים באופן יחסי.

המכללה תבחר את ההצעה הזוכה בהתאם להצעה שקיבלה את הציון המשוקלל הגבוה ביותר מבין ההצעות הכשירות שעמדו בתנאי הסף וביתר תנאי המכרז.

על אף האמור לעיל, המכללה שומרת על זכותה שלא לקבל את ההצעה שתזכה לציון הגבוה ביותר, בכפוף להוראות הקבועות לעניין זה בדין ובתקנות חובת המכרזים.

<u>מפרט השירות:</u>

<u>מטרת התפקיד:</u>

קבלת שירותי תחזוקה שוטפת לאתר האינטרנט קיים, הכולל רכיבי הזדהות, מנוע חיפוש, רכיבי נגישות וחנות וכל הקשור לאתר המכללה. מטרת ההתקשרות היא להבטיח זמינות, אבטחה, עדכונים, ביצועים, המשכיות עסקית, פיתוח תכולות חדשות, שיפור ביצועים, התחדשות וחדשנות וכן לאפשר שיפור מתמשך של חוויית המשתמש והנראות.

<u>תחומי אחריות עיקריים והתנהלות נדרשת:</u>

1. **<u>דרישות כלליות</u>**:

- <u>מנהל לקוח קבוע</u>: הספק ימנה מנהל לקוח קבוע לאורך כל תקופת ההתקשרות.
- <u>מפרט שרתים</u>: יוגדרו בפרט השירות ויהווה דרישת מינימום מחייבת.
- <u>שיטת התחברות</u>: הספק יתאים את עצמו לשיטת ההתחברות בהתאם לדרישות המכללה ו/או המארח. הן בסביבת הטסט והן בסביבת הייצור, בהתאם להנחיות המכללה.

2. **<u>תחזוקה ופעילות שוטפת:</u>**

- הספק יעמיד לרשות המכללה מנהל לקוח קבוע שילווה את המכללה בשגרה ובחירום וירכז אצלו את כל המענים.
ככל שהספק יידרש להחלפת מנהל לקוח ,הדבר יעשה באישור המכללה מראש.
- כל הרכיבים, בהם הספק יעשה שימוש, יהיו ברישוי המכללה, מותאמים ונתמכים ב- WP.

יודגש, כי ישנה עדיפות לרכיב נתמך ולא לפיתוח.

- הספק ינהל את המשימות והקריאות שיתקבלו , הן בהיבט ניהול תחום זה והן בהיבט תפעולי, לרבות באגים, שינויים, פיתוחים וכד', במערכת מידע, בהתאם להחלטת המכללה.
- הספק ייקח חלק בפגישות סטטוס קבועות, שיקבעו בהתאם לצורך ודרישת המכללה, כחלק מהעבודה השוטפת (תכנון, תיעדוף, מעקב ביצוע).
- הספק ינקוט בגישה פרואקטיבית יזומה בכל הקשור לשדרוג האתר, לרבות, הצגת תוכנית רבעונית לפיתוח תכולות חדשות, שיפור ביצועים, התחדשות וחדשנות וכן לאפשר שיפור מתמיד של חוויית המשתמש והנראות והתאמתו בצורה וביכולות המתקדמות ביותר . על הספק ליזום פעולות לתקינות המערכות עפ"י דרישות היצרן ותקני אבטחת מידע וכל זאת על מנת שלא תהיה פגיעה בזמינות ויציבות האתר.
- הספק יידרש להציג דו"ח ביצוע רבעוני אשר יכלול נתוני אמינות האתר (זמינות, ביצועים), SLA, שינויים, פעולות תחזוקה והמלצות התייעלות.
- הספק יידרש לעבוד בשיתוף פעולה עם כלל הגורמים המעורבים בתחזוקה ובתפעול האתר. בין שמדובר בגורמים במכללה ובין שמדובר בספקים חיצוניים.

3. **<u>מודל השירות ואחריות מקצה- לקצה (END-TO-END)</u>**

- הספק יהיה האחראי הבלעדי לתפקודו התקין, זמינותו וביצועיו של אתר המכללה, במודל "מקצה לקצה". האחריות לא תכלול הזנת תוכן שוטף, שתבוצע על ידי המכללה.
- <u>אחריות רוחבית</u>: הספק יעניק מענה מלא לרכיבי BACKEND/FROTEND, שירותי סיסטם ותשתיות, שירותי סטודיו/עיצוב, ככל שידרשו לתחזוקה שוטפת ופיתוחים חדשים.
- <u>תמיכה רב- מכשירנית</u>: על הספק לדאוג לתקינות האתר וכל רכיביו, בכל סוגי המכשירים והדפדפנים הנפוצים (TABLET ,MOBILE DESKTOP).

4. **<u>סביבות עבודה, ניהול שינויים והעברה לייצור:</u>**

- הספק יתחזק סביבת ייצור (PRODUCTION) וסביבת בדיקות (TEST/STAGING), זהות לחלוטין בקונפיגורציה ובנתונים.
- עדכונים ו/או תיקונים יבוצעו תחילה בסביבת הבדיקות ויועברו לייצור רק לאחר אישור פורמלי של המכללה.
- <u>ניהול שרתים וגרסאות</u>: הספק מתבקש לבצע עדכון שוטף של גרסאות הליבה של WORDPRESS,עדכון תוספים (PLUGING), ועדכון גרסאות ה- PHP וה- DB בשרתים, החלפת תעודות SSL וכל תחזוקה נדרשת.
- <u>אחריות על מערכת ההפעלה</u>: הספק יהיה אחראי באופן מלא על התקנת, תפעול ותחזוקת רכיבי התוכנה במערכת ההפעלה בשרתים לאורך כל תקופת ההתקשרות.
- <u>ניהול שינויים (CHANGE MANAGEMENT)</u>: הספק יידרש לתעד באופן מלא כל שינוי ברמה חודשית, כולל תוכנית ROLLBACK ו- CHANGE LOG.
- הגורמים המקצועיים במכללה והספק יגדירו חלון תחזוקה מוסכם לפעולות מתוזמנות ותקשורת יזומה לפני/אחרי שינוי.

5. **<u>תחזוקת רכיבים ייעודיים ומערכות נלוות</u>**:

- <u>מנגנון הזדהות</u>: הספק יידרש למתן תמיכה ותחזוקה מלאה של רכיב ההזדהות הקיים (MINIORGANE) לחיבור למערכת הניהול (IDM) בפרוטוקול SAML.
- <u>מנועי חיפוש</u>: הספק יידרש לתחזוקה ותמיכה ברכיבי החיפוש באתר.
- <u>נגישות</u>: הספק יידרש להבטחת תקינות רכיבי הנגישות ועמידה בתקן AA (מומלץ WCAG 2.1AA). <u>דו"ח נגישות תקופתי מכלי סריקה כמו Accessibe או Axe על מנת לוודא שלא הוספו רכיבים שוברי נגישות.</u>
- <u>חנות האתר</u>: הספק יידרש לתחזוקת מודול WOOCOMMERCE וממשקי הסליקה. נדרש אפיון מחדש בנושא כמפורט בסעיף 7 למפרט השירותים.
- <u>רישויים</u>:

כל הרישויים צריכים להירשם על שם המכללה. על הספק מוטלת האחריות להתנהלות נכונה לחידוש הרישויים על מנת לשמור על יציבות וזמינות האתר. כל רישוי חדש צריך לעבור אישור מראש לפני השימוש, תכנון, פיתוח.
כלל הפיתוחים והתוספים החדשים צריכים להתבסס על טכנולוגיה ידועה ומוכרת בשוק על מנת שלא יווצר מצב של בלעדיות וחוסר יכולת לתמיכה ע"י גורם שהוא לא הספק.

6. **<u>דרישות שיווק ותמיכה עסקית:</u>**

- <u>מסע לקוח (CUSTOMER JOURNEY)</u>: הספק יידרש לבצע ולתמוך בתהליך שיפור מתמשך של חווית המשתמש והנראות באתר המכללה, בקרב סטודנטים פעילים ופוטנציאליים/מתעניינים, מרצים ובוגרים. התהליך יכלול מיפוי מסעות לקוח, איתור צווארי בקבוק והמלצות לשיפור.
- <u>גישה פרואקטיבית יזומה</u>: הספק יידרש להצגת ROADMAP רבעוני הכולל הצעות לפיתוחים, שיפורים וחידושי נראות (UI/UX), לרבות אומדנים ותיעדוף.
- <u>מדידה ותובנות</u>: הספק יידרש להטמעה/תחזוקה של כלי אנליטיקה ואירועים (EVENTS) והפקת דו"חות KPI (כניסות, המרות, חיפוש פנימי ומשפכים).
- <u>SEO טכני</u>: חוויית משתמש(Core Web Vitals) : הספק יבטיח עמידה בציון 'ירוק' במדדי "Google PageSpeed Insights".
- הספק יידרש לפיתוח האפשרות לעמודים ומסמכים הניתנים לגישה באמצעות מערכת ההזדהות.
- <u>פיתוחים קיימים</u>:

הספק יידרש, לתחזק ולפתח את הפיתוחים הקיימים, שנעשו עד תחילת הסכם זה, לתחזק אותם ולהמשיך לפתחם עפ"י הצורך, בין אם מדובר בקוד ייעודי שפותח לאתר ובין אם מדובר ברכיבים ייעודיים של WP.

- הספק יפעל לאופטימיזציה של **מנגנון החיפוש הפנימי** באתר.

7. **<u>אפיון ופיתוח חנות האתר (E- COMMERCE):</u>**

- הספק יאפיין את חנות האתר בהתאם לצרכים שעלו ויעלו מהשטח, לרבות מסכי חנות, סיוג מוצרים/שירותים, תהליכי סליקה, קופונים/מבצעים, אספקה /דיגיטל, הרשאות ודו"חות וכד'.
- הספק יפעל לתחזוקת החנות (WOOCOMMERCE), כולל בדיקות רגרסיה לאחר עדכונים ושמירה על תאימות גרסאות.

8. **<u>אמנת שירות (SLA) וקנסות:</u>**

- המכללה תהיה רשאית להטיל קנסות על הספק, אשר יקוזזו מהתשלום המגיע לספק מהמכללה, ככל שלא יעמוד בזמני התגובה והפתרון בהתאם לטבלה המפורטת להלן:

רמת חומרת התקלה	הגדרת התקלה	SLA	קנס על חריגה מזמן תגובה	קנס על חריגה מזמן פתרון	קנס מוגדל במקרה של כשל חוזר
רמה 1- קריטית	אתר למטה, פריצת אבטחה, תקלה משביתה ב/SSO- הזדהות.	<u>תגובה:</u> בתוך 15-30 דקות (24/7)	2,500 ₪ לכל שעה או חלק ממנה.	5,000 ₪ לכל שעה או חלק ממנה.	אם נרשמו 3 אירועים בחודש,

	רכיב מרכזי לא עובד (למשל: החנות), פגיעה משמעותית בביצועים.	פתרון: עד 4 שעות			תוספת **25%** לכל קנס.
רמה 2- גבוהה-בינונית	באג שאינו משבית, תקלת עיצוב מקומית.	תגובה: בתוך 4 שעות עבודה. פתרון: עד 3 ימי עסקים.	300 ₪ לכל שעת איחור.	1,000 ₪ לכל יום איחור.	אם חריגה חוזרת על 5 תקלות בחודש תוספת **10%**.
רמה 3- נמוכה	פיתוחים חדשים	תגובה: בתוך 3 ימי עסקים. פתרון: לפי תיעדוף	850 ₪ לכל יום איחור.	850 ₪ ליום עסקים מעבר לזמן סביר.	ללא קנס מוגדל.

- ימי ושעות פעילות הספק:

א. עבור תקלה קריטית: 364 ימים בשנה, 24 שעות ביממה (למעט יום כיפור).

ב. עבור תקלה גבוהה, בינונית ונמוכה: במסגרת ימי ושעות העבודה, ימים א-ה, בין השעות 8:30- 17:00.

9. **מוקד שירות, בקרה ושקיפות:**

- מערכת קריאות (TICKETING SYSTEM): הספק יתפעל מערכת לניהול הקריאות בהתאם להחלטת המכללה, בה כל גורם שהינו מורשה לכך, יוכל לצפות בסטטוס הקריאות.
- ערוצי תקשורת: הספק ייתן מענה באמצעות טלפון ומייל. ההתנהלות השוטפת תתנהל דרך מערכת משימות/פרויקטים.
- דו"חות תקופתיים: הספק יציג דו"ח רבעוני הכולל פירוט קריאות, זמני מענה פעולות תחזוקה מונעת וסטטוס עדכוני גרסה. מבנה הדו"ח ייקבע על ידי הגורמים המוסמכים לכך במכללה, בשיתוף הספק.
- ישיבות עבודה: הספק ישתתף בישיבות סטטוס שוטפות (פרונטליות או בTEAMS), כחלק מהעבודה השוטפת.

10. **אבטחת מידע והגנת הפרטיות:**

- הצפנה ותקשורת: הספק יעשה שימוש בפרוטוקול TLS המתאים או לפי הצורך, וכן, הצפנת נתונים רגישים בבסיס הנתונים.
- בקרת גישה: תתבצע על ידי הספק, בהתאם להנחיות שיקבעו על ידי הגורמים המוסמכים לכך במכללה.

- הגנה בענן: הספק ינקוט באופן מימוש IPS וממשק ניהול בגישה מכתובות IP מורשות בלבד (ככל שהאתר מנוהל בענן).
- עדכוני אבטחה: הספק יעדכן את מערכות ההפעלה והתוכנה בעדכוני האבטחה, באופן קבוע.
- בדיקת אבט"מ: בכל מקרה וככל שהמכללה תדרוש ו/או תידרש לכך, הספק יהיה זמין לחקירה ו/או תמיכה ו/או מענה. הספק ישתף פעול ויספק מענה בזמן סביר לדרישות שתעביר לו המכללה.
- הספק יענה לכל דרישות אבט"מ ככל ויעלו מצד המכללה ולפי דרישתה ויפעל בהתאם לאותן דרישות.
- הספק יענה בפירוט לשאלון אבט"ח בנספח ו'1

11. **תמיכה בטכנולוגיה הקיימת באתר ובמעבר הידע:**

- הספק מתחייב לתחזק את הפיתוחים והמודולים הקיימים ולתת מענה מלא מהיום הראשון לעבודתו עם המכללה. אי הכרת הפיתוחים והמודולים הקיימים, לא תהווה סיבה מוצדקת לעיכוב בתיקון תקלות, ולא תהווה עילה לדרישת תשלום נוסף מצד הספק.
- תהליך TRANSITION: הספק מתחייב לבצע לפי דרישה וצורך, סקר קוד, מיפוי תוספים/אינטגרציות, בדיקת תצורה, מיפוי הרשאות וסקר אבטחה.
- מסירת נכסים: הספק מתחייב למסור, ככל שיידרש לכך, קוד מקור, גישות, תעודות, דומינים, חשבונות צד ג', מפת שרתים, תצורה וכד'.

בנוסף לעיל:

תחומי האחריות הספק בתחום תחזוקה ופיתוח אנלטיקה SEO, טכני ותחזוקת חנות, יהיו כמפורט להלן:

- שילוב AI וטכנולוגיות חדשות

- הספק יהיה אחראי על התאמת מבנה האתר למנועי תשובה (LLMs) ויישומי AI, לרבות הטמעת Schema מורחבת עבור קורסים, אירועים ושאלות נפוצות.

- הספק יבצע אופטימיזציה למהירות טעינה מקסימלית (LCP, FID, CLS) כחלק מסטנדרט ה-Core Web Vitals של גוגל.

- הספק ימליץ ויטמיע כלי אוטומציה לניטור תקלות SEO ושינויים בקוד המשפיעים על הדירוג.

- **הספק יהיה אחראי על אופטימיזציה לחיפוש קולי (AEO) AI:** התאמת התוכן והקוד כך שמנועי AIכמו ChatGPT או Gemini יוכלו לסרוק ולצטט את המכללה בקלות.

- **אוטומציה של QA:** הספק יידרש לשימוש בכלי ניטור אוטומטיים שמתריעים בזמן אמת על נפילת תגים או שגיאות 404, בנוסף לתיעודם בדו"ח החודשי שיציג הספק.

- **שימוש ב AI-לניתוח נתונים:** הספק יעשה שימוש בכלי AI לזיהוי אנומליות ב- GA4.

- <u>הספק יהיה אחראי באופן מלא על ניהול והטמעת מערכות אנלטיקה, לרבות:</u>

א. הטמעה, תחזוקה ובדיקת תקינות של GOOGLE TAG MANAGER, ו- GA4 וכל מערכת אחרת בהתאם להנחיית המכללה.

ב. יצירת אירועים (EVENTS), טריגרים ותצורות מדידה בהתאם לצורכי המכללה.

ג. וידוא תקינות סקריפטים לאחר כל שינוי באתר/עדכון גרסה(בדיקות רגרסיה).

ד. ניטור שוטף של תקלות מדידה, שבירת תגים או טעינות חלקיות ותיקונן.

- <u>הספק יהיה אחראי באופן מלא על הפקת דו"חות אנליטיים חודשים וללא תלות בספק SEO חיצוני, לרבות אך לא רק:</u>

א. נתוני תנועה וערוצי מקור (TRAFFIC SOURCES).

ב. נתוני התנהגות משתמשים באתר (USER BEHAVIOR).

ג. נתוני המרה וניתוח משפכים (FUNNELS).

ד. מדידת נטישה (OFF-DROP) בעמודים מרכזיים ובתהליכי רישום/רכישה.

ה. KPI יעודים למכללה (כגון: סטודנטים פעילים לעומת פניות חדשות).

- <u>הספק יהיה אחראי על איפיון (בשיתוף המכללה) ותחזוקת חנות WOOCOMMERCE ותפעול תהליכי CHECKOUT:</u>

א. אפיון החנות בהתאם לצרכי המכללה.

ב. תחזוקה שוטפת של חנות WOOCOMMERCE, כולל עדכוני גרסה ותוספים רלוונטיים.

ג. בדיקת תקינות CHECKOUT לאחר כל שינוי במערכת.

ד. ניהול תוספי סליקה, תיעוד ושמירה על תאימות גרסאות.

ה. אפיון ופיתוח דו"חות בהתאם לצורך.

ו. ביצוע בדיקת עומסים תקופתיות וממוקדות לפני עומסי רישום/ הרשמה.

- <u>הספק יהיה אחראי באופן מלא על יישום בפועל של כל תיקון SEO הדורש שינוי באתר, בקוד או בתשתיות, לרבות:</u>

א. תיקון בעיות אינדוקס ו- CRAW לפי דו"ח (SEARCH CONSOLE).

ב. ניהול הפניות (301/302), תיקון שגיאות 404 ותחזוקת REDIRECT RULS.

ג. טיפול בביצועים לצורך שיפור CORE WEB VITALS (טעינה, תמונות, קבצי JS/CSS).

ד. בדיקת תקינות SEO לאחר כל עדכון גרסה.

ה. מניעת שבירת קישורים, תצורה נכונה של CANONICAL והטמעת STRUCTURED, לפי הצורך.

- <u>הספק יהיה אחראי על תאימות נגישות (ACCESSIBILITY) תוך 3 ימי עסקים:</u>

הספק יהיה אחראי באופן מלא לכך שהאתר יעמוד בכל דרישות הנגישות הדין והתקנים החלים, לרבות

לפחות תקן ישראלי 5568, ויתקן כל חריגה או ליקוי נגישות AA ברמה WCAG 2.1 בתוך 3 ימי עסקים ממועד דרישה.

- <u>אחריות מלאה לתיקוני קוד, שרת ותצורה:</u>

הספק יהווה הגורם המבצע לכל תיקון שנדרש כתוצאה מממצאי SEO, מדידה או בדיקות אנליטיות- ללא תלות בספקים אחרים.

- <u>הספק נדרש לשיתוף פעולה עם חברת SEO (ללא העברת אחריות):</u>

א. הספק יקבל דו"חות SEO מחברת הקידום ויטמיע את התיקונים בפועל.

ב. הספק יבטיח וידאג לכך שלא יגרם מצב בו חברת SEO תאתר תקלה, אך היא לא תטופל על ידי הספק בשל תלות או חוסר גישה. האחריות לביצוע התיקונים תחול על ספק התחזוקה בלבד.

<u>ניסיון המציע</u>

<u>פירוט ניסיון רלבנטי של 5 שנים לפחות בפיתוח ותחזוקה שוטפת של אתר האינטרנט (לפחות 3 לקוחות)</u>

1. שם החברה:	
איש קשר:	טלפון:
תיאור הפעילות:	
תקופת מתן השירותים:	
2. שם החברה:	
איש קשר:	טלפון:
תיאור הפעילות:	
תקופת מתן השירותים:	

3. שם החברה:	
איש קשר:	טלפון:
תיאור הפעילות:	
תקופת מתן השירותים:	

4. שם החברה:	
איש קשר:	טלפון:
תיאור הפעילות:	
תקופת מתן השירותים:	
5. שם החברה:	
איש קשר:	טלפון:
תיאור הפעילות:	
תקופת מתן השירותים:	
6. שם החברה:	
איש קשר:	טלפון:

תיאור הפעילות:	
תקופת מתן השירותים:	

<u>נספח א' – הצעת והצהרות המציע</u>

פרטי המציע:

שם המציע	
מס' עוסק מורשה/ ח.פ	
כתובת מלאה למשלוח דואר	
שם איש קשר	
כתובת דוא"ל	
טלפון נייד	

אנו החתומים מטה לאחר שקראנו בעיון את מסמכי הבקשה לייעוץ בתחום פיתוח ותחזוקה שוטפת של אתר האינטרנט

להלן הצעתינו:

- נא לציין מחיר שעתי בש"ח (לא כולל מע"מ) המכיל את כל תכולת העבודה וכולל את כל ההוצאות הנדרשות על מנת לספק את תכולת העבודה (לרבות נסיעות, אובדן זמן עבודה וכו').
- הצעתי, בהתבסס על אומדן השעות ותכולת העבודה המפרטת היא: _____ ₪ + מע"מ לשעת עבודה

הבהרות בנוגע לביצוע העבודה:

- על המציע להיות זמין לתחילת עבודה מיידית עם הודעת הזכייה.
- המכללה רשאית להזמין רק חלק מן העבודה או את כולה.

אנו מצהירים בזאת:

1. הננו מצהירים בזה כי קראנו והבנו את כל האמור במסמכי הבקשה על פרטיהם ללא יוצא מן הכלל, כי ערכנו את כל הבדיקות הדרושות ו/ או הנחוצות להגשת הצעתנו זו, וכן בחנו את כל הגורמים האחרים המשפיעים על התקשרותנו וכי בהתאם לכך ביססנו את הצעתנו. לא הסתמכנו בהצעתנו זו על מצגים, פרסומים, אמירות או הבטחות כלשהם שנעשו בעל פה על ידי המכללה האקדמית אחוה (ע"ר) להלן: "המכללה" ו או עובדיה ו או מי מטעמה, אלא על האמור במסמכי הבקשה בלבד.
2. הננו מצהירים בזה, כי אנו מסכימים לכל האמור במסמכי הבקשה ללא כל הסתייגות או שינוי וכי לא נציג כל תביעות או דרישות המבוססות על טענות של אי הבנה או אי ידיעה כלשהי של תנאי הבקשה ואנו מוותרים בזה מראש על טענות כאמור.
3. הננו מצהירים כי בידינו כל ההיתרים והרישיונות הנדרשים על פי כל דין לביצוע כל התחייבויותינו על פי הבקשה.
4. הננו מצהירים כי ברשותנו ניסיון מוכח בתחום פיתוח ותחזוקה שוטפת של אתר האינטרנט_של 5 שנים לפחות.
5. הננו מצהירים כי אנו עומדים בכל התנאים הנדרשים מהמשתתפים בהליך בקשת ההצעות, כי הצעתנו זו עונה על כל הדרישות שבמסמכי הבקשה. אנו מתחייבים לספק את הפריטים בהתאם לתנאים המפורטים במסמכי הבקשה כולם יחד, לפי הצעת המחיר שהצענו לשביעות רצונה המלא של המכללה.
6. הננו מצהירים כי איננו נמצאים בניגוד עניינים עם המכללה
7. בחתימתנו על מסמכי הבקשה, אנו מצהירים כי כל העובדות והמצגים שניתנו על ידינו במהלך הליך הבקשה, הינם נכונים ומדויקים, לרבות במועד הגשת ההצעה, ויישארו כך בכל מועד עתידי והינם חלק בלתי נפרד מהצעתנו
8. הצעתנו זו היא בלתי חוזרת ואינה ניתנת לביטול, שינוי או תיקון ותהא תקפה ומחייבת אותנו במשך תקופה של 90 יום מהמועד האחרון להגשת הצעות.
9. הננו מצהירים כי הצעתנו זו מוגשת בתום לב וללא הסכם או קשר עם אנשים או גופים אחרים המגישים הצעות למכירת הפריטים/ השירות
10. הננו מצהירים כי הצעתנו הינה בגדר המטרות והסמכויות הקבועות במסמכי התאגיד בשמו מוגשת ההצעה, כי אנו זכאים לחתום בשם התאגיד על הצעה זו וכי אין כל מניעה על פי כל דין או הסכם לחתימתנו על הצעה זו

_____ _____

חתימה וחותמת הספק תאריך

<u>נספח ב' - כתב סודיות וניגוד עניינים</u>

לכבוד :המכללה האקדמית אחוה

אנו מסכימים כי האמור במסמך זה, יחול לגבינו בקשר עם מתן שירותים למכללה, כדלקמן :

1. <u>התחייבות לשמירה על סודיות</u>

1.1 "מידע סודי" או "המידע" – משמעו מידע או חומר מסוגים שונים שנמסרו לנו על ידכם או שיגיעו לידיעתנו, בין באופן ישיר ובין באופן עקיף, בין בכתב בין בעל פה ובין באמצעות מדיה מגנטית או בכל דרך אחרת שהיא, השייך לכם ו/או לצדדים שלישיים שמסרו לכם את המידע, ו/או לצדדים שלישיים אחרים הקשורים אליכם. מידע סודי לא יכלול מידע שניתן להוכיח לגביו ברשומות בכתב כדלקמן : (א) שהוא בגדר "נחלת הכלל" במועד חתימת הסכם זה ו/או שיהפוך לנחלת הכלל שלא עקב מעשה או מחדל שלנו ו/או עקב הפרה של התחייבויות אינו תחת הסכם זה (ב) שהוא הועבר/ יועבר אלינו על ידי צד ג' שאינו חב בחובת סודיות. (ג) שהיה ברשותנו לפני מסירתו על ידי המכללה (ד) שהוא פותח או יפותח על ידנו באופן עצמאי, ללא הפרה של הסכם זה. היה ותופנה אלינו דרישה על פי דין ע"י גורם מוסמך ו/או רשות מוסמכת למסור להם את כל המידע הסודי או חלק ממנו, במישרין או בעקיפין, אנחנו מתחייבים להודיע למכללה על כך מיד בכתב, לפני מסירת כל מידע סודי כאמור, ואם הדבר אינו אפשרי על פי דין, להודיע למכללה על כך מיד לאחר מסירתו, ובכל מקרה, ליתן למכללה אפשרות סבירה להתגונן בטרם מסירת המידע הסודי כאמור ככל ואין באמור משום אי קיום הוראות דין ו/או רשויות החוק. אם לא תצליחו בהליכים כאלה, אנחנו מתחייבים למסור רק את אותו חלק של המידע שיידרש על פי דין בלבד, ולעשות כמיטב יכולתנו על מנת לוודא שיישמר בסודיות.

1.2 אנו מתחייבים לשמור על סודיות מוחלטת, לא להעתיק לא לשכפל ולא לעשות כל שימוש בין בעצמנו ובין על ידי עובדינו, שלוחנו וכל מי מטעמנו, בין במישרין ובין בעקיפין, ולא להביא לידיעת כל אדם או להעביר בכל דרך אחרת כל מידע סודי שנודע לנו או שיוודע לנו במסגרת המו"מ ו/או מתן השירותים על ידינו. על אף האמור לעיל, מובהר ומוסכם בזאת שאנו רשאים לשתף במידע את עובדי משרדנו, לטובת ביצוע השירותים בלבד, בכפוף לאמור סעיף 1.3 להלן. אנו מתחייבים בזאת לנקוט אמצעי זהירות קפדניים ולעשות את כל הדרוש על מנת להבטיח קיום הוראות כתב התחייבות זה גם על ידי עובדינו או מי מהפועלים מטעמנו והכל בכפוף לסעיף 1.2 לעיל .ככל שנדרש, נחתים את עובדנו וכל מי מטעמנו שקשורים במשא ומתן ושעסקו ושיעסקו בביצוע השירותים ,על התחייבות לסודיות בנוסח שיהיה מקובל עליכם.

1.3 אנו מצהירים כי ידוע לנו, שהמידע הוא בבעלותכם ואין לנו ולא תהיה לנו כל זכות בקשר למידע זה, לרבות זכות עיכבון או כל זכות אחרת על פי דין.

1.4 בהתאם לדרישתכם כפי שתועבר אלינו בכתב, אנחנו נעביר את כל המידע שברשותנו בצורה מסודרת, אליכם ולא נשמור בידינו כל מידע שהוא.

1.5 במקרה ונדרש, על פי דין, למסור את המידע ו/או כל חלק ממנו ,אנו מתחייבים להודיע לכם על כך בכתב ומיד, על מנת שתוכלו לשקול נקיטת הליכים משפטיים מתאימים .אם לא תצליחו

בהליכים כאלה ,אנחנו מתחייבים למסור רק את אותו חלק של המידע שיידרש על פי דין בלבד, ולעשות כמיטב יכולתנו על מנת לוודא שיישמר בסודיות בכפוף לאמור בסעיף 1.1 לעיל.

2. <u>התחייבות לאי ניגוד עניינים</u>

2.1 אנו מתחייבים כי במשך תקופת מתן השירותים, לא יווצר מצב בו יהא לנו ו/או למי מטעמנו ו/או מי מעובדינו ניגוד עניינים כלשהו, לרבות בין ענייני המכללה או השירותים הניתנים למכללה על פי הסכם זה, לבין ענייניהם האישיים ו/או המקצועיים שלכם ו/או מי מעובדיכם ו/או מי מטעמכם. אנו מתחייבים להודיע למכללה באופן מיידי, על כל מקרה בו עלול להיווצר ניגוד עניינים כאמור. כמו כן, אנו מצהירים ומתחייבים כי נכון למועד החתימה על הסכם זה, לא קיים ניגוד עניינים כאמור.

2.2 אנו מאשרים כי לא שילמנו ולא נשלם כל תשלום או עמלה, בין בכסף ובין בשווי כסף, לצד שלישי כלשהו, בגין התקשרות בהסכם עם המכללה ומתן השירותים בהתאם להסכם וכי איננו משתפים מי מעובדי המכללה ברווחים.

2.3 כי במשך תקופת ההסכם, אנחנו ו/או מי מטעמנו, לא נקבל, במישרין ו/או בעקיפין, כל תשלום ו/או עמלה ו/או טובת הנאה אחרת ו/או ההבטחה לתשלום ו/או טובת הנאה אחרת מכל צד שלישי ,בקשר ישיר או עקיף עם מתן השירותים על פי הסכם זה.

3. <u>אבטחת מידע</u>

מבלי לגרוע מאלו מהחובות החלות עלינו על פי כל דין ו/או דרישות רשות מוסמכת בכל הנוגע לאבטחת המידע שיגיע לידנו עקב ו/או במהלך ו/או בקשר עם ביצוע השירותים שאנו מעניקים למכללה, אנו מתחייבים לשמור על נהלי אבטחת מידע כפי שתפרסם המכללה מפעם לפעם, ולקיים במלואן את הוראות חוק הגנת הפרטיות. תשמ"א - 1981, והתקנות שהוצאו לפיו, את הוראות והנחיות הרשות להגנת הפרטיות, ואת חוק המחשבים, תשנ"ה- 1995.

4. <u>קניין רוחני</u>

4.1 כל ההצעות, הרעיונות, הדוחות, חוות הדעת, התוכניות, הרשימות, התוכנות, התוצרים וכל חומר שהגיע מהמכללה ו/או שנוצר על ידינו במסגרת מתן השירותים, לרבות חומרים ותוצרים אשר יוכנו על ידי המכללה במסגרת מתן השירותים ו/או ביצוע הפרויקט (להלן: "**החומרים**"), יהיו רכוש המכללה בלבד, ולמכללה תהיינה הזכויות בכל החומרים, לרבות זכויות הקניין הרוחני, זכויות יוצרים וזכויות דומות.

4.2 אנו לא נהיה רשאים להשתמש בחומרים, מבלי לקבל את הסכמת המכללה מראש ובכתב לשימוש על
ידו.

4.3 המכללה רשאית לעשות שינויים, תוספות, השמטות וכו' לפי שיקול דעתה בחומרים.

4.4 אנו מוותרים בזאת על כל זכות תביעה ו/או סעד מכוח קניין רוחני ו/או זכויות יוצרים ו/או

זכות מוסרית בקשר לתוצרים או החומרים הנלווים למתן השירותים.

ולראיה באנו על החתום ביום_____ לחודש_____
שנת_____
חתימה:_____

נספח ג'- נספח ביטוח

לעניין הגדרות נספח ביטוח זה:

"**הספק**" - _____(הספק הזוכה).

"**המזמין**" - המכללה אקדמית אחוה ו/או חברות אם ו/או חברות בנות ו/או חברות אחיות ו/או חברות קשורות ו/או מנהליהם ו/או עובדיהם.

"**השירותים**" - מתן שירותי פיתוח ותחזוקה ושוטפת של אתר האינטרנט עבור מבקש האישור ו/או כפי הגדרתם בהסכם.

נספח זה גובר על כל הוראה בהסכם אשר עניינה ביטוח ובכל מקרה של סתירה בין הוראות ההסכם לבין הוראות נספח זה, יגברו הוראות נספח זה. המונחים המשמשים בנספח זה יפורשו בדרך בה הם מתפרשים בהסכם.

1. מבלי לגרוע מאחריות הספק על פי הסכם זה או על פי כל דין, על הספק לערוך ולקיים, במשך כל תקופת **השירותים**, אצל חברת ביטוח מורשית כדין בישראל, **ובקשר עם ביטוחים שהינם על בסיס מועד הגשת התביעה, למשך תקופה נוספת של 3 שנים לאחר מכן**, את הביטוחים המפורטים להלן ובאישור קיום הביטוחים המצ"ב להסכם זה והמהווה חלק בלתי נפרד הימנו והמסומן כנספח ג'1 (בהתאמה להלן: "**ביטוחי הספק**" ו-"**אישור עריכת הביטוח**"):

1.1. **ביטוח אחריות כלפי צד שלישי** - בגבול אחריות של 1,000,000 ₪ לאירוע ובמצטבר לתקופת הביטוח.

***הביטוח יכלול ביטול חריג סייבר. לחלופין, יערוך הספק ביטוח סייבר, כמפורט להלן.

1.2. **ביטוח חבות מעבידים** - בגבול אחריות של 20,000,000 ₪ לתובע, לאירוע ובמצטבר לתקופת הביטוח.

מוסכם כי ככל שהספק אינו חברה בע"מ ואינו מעסיק עובדים, רשאי הספק שלא לערוך ביטוח זה, בכפוף להתחייבותו לרכוש ביטוח כאמור, ככל שיועסקו עובדים על-ידו, וטרם העסקתם.

1.3. **ביטוח אחריות מקצועית** - בגבול אחריות של 1,000,000 ₪ לאירוע ובמצטבר לתקופת הביטוח.

המבטח את חבות הספק על-פי דין בשל תביעה ו/או דרישה שהוגשה לראשונה במהלך תקופת הביטוח, בגין מעשה או מחדל מקצועי בכל הקשור לשירותים. הביטוח יכלול מועד למפרע אשר לא מאוחר ממועד תחילת השירותים.

***הביטוח יכלול ביטול חריג סייבר. לחלופין, יערוך הספק ביטוח סייבר, כמפורט להלן.

1.4. **ביטוח סייבר** - בגבול אחריות של 1,000,000 ₪ לאירוע ובמצטבר לתקופת הביטוח.

המבטח אבדן או נזק שיגרם לצד שלישי כלשהו עקב אירוע סייבר במערכות המידע של המזמין ו/או הוצאות הנדרשות לצורך שחזור נתונים הנמצאים ברשת של או שבשימוש של הספק, לרבות ומבלי לגרוע מכלליות האמור, אבדן או נזק עקב הפרת הסודיות, פגיעה בפרטיות, השמצה, הוצאת לשון הרע, הוצאת דיבה, גניבת מידע, מרמה ואי יושר עובדים, פגיעה במוניטין, הפרת זכויות קניין רוחני וכן גניבה אובדן או גילוי בלתי מורשה של מידע. הביטוח יכלול מועד למפרע אשר לא מאוחר ממועד תחילת השירותים.

2. הוראות כלליות בדבר ביטוחי הספק:

2.1. הינם קודמים לכל ביטוח הנערך על-ידי המזמין ו/או על ידי בעלי הזכויות הנוספים וכי המבטחים מוותרים על כל טענה ו/או תביעה לשיתוף ביטוחי המזמין.

2.2. אי קיום תנאי הביטוחים בתום לב לא יגרע מזכויות המזמין לשיפוי על פי הביטוחים כאמור.

2.3. היקף הכיסוי (למעט ביטוח אחריות מקצועית) לא יפחת מתנאי מהדורת ביט או דומיו. חריג רשלנות רבתי (אם קיים) יבוטל, אולם אין בביטול כאמור כדי לגרוע מזכויות המבטח וחובות המבוטח על פי דין.

2.4. יכלל סעיף על-פיו מבטח הספק מוותר על זכות התחלוף כלפי המזמין וכלפי הבאים מטעם המזמין, אולם הויתור על זכות התחלוף כאמור לא יחול כלפי אדם שגרם לנזק בזדון.

2.5. "**המזמין**" יכלול גם חברות אם ו/או חברות בנות ו/או חברות אחיות ו/או חברות קשורות ו/או את משתתפי הפעילות נשוא השירותים.

2.6. "**בעלי הזכויות הנוספים**" יכללו את מזמין השירותים ו/או את לקוחות המזמין.

3. טרם תחילת מתן השירותים, על הספק להמציא את אישור עריכת הביטוח, כשהוא חתום בידי המבטח, וכך למשך כל תקופת השירותים, בגין עריכת ביטוחי הספק לתקופת נוספת, וזאת מידי תקופת ביטוח ולפני פקיעת ביטוחי הספק או איזה מהם, וכל עוד מוטלת על הספק החובה לערוך ביטוחים כמפורט בנספח ביטוח זה.

בכל פעם שמבטח הספק יודיע למזמין כי מי מביטוחי הספק עומד להיות מבוטל או עומד לחול בו שינוי לרעה, כאמור בסיפא לאישור עריכת הביטוח, על הספק לערוך את אותו הביטוח מחדש ולהמציא אישור עריכת ביטוח חדש, לפני מועד ביטול הביטוח או השינוי לרעה כאמור.

מוסכם כי בכל מקרה בו יחול שינוי בהוראות המפקח על הביטוח בדבר אישור ביטוח אחיד, רשאי המזמין להחליף את דוגמת נוסח אישור עריכת הביטוח בנוסח חלופי, וזאת בכפוף להתחייבויות הספק בנספח ביטוח זה ובאישור עריכת הביטוח.

4. בכל מקרה של אי התאמה בין אישור עריכת הביטוח החתום לבין הוראות נספח ביטוח זה, ולדרישת המזמין, על הספק לגרום לשינוי האישור על מנת להתאימו להוראות הביטוח נספח ביטוח זה, והכל בכפוף להנחיות המפקח על הביטוח בדבר אישור ביטוח אחיד. מוסכם בזה במפורש כי אין בעריכת ביטוחי הספק, בהמצאת אישור עריכת הביטוח ו/או בבדיקתם ו/או באי בדיקתם ו/או בשינויים, כדי להוות אישור בדבר התאמת ביטוחי הספק לנדרש ו/או בכדי לגרוע מאחריות הספק ו/או בכדי להטיל אחריות כלשהי על המזמין ו/או הבאים מטעם המזמין.

מובהר כי אי המצאת אישור עריכת הביטוח בהתאם להוראות נספח ביטוח זה, לא תגרע מהתחייבויות הספק, ועל הספק לקיים את התחייבויותיו על פי הסכם זה גם אם ימנע מהספק מתן השירותים בשל אי הצגת אישור עריכת הביטוח כאמור. הספק יהיה מנוע מלהעלות טענה ו/או דרישה כלפי המזמין ו/או כלפי מי מטעם המזמין, עקב כך שלא יתאפשר לספק לקיים את השירותים, טרם הומצא אישור עריכת הביטוח כנדרש.

5. מוסכם כי היקף הכיסוי הביטוחי ובכלל זאת גבולות האחריות כאמור בנספח זה ובאישור עריכת הביטוח, הינם בבחינת דרישה מזערית המוטלת על הספק. הספק מצהיר ומאשר כי יהיה מנוע מלהעלות כל טענה ו/או דרישה כלפי המזמין ו/או כלפי מי מטעם המזמין, בכל הקשור לגבולות האחריות האמורים ו/או גובה והיקף הכיסוי כאמור.

היה ולדעת הספק יש צורך בעריכת ביטוחים נוספים ו/או משלימים כלשהם לביטוחי הספק בקשר לשירותים נשוא הסכם זה, רשאי הספק לערוך ולקיים את הביטוח המשלים ו/או הנוסף כאמור. בכל ביטוח רכוש שיערך על-ידי הספק כאמור, ייכלל סעיף בדבר ויתור המבטח על זכות התחלוף כלפי המזמין ו/או כלפי הבאים מטעם המזמין, אולם הוויתור כאמור לא יחול לטובת אדם שגרם לנזק בזדון. מוסכם כי האמור ביחס לביטוחי הרכוש של השוכר כמפורט בנספח ביטוח זה, יחולו גם על הביטוחים הנוספים כאמור.

6. הספק ימלא אחר דרישות והתנאות ביטוחי הספק, יודיע למזמין עם היוודע לו אודות קרות מקרה ביטוח הקשור לשירותים נשוא הסכם זה, ויישא בעלות הביטוחים ובסכומי ההשתתפות העצמית על פיהם.

7. **הספק פוטר את המזמין ו/או את מי מהבאים מטעם המזמין, מאחריות לאבדן או נזק, לרבות אבדן תוצאתי, אשר עלול להיגרם לרכוש ו/או ציוד אשר משמש את הספק לצורך מתן השירותים ו/או שיובא על-ידי ו/או מטעם ו/או עבור הספק לצורך מתן השירותים (ומבלי לגרוע מכלליות האמור, לרבות משאיות, כלי רכב, נגררים וכלי שינוע כלשהם), אולם הפטור כאמור לא יחול לטובת אדם שגרם לנזק בזדון**.

בכפוף לפטור המפורט בסעיף זה לעיל, רשאי הספק שלא לערוך ביטוחי רכוש ואבדן תוצאתי, במלואם או בחלקם, ואולם הפטור יחול כאילו נערכו הביטוחים כאמור במלואם.

8. **בהתקשרות הספק עם גורמים מטעמו במסגרת או בקשר עם השירותים, על הספק מוטלת האחריות לכלול בהסכמי ההתקשרות עימם הוראות ביטוח הולמות, בהתאם לאופי והיקף ההתקשרות עימם. הסכמי ההתקשרות כאמור יכללו במפורש סעיפים לפיהם כל הזכויות בביטוחיהם, כגון וויתור על זכות התחלוף, הרחבות שיפוי, ראשוניות ופטור בגין נזק לרכושם, יוקנו גם לטובת המזמין**.

9. **נספח הביטוח הינו מעיקרי ההסכם והפרתו מהווה הפרה יסודית**. על אף האמור לעיל, אי המצאת אישור עריכת הביטוח במועד לא תהווה הפרה יסודית, אלא אם חלפו 10 ימים ממועד בקשת המזמין בכתב, להמצאת האישור כאמור.

נספח ג'1 - אישור עריכת הביטוח

אישור קיום ביטוחים	תאריך הנפקת האישור:

אישור ביטוח זה מהווה אסמכתא לכך שלמבוטח ישנה פוליסת ביטוח בתוקף, בהתאם למידע המפורט בה. המידע המפורט באישור זה אינו כולל את כל תנאי הפוליסה וחריגיה. יחד עם זאת, במקרה של סתירה בין התנאים שמפורטים באישור זה לבין התנאים הקבועים בפוליסת הביטוח יגבר האמור בפוליסת הביטוח למעט במקרה שבו תנאי באישור זה מיטיב עם מבקש האישור.

מבקש האישור הראשי	גורמים נוספים הקשורים למבקש האישור וייחשבו כמבקש האישור	המבוטח	אופי העסקה והעיסוק המבוטח	מעמד מבקש האישור
שם: המכללה אקדמית אחוה ע"ר	שם: חברות אם ו/או חברות בנות ו/או חברות אחיות ו/או חברות קשורות ו/או מנהליהם ו/או עובדיהם ו/או לקוחות מבקש האישור	שם: _____ (הספק הזוכה)	☐ נדל"ן ☒ שירותים ☐ אספקת מוצרים ☒ אחר: מתן שירותי פיתוח ותחזוקה ושוטפת של אתר האינטרנט עבור מבקש האישור ו/או כפי הגדרתם בהסכם.	☐ משכיר ☐ שוכר ☐ זכיין ☐ קבלני משנה ☒ מזמין שירותים ☐ מזמין מוצרים ☐ אחר: _____
ת.ז./ח.פ.: 580250231	ת.ז./ח.פ.: _____	ת.ז./ח.פ.: _____		
מען: ד.נ. שקמים 79800	מען: _____ תיאור הקשר למבקש האישור הראשי: חברת אם ו/או חברת בת ו/או חברת אחות ו/או חברה קשורה ו/או חברה שלובה ו/או חלק מקבוצה.	מען: _____		

כיסויים

סוג הביטוח חלוקה לפי גבולות אחריות או סכומי ביטוח	מספר הפוליסה	נוסח ומהדורת פוליסה	ת. תחילה (ניתן להזין ת.	ת. סיום (ניתן להזין ת.	גבול אחריות לכלל פעילות המבוטח/ סכום ביטוח		מטבע	כיסויים נוספים בתוקף וביטול חריגים
					לתקופה	למקרה		

צד ג'		ביט			1,000,000	1,000,000	₪	302, 304, 307, 309, 315, 321, 322, 328, 329, 339 - הרחבה לסיכון סייבר 1
אחריות מעבידים		ביט			20,000,000	20,000,000	₪	309, 319, 328, 350
אחריות מקצועית			ת. רטרו _____		1,000,000	1,000,000	₪	301, 302, 303, 304, 309, 321, 325, 326, 327, 328, 332 (06 חודשים) 339 - הרחבה לסיכון סייבר 2
אחר : סייבר		ביט	ת. רטרו _____		1,000,000	1,000,000	₪	301, 302, 303, 304, 309, 321, 325, 326, 327, 328, 332 (06 חודשים)

פירוט השירותים (בכפוף, לשירותים המפורטים בהסכם בין המבוטח למבקש האישור, יש לציין את קוד השירות מתוך הרשימה הסגורה המפורטת בנספח ג' כפי שמפורסם על ידי רשות שוק ההון, ביטוח וחסכון. ניתן להציג בנוסף גם המלל המוצג לצד הקוד ברשימה הסגורה)
043 - מחשוב 088 - שירותי תחזוקה ותפעול 098 - תחזוקת ציוד ורשתות חשמל ותקשורת

ביטול/שינוי הפוליסה
שינוי לרעת מבקש האישור או ביטול של פוליסת ביטוח, לא ייכנס לתוקף אלא 30 יום לאחר משלוח הודעה למבקש האישור בדבר השינוי או הביטול.

[1] ניתן למחוק את הקוד ולחתום על ביטוח סייבר. לחלופין, ככל שנחתם קוד זה, ניתן למחוק ביטוח סייבר.
[2] ניתן למחוק את הקוד ולחתום על ביטוח סייבר. לחלופין, ככל שנחתם קוד זה, ניתן למחוק ביטוח סייבר.

חתימת האישור
המבטח:

נספח ד' - שאלון שביעות רצון לקוחות - (אין למלא נספח זה, ימולא על ידי המזמינה)

שם הלקוח: _____

שם המרואיין: _____

הציונים בטבלאות שלהלן ימולאו על ידי נציגי ועדת המכרזים שמונו לביצוע השיחות, לאחר שיחה טלפונית שיקיימו עם לקוחות המציע.

1. **זמינות במתן השירותים** – האם היית שבע רצון מזמינות המציע באספקת השירותים?

1 נקודות	2 נקודות	3 נקודות	4 נקודות	5 נקודות
כלל לא	במידה מעטה	במידה בינונית	במידה רבה	במידה רבה מאוד

2. **עמידה בתנאי ההתקשרות** – האם השירות שניתן על ידי המציע עמד בדרישות ההתקשרות עימו?

1 נקודות	2 נקודות	3 נקודות	4 נקודות	5 נקודות
כלל לא	במידה מעטה	במידה בינונית	במידה רבה	במידה רבה מאוד

3. **איכות השירות ותוצריו** – האם היית שבע רצון מאיכות השירות ותוצריו?

1 נקודות	2 נקודות	3 נקודות	4 נקודות	5 נקודות
כלל לא	במידה מעטה	במידה בינונית	במידה רבה	במידה רבה מאוד

4. **מקצועיות** – האם המציע הפגין מקצועיות וידע במסגרת מתן השירותים?

1 נקודות	2 נקודות	3 נקודות	4 נקודות	5 נקודות
כלל לא	במידה מעטה	במידה בינונית	במידה רבה	במידה רבה מאוד

5. **שביעות רצון כללית** – האם אתה ממליץ למזמינה להתקשר עם המציע?

1 נקודות	2 נקודות	3 נקודות	4 נקודות	5 נקודות
כלל לא	במידה מעטה	במידה בינונית	במידה רבה	במידה רבה מאוד

שם וחתימת המראיין: _____ **תאריך**: _____

נ

<u>ספח ה'- נספח סודיות, פרטיות ואבטחת מידע</u>

"**ההסכם**") הנחתם בין המכללה האקדמית אחוה (ע"ר) 580363554 כחלק מהסכם השירותים (להלן: (להלן "**נותן השירותים**"), במסגרתו (להלן: "**החברה**"), לבין _____ בע"מ, ח.פ. _____ יספק נותן השירותים לחברה את השירותים כמפורט בהסכם (להלן: "**השירותים**"), יועבר לנותן השירותים מידע אישי ו/או תינתן גישה למידע אישי הכלול במאגרי המידע שבשליטת החברה.

לאור האמור לעיל נותן השירותים מצהיר, מאשר ומתחייב כלפי החברה כדלקמן:

1. ידועים לו כל החוקים, התקנות וכל הוראה אחרת הנוגעים לאספקת השירותים והוא מתחייב למלא אחר הוראות כל דין, לרבות, אך לא רק, חוק הגנת הפרטיות, התשמ"א-1981 והתקנות המותקנות מכוחו, לרבות תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן "**תקנות האבטחה**"), תקנות נוספות ו/או חלופיות שיותקנו מכוחו, הנחיות רשם מאגרי המידע כפי שיעודכנו מעת לעת וכיו"ב.

2. כחלק מיישומו של ההסכם, נותן השירותים יחשף למידע מתוך מאגרי המידע של החברה, עליו חלות הוראות חוק הגנת הפרטיות והתקנות. סוגי המידע אליו יהיה חשוף נותן השירותים ו/או מי מטעמו (בין אם באופן של העברת המידע אליו, או באופן של אפשרות גישה אליו) הוא:

2.1 _____;

2.2 _____;

2.3 _____.

3. לצורך מתן השירותים כאמור בהסכם יהיה רשאי נותן השירותים ו/או מי מטעמו לגשת למערכות מאגרי המידע, כמפורט להלן:

3.1 _____;

3.2 _____;

3.3 _____.

4. נותן השירותים מתחייב לקיים נהלי אבטחת מידע כדין בהתאם להוראות הקבועות בתקנות האבטחה, לרבות נוהל אבטחת מידע כללי, ונהלים בתחומים כדלקמן: אבטחת מידע פיזית וסביבתית; תיעוד ובקרה; אימות, זיהוי וסיסמאות; בקרת גישה וניהול משתמשים; גיבוי ושחזור מידע; התמודדות עם אירועי אבטחת מידע; התקנים ניידים; ניהול כוח אדם הנגיש למידע; עבודה במיקור חוץ; אבטחת תקשורת; ביקורות תקופתיות וכל נוהל אחר הנדרש בהתאם להוראות הדין.

5. נותן השירותים מצהיר, כי אין בביצוע שירותיו וקיום נספח זה (לרבות כל מי מהמועסקים על ידו או מטעמו) כדי ליצור ניגוד עניינים כלשהו, בין במישרין ובין בעקיפין, בינו ובין החברה. נותן השירותים ידווח לחברה בהקדם בכל מקרה שייווצר חשש כלשהו לניגוד עניינים שכזה.

6. מבלי לגרוע מכלליות האמור, נותן השירותים מתחייב שיעשה שימוש במידע האישי המועבר אליו במסגרת ההתקשרות אך ורק למען אספקת השירותים לחברה והמטרות כפי שמוגדרות בהסכם, ומתחייב לעמוד בדרישות אבטחת מידע מקובלות לכל אורך ההתקשרות וכל עוד מידע אישי מצוי

בחזקתו אשר הועבר במסגרת ההתקשרות, להחתים עובדיו על כתב סודיות ביחס להתקשרות, להשמיד את כלל המידע האישי המועבר במסגרת ההתקשרות (להלן: "**המידע**") מיד עם סיומה ולאחר אישור החברה ו/או על-פי דרישתה, לשמור על סודיות המידע בכל עת ולא לעשות בו שימוש מחוץ למסגרת ההסכם וללא אישור החברה בכתב, וכן לאפשר ביצוע פיקוח ובקרה על התנהלותו על ידי החברה ו/או מי מטעמה.

7. נותן השירותים ימסור לחברה כל מידע אשר יידרש ממנו על-ידה בנוגע לאספקת השירותים, אשר מצוי בידו ואשר אין מניעה לגלותו על-פי דין ו/או הסכם, במועד ובאופן שתקבע בסבירות החברה, ובכלל זה דו"חות, נתונים או כל מידע אחר, שיידרש על-ידה מעת לעת ובכלל זה גם בתום תקופת ההסכם.

8. נותן השירותים לא יעסיק קבלני משנה אשר יקבלו ו/או יעשו שימוש ו/או תינתן להם גישה למידע האישי ללא הסכמת החברה מראש ובכתב, למעט ספקי המשנה הקיימים עת חתימת הסכם זה אשר מאושרים מראש, כמפורט להלן:

8.1. _____;

8.2. _____;

9. למען הסר ספק, היה ותאשר החברה בכתב לנותן השירותים לגלות מידע אישי לקבלן משנה של נותן השירותים, הרי שלפני כל גילוי כאמור, יתקשר נותן השירותים בהסכם כתוב, תקף ואכיף עם קבלן המשנה הכולל לכל הפחות הסכם סודיות והסכם לשמירה ואבטחת מידע בתנאים שאינם פחותים במהותם לתנאים המופיעים בהסכם זה. מובהר, כי אין באישור קבלן משנה כדי לגרוע מאחריות נותן השירותים, ונותן השירותים יהיה אחראי לכל מעשה ו/או מחדל של ספק השירותים המשנה מטעמו ולכל הפרה של תנאים אלו על ידי קבלני המשנה מטעמו. מבלי לגרוע מהאמור לעיל, נותן השירותים יוותר האחראי היחיד לפי ההסכם ונספח זה, אף אם ייגרם נזק מכל מין וסוג על-ידי מי מקבלי המשנה שיעסיק ובכפוף לתנאי האחריות והשיפוי בהסכם.

10. מבלי לגרוע מהאמור לעיל, נותן השירותים מתחייב, כי העברת מידע תהא מוגבלת לעובדיו ו/או למי מטעמו אשר להם צורך של ממש ("Need to Know") בקבלת המידע לצורך אספקת השירותים בלבד, ושהובהר להם כי מדובר במידע האישי.

11. נותן השירותים מתחייב לעדכן את החברה בתוך 3 ימים על כל אדם אשר יבקש לעיין ו/או לתקן את המידע אודותיו ו/או את הסרתו מרשימת דיוור מסויימת או בכלל. כל נזק אשר ייגרם לחברה בעקבות חוסר עדכון כאמור יהא באחריותו המלאה של נותן השירותים.

12. נותן השירותים מתחייב, התחייבות בלתי חוזרת לכל אורך תקופת ההסכם לשמור את המידע בסודיות מוחלטת ולא להעביר או לגלות, בין במישרין ובין בעקיפין, בין בתמורה ובין שלא בתמורה, לצד שלישי כלשהו שאינו מורשה לכך במפורש לפי הסכם זה, את המידע אשר הועבר לידיו על-ידי החברה או מידע שהתקבל אגב, בעקבות או למען אספקת השירותים, ללא הסכמת החברה, מראש ובכתב, ולא לעשות כל שימוש במידע למטרה אשר אינה קשורה לאספקת השירותים ו/או ביצוע הסכם זה. עם אספקת השירותים, נותן השירותים מתחייב למחוק כל מידע אישי שקיבל במסגרת ההתקשרות בין הצדדים.

13. נותן השירותים ידווח לחברה מיידית ובכל מקרה תוך לא יאוחר מ-12 שעות מן המועד בו ייוודע לו על שימוש שאינו בהתאם להרשאה במידע של החברה או במערכות הרלבנטיות למידע של החברה, או בעת חשש לאירוע אבטחה כהגדרתו בחוק ו/או בתקנות או בהנחיות הרשות להגנת הפרטיות, ביחס למידע שהגיע מהחברה או קשור לעובדיה ו/או לקוחותיה ו/או למאגר המידע שבשליטתה. נותן השירותים יספק לחברה את כל המידע הדרוש כדי שהחברה תוכל לעמוד בחובות הדיווח המוטלות עליה, לרבות חובת הדיווח לרשות להגנת הפרטיות לנושאי המידע, ככל שיידרש לעשות כן.

14. מבלי לגרוע מכלליות האמור לעיל, המידע שיימסר לחברה על ידי נותן השירותים כאמור לעיל יכלול, בין היתר: (א) תיאור אירוע האבטחה; (ב) הקטגוריות והכמות של נושאי המידע והמידע האישי הקשורים לאירוע האבטחה (ג) שם ופרטי יצירת קשר של נותן השירותים וספקי המשנה מטעמו (ככל שרלוונטי), הממונה/האחראי על אבטחת המידע אצל נותן השירותים או כל גורם רלוונטי אחר אצל נותן השירותים; (ד) תיאור ההשלכות האפשריות של אירוע האבטחה לדעת נותן השירותים; וכן (ה) תיאור הצעדים שננקטו או שהוצעו כדי לטפל באירוע האבטחה, כולל אמצעים למתן את ההשפעות השליליות האפשריות. נותן השירותים ישתף פעולה עם החברה וינקוט באמצעים סבירים כדי למנוע, להקטין ולתקן את אירוע האבטחה וינקוט בכל האמצעים הנדרשים ואת הפעולות המתקנות הנדרשות באופן סביר על-ידי החברה כדי לבחון ולתקן אירועי אבטחה. נותן השירותים יתעד את כל אירועי האבטחה כהגדרתם בחוק (לרבות הנסיבות הנוגעות לאירוע האבטחה, השפעותיו והפעולות המתקנות שננקטו בעקבותיו) באופן הנדרש על מנת לאפשר לחברה לעמוד בדרישות החוק והתקנות.

15. הודעה או דיווח מכל סוג המתייחסים לאירוע אבטחה באופן הקושר את הצדדים, או לכל נתון המאזכר את הצדדים יבוצע על-ידי החברה ולפי שיקול דעתה הבלעדי, אלא אם אושר בכתב אחרת, וזאת למעט ככל שפרסום או דיווח על ידי נותן השירותים נדרש על פי דין.

16. במקרה של פגיעה באבטחת מידע, ידונו הצדדים בענין ויגיעו להסכמה בכל הנוגע לאמצעים הנדרשים לתיקון הפגיעה ולוח הזמנים ליישומם. ככל שנותן השירותים לא עמד בהסכמה כאמור, או שהצדדים לא הצליחו להגיע להסכמה לשביעות רצון החברה, תהיה החברה זכאית לסיים את ההתקשרות עם נותן השירותים באופן מיידי וזאת באמצעות שליחת הודעה בכתב.

17. נותן השירותים ידווח לחברה אחת לשנה על עמידתו בהוראות הדין, ההסכם וכן על אמצעי הבקרה והפיקוח בהם נקט לאורך השנה החולפת, לצורך עמידתו בחובותיו על-פי הסכם זה.

18. נותן השירותים יהיה אחראי לכל נזק אשר ייגרם לחברה, כתוצאה מהפרת הוראות נספח זה וישפה אותה על כך.

19. במקרה של סתירה בין הוראות הסכם מיקור חוץ זה לבין הוראות הסכם ההתקשרות, יגברו הוראות הסכם מיקור חוץ זה, אלא אם כן נאמר אחרת במפורש.

חתימת נותן השירותים: _____

תאריך: ..... שם ותפקיד: ..... חתימה: .....

נספח ו'- הסכם אבטחת מידע

הסכם אבטחת מידע

שנחתם ביום _____ לחודש _____ בשנת _____

בין _____

ח.פ _____

(להלן: "**החברה**")

לבין _____

ח.פ _____

(להלן: "**הספק**")

1. **הנחיות כללית**:

1.1. הספק ישמור את המידע וכן את התשתיות והמערכות המשמשות למתן השירות, במקום מוגן, המונע חדירה וכניסה אליו ללא הרשאה והתואם את אופי הפעילות ורגישות המידע.

1.2. הספק ינקוט אמצעים הולמים לאבטחה הפיזית של המידע וסביבת העבודה, הן במשרדיו והן מחוצה להם, ויימנע מהוצאת עותקים פיזיים של המידע אל מחוץ למשרד, ככל שהדבר אינו הכרחי לצורך מתן השירותים.

1.3. ככל שיעשה שימוש בכלי בינה מלאכותית ומודולי שפה (GAI), הספק מתחייב שלא לעשות שימוש בנתוני החברה לצורך אימון המודל ו/או לחשוף את המידע של החברה בכלים אלה.

1.4. הספק ייתן הרשאות גישה למידע לבעלי ההרשאה מטעמו רק לאחר נקיטת אמצעים סבירים, המקובלים בהליכי מיון ושיבוץ עובדים.

1.5. הספק יקיים הדרכות מודעות בנושאי אבטחת מידע והגנת הפרטיות לבעלי הרשאות גישה למידע מטעמו ובהתאם לתקנה 7 לתקנות אבטחת מידע.

1.6. הספק יישם מידור פנימי בגישה הניתנת על ידו למידע וקבצים של החברה, באופן שהגישה למידע וקבצים אלה תתאפשר רק לבעל הרשאה שעבודתו ותפקידו בחברה מחייבים זאת.

1.7. אופן זיהוי של בעל ההרשאה מטעם הספק למידע של החברה יעמוד בקריטריונים הבאים:

1.7.1. שימוש במדיניות סיסמאות חזקה המורכבת מאותיות וספרות, ובעלת אורך סיסמא מינימלי של 8 תווים.

1.7.2. החלפת סיסמאות לפחות כל 6 חודשים.

1.7.3. הגדרת נעילת משתמש לאחר מספר ניסיונות גישה שגויים (לכל היותר 5 ניסיונות). שחרור הנעילה יתבצע על ידי גורם מורשה מטעם הספק.

1.7.4. הגדרת Session Time Out לאחר פרק זמן של אי פעילות, המחייב זיהוי מחדש של המשתמש. ברירת המחדל לסיום Session תהיה 30 דקות.

1.7.5. גישת אדמין (מנהל מערכת) תהיה באמצעות אימות רב שלבי (MFA).

1.7.6. בגישה מרחוק, באמצעות רשת האינטרנט או רשת ציבורית אחרת, הספק יעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של בעל ההרשאה שמטרתו לזהות את המתקשר והמאמת את הרשאתו לביצוע הפעילות מרחוק ואת היקפה (לדוגמה: OTP, גישה מכתובת IP קבועה, Token, וכיו"ב).

1.7.7. הספק יבצע בקרת הרשאות תקופתית לבעלי ההרשאות מטעמו לפחות אחת לשנה.

1.7.8. מיד עם סיום תפקידו של בעל ההרשאה מטעם הספק, הספק יבטל את הרשאותיו.

1.8. הספק ינקוט באמצעי אבטחה הולמים, בהתאם לרמת רגישות המידע, שימנעו חדירה מכוונת או מקרית למערכת או אל קווי התקשורת בין החברה אל הספק (מערכות הגנה, Fire Wall וכיו"ב) ולכל הפחות:

1.8.1. הגבלת או מניעת אפשרות חיבור התקנים ניידים לעמדות קצה ו/או שרתים המכילים את המידע של החברה.

1.8.2. התקנת תוכנת הגנה תקנית ומעודכנת נגד נוזקות על מחשבים המשמשים למתן השירות.

1.8.3. הספק יפריד, ככל הניתן, בין המערכות אשר ניתן לגשת מהן למידע שבמאגר, לבין מערכות מחשוב אחרות שמשמשות את הספק.

2. **אירועי אבטחת מידע:**

2.1. הספק יתעד אירועי אבטחת מידע, ככל האפשר באמצעות רישום אוטומטי בלוג.

2.2. הספק מתחייב לדווח לחברה באופן מידי בכל מקרה של חשש לאירוע אבטחת מידע או שימוש חורג מההרשאה שניתנה לספק ו/או למי מטעמו.

2.3. ההודעה תכלול לכל הפחות תיאור של האירוע, המס' המשוער של נושאי המידע המעורבים באירוע, תיאור ההשלכות האפשריות של האירוע, האמצעים שננקטו לטיול באירוע.

2.4. במקרה של אירוע אבטחת מידע, הספק מתחייב לספק מענה מיטבי והולם, כך שזמן החזרה לכשירות וזמינות המידע יהיה בצורה המהירה ביותר, בהתאם לאמנת השירות (להלן: "SLA") שהוגדרה בין הצדדים.

2.5. הספק יספק מענה אנושי (לא אוטומטי) לטיפול באירועי סייבר.

3. **מדיניות פרטיות ואופן שימוש בעוגיות (ככל שהמערכת כוללת ממשק משתמש קצה ב-WEB)**

3.1. ידוע לספק כי עליו לגבש את מדיניות הפרטיות ואת אופן שימוש בעוגיות יחד עם החברה. למען הסר ספק, לא תתכן עלייה לאוויר טרם אישור נוסח מדיניות הפרטיות ואופן שימוש בעוגיות על ידי החברה.

4. **דרישות מערכת ופיתוח) ככל שמדובר בספק אשר מפתח מערכת עבור החברה):**

4.1. פיתוח המערכת ועדכוניה יבוצעו בכפוף לנוהל פיתוח מאובטח (SSDLC) המבוסס על תקן OWASP עדכני או תקן מקביל שיאושר ע"י החברה.

4.2. פיתוח המערכת יתבסס על גרסאות מעודכנות ונתמכות של שפות הפיתוח.

4.3. <u>ספריית קוד פתוח</u>:

4.3.1. הספק מתחייב להטמיע תהליך סדור לניהול רכיבי קוד פתוח (Open Source Software Management) לאורך כל מחזור חיי הפיתוח (SDLC), הכולל שימוש בכלי סריקה אוטומטיים (SCA) לזיהוי חולשות אבטחה (CVEs) וחריגות ברישוי.

4.3.2. כחלק מדרישה זו, על הספק לייצר, לתחזק ולספק ללקוח בכל גרסה רשמית ו/או הפצת עדכון, קובץ Software bill of Materials (SBOM) פורמט סטנדרטי (כגון CycloneDX או SPDX), המפרט את כלל רכיבי הצד-השלישי שלהם.

4.3.3. הספק מתחייב לנטר באופן רציף את הרכיבים המופיעים ב-SBOM, לבצע ניתוח סיכונים תקופתי, ולהחיל עדכוני אבטחה או תיקונים (Patches) בהתאם ללוחות הזמנים המוגדרים במדיניות הטיפול בחולשות של החברה.

4.3.4. במידה ותתגלה חולשת אבטחה קריטית או גבוהה ברכיב קוד פתוח הנמצא בשימוש, הספק מתחייב ליידע את החברה בכתב ובעל פה, מיידית עם גילוי החולשה.

4.4. פיתוח המערכת בהתאם למסמך דרישות האפיון שאושר מראש על ידי החברה. במקרה של מערכת מדף (As Is), כל תוספת הדורשת פיתוח, תעמוד בכללי פיתוח מאובטח והוראות החברה.

4.5. בשימוש בספריות צד ג׳ , קוד פתוח או לאחר רכישה, יש לוודא עמידה בדרישות אבטחת המידע גם שלהם.

4.5.1. הספק מחויב לוודא שכל רכיב קוד פתוח שבו נעשה שימוש, הינו בעל רישיון המאפשר שימוש מסחרי.

4.5.2. חל איסור להשתמש בספריות שהופסקה תחזוקתן או שהתגלו בהן חולשות אבטחה חמורות ללא תיקון רשמי.

4.5.3. חל איסור על שימוש בספריות קוד פתוח בלתי מאומתות ממקורות שאינם רשמיים

4.5.4. יש לנהל מדיניות עדכון ספריות שמבטיחה שהגרסאות יהיו תמיד עדכניות, נתמכות וללא חולשות אבטחה קריטיות.

4.6. לא יעשה שימוש בנתונים אמיתיים בסביבת הפיתוח.

4.7. ביצוע בדיקות מסירה ע״י הספק לווידוא קיום דרישות אבטחת מידע באפיון.

4.8. הפקדת קוד המקור אצל החברה או אצל נאמן, בהתאם להסכמה בין הצדדים.

4.9. המערכת תכלול הפרדה בין הנתונים של החברה לבין נתונים של לקוחות אחרים. הפרדה כאמור יכולה להיות לוגית, תוך מתן הסבר לחברה על אופן ההפרדה.

4.10. יישום הגנות על בסיס הנתונים והקשחות עפ״י הנחיות היצרן.

4.11. המערכת תכלול רכיב ניטור שינויים בבסיסי הנתונים ויכולת הפקת דו״ח לפי דרישת החברה.

4.12. שימוש במערכות הפעלה, דפדפנים, בסיסי נתונים ותשתיות תוכנה בגרסאות נתמכות בלבד. לא ייעשה שימוש במערכות שהיצרן לא תומך בהיבטי אבטחה שלהן אלא אם כן ניתן מענה אבטחתי מתאים.

4.13. המערכת תייצר יומן רישום (log) לנתוני האבטחה הבאים: זיהוי ואימות; נעילות משתמש; פעולות עדכון ע״י המשתמשים כולל שמירת ערך קודם; העלאות תכנים; גישה מרחוק; אירועי אבטחה.

4.14. המערכת תכיל ממשק API למערכת ניטור מרכזית (כגון SIEM).

4.15. תתבצע החלפה תקופתית של מפתחות ההצפנה, ובפרט של API&Host keys, זאת לצורך שמירה על סודיות, שלמות ואמינות המידע.

4.16. במידת הצורך ועבור מתן מענה ראוי לאתגרי וסיכוני אבטחה רלוונטיים, המערכת תכלול אפשרות לשימוש בטכנולוגיות הצפנה נוספות, כדוגמת- Anonymization, Masking וכן Tokenization.

4.17. הספק ידווח לגורם הרלוונטי בחברה על כל השבתה של המערכת.

4.18. העברת המערכת מסביבת פיתוח לייצור בצורה מבוקרת ולאחר ביצוע מבדק חדירה וטיפול בממצאי המבדק.

4.19. ביצוע סקר סיכונים ומבדק חדירה, אחת ל-18 חודשים לכל הפחות.

4.20. המערכת תעבור סקר קוד (Code review), ובקרת הפעלה בהיבטי אבטחת המידע לפני שתועבר לסביבת הייצור, וכן באופן תקופתי.

4.21. <u>הזדהות וניהול הרשאות במערכת:</u>

4.21.1. עבור מערכת שאינה מאוחסנת בשרתי החברה והגישה אליה מרוחקת, כלל הגישה למערכת, הן עבור משתמשי אדמין והן עבור משתמשים רגילים, תהיה באמצעות אימות רב שלבי (MFA).

4.21.2. אפשרות לניהול הזהויות דרך ה-Directory של החברה.

4.21.3. שימוש במדיניות סיסמאות חזקה המורכבת מאותיות וספרות, ובעלת אורך סיסמא מינימלי של 8 תווים.

4.21.4. החלפת סיסמאות לפחות כל 6 חודשים.

4.21.5. הגדרת מספר ניסיונות הקשה שגויים של סיסמא בטרם נעילת המשתמש (לכל היותר 5).

4.21.6. הגדרת Session Time Out לאחר פרק זמן של אי פעילות, המחייב זיהוי מחדש של המשתמש. ברירת המחדל לסיום Session תהיה 30 דקות.

4.21.7. הצפנת הסיסמאות בהצפנה חד כיוונית בבסיס הנתונים.

4.21.8. יישום תיעוד לכל שינוי בטבלת ההרשאות.

4.21.9. הגדרת אופן טיפול בתקלות הקשורות באימות זהות.

4.22. <u>המערכת תכיל בקרות קלט ופלט כמפורט להלן:</u>

4.22.1. וידוא שאין בדו"חות המופקים מהמערכת חשיפה של שדות שלא נדרשים.

4.22.2. שימוש בפרוטוקול HTTPS בכל דפי היישום.

4.22.3. הגדרת רשימת ערכים וטווחים מותרים לשדות קלט (כולל CAPTCHA).

4.22.4. מניעת אפשרות למניפולציה של כתובת ה-URL (חסימת אפשרות לשינוי UID בסוף הדף, חסימת שינוי או הוספת דפי משנה).

4.22.5. מניעת חשיפה עבור משתמש הקצה להודעות שגיאה אפליקטיביות העלולות להסגיר קוד וטבלאות בתוך היישום. שגיאות כאלה יש לכתוב לקובץ לוג בלבד או לתת הודעה גנרית.

4.22.6. במקרה של העלאת קבצים למערכת: ווידוא כי קובץ העולה לשרת יעבור סניטציה ויישמר בשרת כקובץ בעל סיומת לא פוגענית כגון html ו/או php.

4.22.7. מתן אפשרות לחברה לשינוי / עדכון שדות מידע בודדים.

4.23. <u>שילוב יכולות AI בפיתוח (ככל שנעשה שימוש בכלי AI)</u>

בעת שימוש במודלי AI או קריאות API לפתרונות AI ושילובם בתהליכי הפיתוח ו/או השימוש במערכת, יושמו כללי האבטחה הבאים:

4.23.1. קריאה למערכת ה-AI לא תאפשר העברת מידע אישי ו/או עסקי של החברה למערכת ה-AI, בצורה בה המידע הנ"ל יכול לשמש לאימון ולימוד המודלים.

4.23.2. השימוש במודלים יבוצע כך שהמידע עליו אומנו המודלים יכלול מידע חיצוני, אבל כל מידע המועבר למערכת, יישאר בתחום המידע המאובטח והמוגן בהתאם למדיניות ניהול הגנת המידע של החברה.

4.23.3. פיתוח המערכת יבוצע לאחר אפיון הכולל התייחסות לאבטחת המידע בפיתוח פתרונות המשלבים כלי AI.

4.23.4. האפיון יכלול את ניתוח הסיכונים, הגדרת מענה הולם לכל סיכון.

4.23.5. האפיון יכלול טיפול בנושאי האבטחה לכל אורך חיי המערכת, כולל בטיפול בבאגים ופעילות שינויים ושיפורים.

4.23.6. באחריות הספק להפעיל מנגנון QA שיבחן גם את המענה לסיכוני האבטחה שהוגדרו באפיון.

4.23.7. שימוש במודלים חיצוניים מחייב אפשרות לעדכוני גרסאות וטיפול בחולשות אבטחה המתגלות מעת לעת.

4.23.8. הספק מתחייב לפתח את המערכת בהתאם לסטנדרטים המקובלים בתעשייה, ובהם הנחיות מערך הסייבר הלאומי בהקשר של פיתוח מאובטח של מוצרי בינה מלאכותית.

4.23.9. הספק מתחייב שמפתחות ההצפנה של הקוד לא יעלו לענן ו/או לכלי ה-AI.

5. **<u>אחסון (ככל שמדובר בספק שמאחסן את המערכת עבור החברה):</u>**

5.1. הספק לא יחבר את מערכות המאגר לרשת האינטרנט או לרשת ציבורית אחרת, ללא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש.

5.2. הספק יוודא במערכות ההגנה, חסימת תעבורה ממדינות עוינות ו/או מקורות הידועים כבעלי מוניטין בעייתי ו/או עוין. ככל הניתן, יחסמו מקורות TOR ו- Anonymizer המאפשרים גלישה אנונימית.

5.3. הספק יגדיר נוהל בדיקה שגרתי של יומני הרישום (Logs) למנגנון הבקרה, כמפורט בסעיף 39.13 להסכם זה, כולל דו"ח של הבעיות שהתגלו והצעדים שננקטו בעקבותיהן.

5.4. הספק ישמור את יומני הרישום הללו באופן מאובטח, למשך 24 חודשים, לכל הפחות.

5.5. הספק יגבה את נתוני האבטחה באופן שיבטיח את האפשרות לשחזרם למצבם המקורי.

5.6. הספק יגדיר נוהל לביצוע גיבויים ושחזורים של נתוני האבטחה באופן תקופתי ושגרתי.

5.7. <u>עבור אחסון בשירותי ענן:</u>

5.7.1. ככל שמיקומה הגיאוגרפי של פעילות הענן הינה מחוץ לגבולות מדינת ישראל, הנ"ל יתבצע תוך עמידה בתקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001, וכן כל תקן ו/או רגולציה נדרשת אחרת.

5.7.2. הספק יעשה שימוש ב-WEB SERVICE או STORED PROCEDURES על מנת למנוע ממשק ישיר בין המשתמש לשרת בסיס הנתונים.

5.7.3. ממשק ניהול בגישה מהרשת המקומית בלבד או מכתובות שיסופקו על ידי החברה (Trusted / Secured Host).

5.7.4. רכיב Firewall מסוג NGFW לרבות מימוש IPS. במקרה שמדובר באפליקציה המצויה בענן ושניתן לגשת אליה מכל מקום בעולם (Publicly available) נדרש גם התקנה והטמעה של WAF. מימוש הצפנה בתקשורת באמצעות פרוטוקולTLS1.2 ומעלה או פרוטוקול אחר שיאושר ע"י החברה.

5.7.5. נדרשת הצפנת שדות מידע רגיש ברמת ה-DB.

5.7.6. נדרשת הצפנת Data at rest ברמת ה-Volume (עבור אחסון אובייקטים).

5.7.7. לצורך מתן מענה לאתגרי וסיכוני "נעילה" (Vendor lock-in) במסגרת חברת שירותי הענן הקיימת, יתבצע תיעוד כלל הממשקים וה-API אשר נעשה בהם שימוש, וכן גיבוי תקופתי של המידע הקיים בסביבת הענן לסביבת צד ג' אחרת. האמור מתייחס גם ל-Meta Data הרלוונטי.

5.7.8. הספק יספק לחברה יכולת שליטה ובקרה על הנתונים בענן וכן אפשרות חד צדדית להפסקת השימוש בשירותי הענן תוך מחיקת המידע באופן שלא ניתן לאחזור.

6. **<u>דרישות אבטחת מידע לסביבת ענן SaaS מרובת-דיירים (Multi-Tenant)</u>**

6.1. <u>תקנים, הסמכות וציות (Compliance): הספק מתחייב כי סביבת הענן ושירות ה-SaaS יעמדו, לכל הפחות, בדרישות הבאות (ככל שרלוונטי לשירות):</u>

6.1.1. החזקת הסמכה תקפה ISO/IEC 27001 (או שוות ערך) עבור היקף הכולל את השירותים הניתנים לחברה, או חלופה: דוח SOC 2 Type II.

6.1.2. התחייבות לעמידה ב-ISO/IEC 27017 (בקרות אבטחה לשירותי ענן) ו-ISO/IEC 27018 (הגנת מידע אישי בענן) או בקרות מקבילות.

6.1.3. לפי דרישת החברה, הספק יספק אחת לשנה אישורים/דוחות עדכניים (למשל: תעודת ISO, דוח SOC, תקציר ממצאים ותוכנית טיפול) וכן ימסור מענה לשאלון אבטחת מידע.

6.2. <u>הפרדת דיירים (Tenant Isolation) והגנה מפני משתמשים/לקוחות אחרים:</u>

6.2.1. המערכת תספק הפרדה ברורה בין נתוני החברה, משתמשיה ותהליכיה לבין נתונים ותהליכים של לקוחות אחרים, כך שלא תתאפשר גישה, חשיפה, שאילתא, תצוגה, שינוי או מחיקה של נתוני החברה על ידי משתמשים/תהליכים שאינם שייכים לחברה.

6.2.2. יישום הפרדה ב-Application layer וב-Data layer (לכל הפחות לוגית), עם מנגנון אימות שיוך Tenant בכל קריאה/שאילתא.

6.2.3. איסור מוחלט על שימוש בהרשאות רוחביות/משותפות (למשל shared admin) בין לקוחות, למעט הרשאות תשתית מבוקרות של הספק לצורכי תפעול, בכפוף ל-logging וניהול גישה Just-In-Time ככל שניתן.

6.2.4. ביצוע בדיקות תקופתיות למניעת כשלים מסוג IDOR/גישה חוצה-דיירים, כולל בדיקות authorization ברמת object לכל משאב.

6.2.5. במקרה של חשד/אירוע חשיפת נתונים בין דיירים – הודעה מיידית לחברה, ביצוע containment, תחקור שורש, והצגת post-mortem ותוכנית מניעה.

6.3. <u>ניהול זהויות והרשאות (IAM): הספק יעמיד יכולות ניהול זהויות והרשאות המותאמות לסביבת SaaS מרובת משתמשים, לרבות:</u>

6.3.1. תמיכה ב-SSO באמצעות SAML 2.0 ו/או OIDC, והגדרת MFA לכל משתמשי אדמין ולפי מדיניות החברה גם למשתמשים רגילים.

6.3.2. מודל הרשאות RBAC (ולפי הצורך ABAC) עם עקרון הרשאות מינימליות (Least Privilege), אפשרות להפרדת תפקידים (SoD) ומיפוי הרשאות ברמת אובייקט/ישות.

6.3.3. תמיכה ב-SCIM או מנגנון מקביל לאספקת/הסרת משתמשים אוטומטית (Provisioning/Deprovisioning).

6.3.4. ניהול הרשאות אדמיניסטרציה עם תיעוד מלא (מי/מה/מתי), כולל פעולות רגישות (הקצאת הרשאות, יצוא נתונים, מחיקה, שינוי הגדרות אבטחה).

6.4. <u>הצפנה וניהול מפתחות: הספק יישם הצפנה מקצה לקצה, בהתאם למקובל בתעשייה, לרבות:</u>

6.4.1. הצפנה בתקשורת (in transit) בפרוטוקול TLS 1.2 ומעלה, עם ניהול תעודות (certificates) תקין וחידוש מבעוד מועד.

6.4.2. הצפנת נתונים במנוחה (at rest) לרבות בסיסי נתונים, גיבויים ולוגים.

6.4.3. ניהול מפתחות באמצעות KMS/HSM, הפרדת תפקידים למשתמשי מפתחות, ורוטציה תקופתית של מפתחות.

6.4.4. ככל שנדרש על ידי החברה: אפשרות BYOK / HYOK או חלופה מוסכמת, לרבות תיעוד תהליך החלפה/ביטול מפתחות והשפעתו על זמינות השירות.

6.5. <u>אבטחת API ואינטגרציות: ככל שהמערכת מספקת ממשקי API ו/או ממשקי אינטגרציה (לרבות אפליקציות מובייל/עמדות טעינה/צדדים שלישיים), יחולו הדרישות הבאות:</u>

6.5.1. אימות והרשאות ל-API באמצעות OAuth2 ו/או חתימות/מפתחות, עם הפרדה בין מפתחות ללקוח/דייר, ותוקף/רוטציה.

6.5.2. יישום הגנות Rate limiting, מניעת abuse, וחסימת Brute force בהתאם לסיכון.

6.5.3. הקשחת API Gateway / WAF, ולכל הפחות הקפדה על בקרות קלט/פלט ומניעת OWASP API Top 10.

6.5.4. הפרדת סביבות ומפתחות בין Production, Staging ו-Dev, ואיסור שימוש במפתחות ייצור בסביבת פיתוח.

6.6. <u>לוגים, ניטור וזיהוי חריגות: הספק יפעיל מנגנוני ניטור וזיהוי אירועים בסביבת הענן, ויאפשר לחברה לקבל נתונים/דוחות בהתאם לצורך, לרבות:</u>

6.6.1. תיעוד פעולות משתמשים ואדמינים (כולל פעולות גישה, שינוי הרשאות, יצוא/הורדה, מחיקה, שינוי תצורה), באופן שמאפשר Audit trail מלא.

6.6.2. הפרדת לוגים בין "דיירים", כך שלקוחות אחרים לא יוכלו לצפות/להפיק לוגים הקשורים לחברה.

6.6.3. שמירת לוגים לתקופה שלא תפחת מ-24 חודשים (אלא אם נדרש אחרת על ידי החברה/דין), או אפשרות יצוא/Forwarding ל-SIEM של החברה, ככל שהדבר נתמך טכנית.

6.6.4. הפעלת התראות על חריגות (למשל: ניסיונות כניסה כושלים רבים, פעולות יצוא חריגות, שינויי הרשאות, גישה ממדינות/כתובות חריגות) והליך טיפול מובנה.

6.7. <u>ניהול פגיעויות, עדכונים ורכיבי צד ג': הספק יפעיל תהליך סדור לניהול פגיעויות בשירות, לרבות:</u>

6.7.1. סריקות פגיעויות תקופתיות לתשתית וליישום (כולל תלויות קוד), ומדיניות תיקון לפי רמות חומרה (למשל Critical/High/Medium) עם זמני תיקון מוסכמים.

6.7.2. מדיניות Patch management לתשתיות ענן, מערכות הפעלה, מסדי נתונים, רכיבי containers וספריות.

6.7.3. ביצוע בדיקות חדירה חיצוניות לשירות (או לכל הפחות לרכיבים החשופים לאינטרנט) אחת לשנה, ושיתוף תקציר ממצאים ותוכנית טיפול לפי דרישת החברה.

6.7.4. לפי דרישת החברה: אספקת SBOM (רשימת רכיבי תוכנה) עבור רכיבי המערכת, או פירוט תלויות מהותיות וגרסאות.

6.8. <u>זמינות, גיבויים והתאוששות מאסון (BCP/DR): הספק יבטיח תפעול רציף של שירות ה-SaaS בהתאם ל-SLA, ובכלל זאת:</u>

6.8.1. גיבויים תקופתיים מוצפנים של נתוני החברה, כולל בדיקות שחזור (restore tests) בתדירות סבירה.

6.8.2. הגדרת יעדי התאוששות RPO/RTO לשירות, והצגתם לחברה לפי דרישה.

6.8.3. תחזוקה מתוכננת תבוצע בהודעה מראש, ותכלול צעדי הפחתת סיכון (rollback) ככל הניתן.

6.9. מיקום נתונים, עיבוד בענן וספקי משנה: מבלי לגרוע מהוראות נספח זה ביחס להעברת מידע מחוץ לישראל, יחולו גם ההוראות הבאות:

6.9.1. הספק יפרט לחברה (לפי דרישה) את אזורי האחסון/עיבוד (Regions) ואת מיקום הגיבויים, וכן את רשימת ספקי המשנה המשמעותיים בשירות.

6.9.2. הספק לא ישנה מהותית את מיקום העיבוד/האחסון ו/או ספקי משנה מהותיים ללא הודעה מראש לחברה, ובמקרים רלוונטיים – קבלת אישור החברה.

6.9.3. כל ספק משנה המעורב בעיבוד מידע של החברה יחוייב בהתחייבויות אבטחת מידע והגנת פרטיות שאינן נופלות מהותית מהתחייבויות נספח זה.

6.10. הפרדת סביבות ותמיכה תפעולית (Support Access): הספק יבטיח כי עבודת הפיתוח/בדיקות/תמיכה לא תסכן את סודיות המידע וזמינות השירות:

6.10.1. הפרדה בין סביבות Dev/Test/Staging/Prod, כולל הפרדת הרשאות ומפתחות, וניהול שינויים מבוקר בסביבת ייצור.

6.10.2. איסור שימוש בנתונים אמיתיים של החברה בסביבות שאינן ייצור, אלא אם התקבל אישור מראש ובכתב מהחברה ובוצעו אמצעי הגנה (אנונימיזציה/מיסוך) בהתאם לצורך.

6.10.3. גישה תפעולית של נציגי הספק למידע (לצרכי support) תתבצע רק לצורך מוגדר, בהרשאות מינימליות, לתקופה מוגבלת, תוך תיעוד מלא ויכולת הצגת דוח לחברה לפי דרישה.

6.11. מחזור חיי מידע (Data Lifecycle) לשם שמירה על פרטיות וצמצום סיכונים בסביבת SaaS, יחולו ההוראות הבאות:

6.11.1. הספק יאפשר יצוא נתוני החברה בפורמט סביר ומקובל (למשל CSV/JSON) לפי דרישה סבירה, ובכפוף להרשאות מתאימות.

6.11.2. מחיקת נתוני החברה בסיום התקשרות תכלול גם מחיקה ממערכות גיבוי/שחזור בהתאם למדיניות מחזור חיים מתועדת, בתוך פרק זמן מוסכם, ותוך העברת אישור מחיקה לחברה לפי דרישה.

6.11.3. הגדרת תקופות שמירה (Retention) ללוגים/גיבויים/דוחות ותהליכי Purge תקופתיים.

ולראיה באתי על החתום:

שם + שם משפחה _____ תפקיד _____

תאריך _____ חתימה + חותמת הספק _____

נספח ו'1- שאלון ספק

שאלות עבור כלל הספקים	**כללי**	האם מוגדר אצל הספק גורם האחראי לאבטחת המידע והגנה בסייבר?
		האם מיושמות תקנות הגנת הפרטיות (אבטחת מידע) - התשע"ז, 2017?
		האם לספק קיימים הסכמי סודיות ואבטחת מידע עם ספקים שלו (ספקי משנה)?
		האם לספק קיימים תקני אבטחה ופרטיות (אם כן, נא לפרט)?
	משאבי אנוש	האם מתקיימות בדיקות מהימנות / רקע בתהליכי גיוס עובדים, ובמהלך תפקודם?
		האם כלל עובדי הספק חתומים על הסכם סודיות מול הספק?
	הזדהות וניהול הרשאות	האם מדיניות בקרת הגישה אצל הספק כוללת את יישום עקרון המידור, לפיו עובד ייחשף אך ורק למידע אשר הוא נדרש לו לצורך מילוי תפקידו ועקרון של מתן הרשאות מינימליות?
		האם השימוש במשתמשים בעלי הרשאות חזקות / גבוהות מוגבל למינימום הנדרש?
		האם קיים תהליך לבקרת הרשאות תקופתית?
		האם זיהוי משתמש נעשה על בסיס אמצעי פיזי/FA/MFA2?
	מדיניות סיסמאות של עובדי הספק	האם מוגדרת מדיניות סיסמאות חזקה (מינימום תווים, היסטוריית סיסמאות, מורכבות וכו') למחשבים ומערכות הספק ?
		האם מוגדרת מדיניות נעילת משתמשים לאחר מספר ניסיונות גישה כושלים למחשבי ומערכות הספק ?
	גישה מרחוק וגישה למערכות ניהול	האם גישה מרחוק למערכות/מחשבי הספק ומערכות ניהול של הספק, מתבצעת באמצעות אימות דו/רב שלבי (FA/MFA2)?
		האם חיבור מרחוק/חיבור למערכות ניהול של הספק/חיבור למערכות המכילות מידע של החברה מתבצע באמצעות – משתמש אישי לכל עובד?
		האם הספק משתמש באמצעי אבטחה (אימות דו שלבי/רב שלבי) לצורך מתן גישה מרחוק למאגרי המידע של לקוחותיו?
		במידה ורלוונטי לפעילות הספק - האם קיימת מדיניות מחמירה למניעת גישה אל מול מידע רגיש של המכללה, אשר דורשת בין היתר ולכל הפחות: הזדהות חזקה (MFA), גישה וזיהוי חד ערכי, אי הכחשה, גישה מכתובת מוגדרת ומוגבלת, הגבלת גישה מרחוק לפי רשימת כתובות של החברה, מנגנון הזדהות חזק יותר (כולל מדיניות סיסמאות חזקה יותר) וכו'?

	ניהול מאובטח בתשתיות המחשוב של הספק	האם קיים נוהל להגנה על תחנות קצה ושרתים (כולל הקשחה, אמצעי הגנה, הגבלת גישה וכו')?
		האם ברשת הספק קיימת סגמנטציה ברמת התקשורת בין מרכיבים שונים (דוגמת – שרתים, תחנות קצה, מצלמות, מדפסות וכו')?
		האם קיימת מדיניות עדכוני אבטחה למערכות הפעלה, דפדפנים, בסיסי נתונים ותשתיות תוכנה?
		האם נעשה שימוש בפתרון EPP/EDR/XDR/MDR/NDR כדי להגן על תחנות קצה ושרתים? אם כן מאיזה סוג?
	אבטחת תקשורת	האם קיים שימוש באמצעי אבטחה מקובלים (בהתאם לרמת רגישות המידע), שימנעו חדירה מכוונת או מקרית לתשתיות התקשורת של הספק (לכל הפחות - Firewall ו-IPS, הצפנה בפרוטוקול TLS 1.2 ומעלה)?
		האם הספק עושה שימוש במערכות ההגנה להגנת על אפליקציות ושירות WEB (כגון WAF)?
	ביקורת תקופתית	האם נערכת ביקורת פנימית או חיצונית, לעניין עמידת הספק בתקנות אבטחת מידע וניהול סיכוני אבטחת מידע?
		האם נערכים סקרי סיכונים ובדיקות חדירה אחת ל-18 חודשים לכל הפחות? אם כן, מתי בוצעו סקר הסיכונים ו/או מבדק החדירה לאחרונה?
	אירועי אבטחה	האם קיימים לוגים והתראות על חשד לאירועי אבטחה ממערכות ניהול המשתמשים ומערכות ההגנה ?
		האם קיים נוהל אבטחה לעניין התמודדות עם אירועי אבטחת מידע וסייבר והתאוששות מאירוע כאמור, לפי חומרת האירוע ומידת רגישות המידע, לרבות לעניין ביטול הרשאות וצעדים מיידיים אחרים הנדרשים וכן הוראות לעניין דיווח למנהל אבטחת המידע של החברה על אירועי אבטחה ועל הפעולות שננקטו בעקבותיהם?
		במידה וקיים נוהל, האם מתקיים דיון תקופתי בנושא אירועי?
		האם קיים תיעוד אירוע אבטחת מידע באופן מאובטח ולמשך 24 חודשים לכל הפחות?
<u>שאלות עבור ספקים אשר מאחסנים מערכות של המכללה</u>	**כללי**	האם קיימת הפרדה בין מערכות הספק אשר ניתן לגשת מהן למידע רגיש של המכללה, לבין מערכות מחשוב אחרות שמשמשות את הספק?
		האם קיימת הפרדה בין בסיס הנתונים של החברה לבין בסיסי נתונים של חברות אחרות?
		האם קיימות יכולות ניטור שינויים בבסיסי הנתונים והפקת דוח למנהל אבטחת המידע של החברה לפי דרישתו?
		האם לספק יש תרשים רשת מעודכן?

	בקרה ותיעוד גישה	האם קיים לוג מסודר והתראות מהמערכות הבאות? : AD/Entra/LDAP Services מערכות גישה מרחוק (VPN/VDI/ZTNA) PAM/SSO/IDM (במידת הרלוונטיות) SQL (במידת הרלוונטיות) Application (במידת הרלוונטיות) AV/EPP/EDR/XDR/MDR Firewalls מערכות הגנה נוספות (NAC, DLP, WAF וכו')
		האם מתקיים מעקב ועיון בלוג אירועים בגין התראות המתקבלות מהמערכות שצוינו לעיל?
		האם הלוגים נשמרים לפרק זמן של לפחות 24 חודשים?
		אילו שדות מתועדים בלוגים (זיהוי ואימות, נעילות משתמשים, פעולות עדכון משתמשים כולל שמירת ערך קודם, העלאות תכנים, גישה מרחוק)?
	פיתוח מאובטח	האם קיים נוהל פיתוח מאובטח (SDLC) המבוסס על הנחיות OWASP Top 10:2025 או מתודה מקבילה אחרת?
		במקרה של כתיבת קוד באמצעות AI/LLM או הטמעת מנגנונים מבוססי AI, האם מבוצע יישום של פיתוח מאובטח בהתאם ל-OWASP Top 10 for LLM Application 2025 או מתודה מקובלת אחרת להגנה על AI?
		האם קיים שימוש בגרסאות עדכניות ונתמכות של שפות הפיתוח?
		האם הפיתוח מבוצע על בסיס דרישות מסמכי האפיון?
		האם מבוצעות בדיקות מסירה לווידוא קיום דרישות אבטחת המידע הקיימות במסמך האפיון?
		האם מבוצעות בדיקות חדירה למערכת טרם העברתה לסביבת הייצור?
	הגנה אפליקטיבית - הזדהות והרשאות	האם קיימת אפשרות הגדרת מדיניות סיסמאות חזקה הכוללת לכל הפחות : סיסמה מורכבת מאותיות לטיניות וספרות, סיסמה מורכבת מ-Uppercase letter ו- Lowercase letter, אורך סיסמה מינימלי בן 8 תווים, הגדרת פרק זמן Session Time Out לאחר אי פעילות, הגדרת הצפנה חד כיוונית בבסיס הנתונים, ושימוש ב-MFA?
		האם קיימת אפשרות ליישום עקרונות מידור, לפיו עובד ו/או תושב ייחשף אך ורק למידע אשר הוא נדרש לו לצורך מילוי תפקידו ועקרון של מתן הרשאות מינימליות?
		האם קיימת אפשרות להגדרת ברירת מחדל לנעילת חשבון לאחר מספר מסוים של ניסיונות כניסה?
		האם קיים תיעוד לכלל השינויים בטבלת ההרשאות?
		האם קיימת אפשרות להפקת דוח הרשאות תקפות?

		האם קיימת אפשרות להגביל את תוקף הסיסמה? אם כן, האם ניתן להגדיר מינימום 5 דורות לסיסמה?
	הגנה אפליקטיבית - בקרות קלט-פלט	האם קיים שימוש בפרוטוקול https בכל דפי היישום?
		האם מוגדרת רשימת ערכים וטווחים מותרים לשדות קלט (כולל הגנה על FORM באמצעות CAPTCHA)?
		האם קיימת בקרה לבחינת חשיפת שדות לא נדרשים בדוחות המופקים מהמערכת?
		העלאת קבצים למערכת: האם קיימת סניטציה לקבצים העולים לשרת (קובץ אינו נשמר כ-html ו/או php)?
		האם קיימת מניעת מניפולציה לכתובת ה-URL (חסימת יכולת שינוי UID בסוף הדף ו/או הוספת / שינוי דפי משנה)?
		האם קיימת הסתרת הודעות שגיאה אפליקטיביות הכוללת קוד ו/או טבלאות בתוך היישום?
		האם קיימת הפרדת סביבות (ייצור ופיתוח)? אם כן, האם קיים שימוש בנתוני אמת בסביבת הפיתוח?
	ניהול שירותי SaaS וסביבות ענן	האם ממשק הניהול נגיש מהאינטרנט או שהוא מוגבל לכתובות IP?
		האם קיימים משתמשים אישיים לכלל העובדים שלכם הניגשים לממשק הניהול?
		האם קיימים לוגים על ניסיונות גישה של עובדים שלכם לממשק הניהול?
		האם קיימים לוגים על שינויים ואירועי אבטחה?
		לכמה זמן הלוגים נשמרים?
		כיצד מבוצעת הסרת גישה של עובד שעוזב?
		באיזו סביבה השרתים ממוקמים (AWS/Azure/GCP/אחר)?
		באיזה אזור ממוקמת סביבת הענן (ישראל, אירופה וכו')?
		האם העובדים שלכם נגישים למידע במערכת עצמה?
		האם העובדים שלכם יכולים לשנות מידע/למחוק מידע?
		האם קיימת אפשרות להוריד את המידע למחשב האישי? אם כן, כיצד?
		האם קיימת התנהלות מסודרת בנוגע לעדכון גרסה של המערכת?