נספח התקשרות עם ספק תוכנה

שנחתם ביום _____ לחודש _____ בשנת _____

בין

אוניברסיטת בר אילן

ח.פ 580063683

(להלן: "**האוניברסיטה**")

לבין

_____

ח.פ _____

(להלן: "**הספק**")

הואיל והצדדים חתמו ביניהם על הסכם התקשרות ל_____ ביום XX/XX/XXXX ("**ההסכם**");

והואיל ובמסגרת ההתקשרות הספק עשוי להיחשף למידע ממאגרי המידע של האוניברסיטה;

והואיל ומחזור הפיתוח של תוכנה ו/או מערכת ממוחשבת נדרשים בהתאמה לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017;

והואיל והצדדים מעוניינים להסדיר את נושאי אבטחת המידע והגנת הפרטיות במסגרת השירותים בהתאם להוראות דיני הגנת הפרטיות;

לפיכך הוסכם, הוצהר והותנה בין הצדדים כדלקמן:

<u>הוראות כלליות:</u>

1. הספק מצהיר כי לשם מתן השירותים אשר פורטו בהסכם, הוא עשוי להיחשף למידע ממאגרי המידע ו/או למידע חסוי של האוניברסיטה, כמפורט להלן ("המידע המורשה"):
   1.1. [...]
   1.2. [...]

   וזאת למטרת ביצוע השירותים בלבד, כפי שהוגדרה בהסכם ("**מטרת השירות**");
2. העברת מידע בין הספק ללקוח או להיפך תתבצע באמצעות _____
3. במסגרת ההסכם, הספק *אינו רשאי לגשת למערכות המידע / במסגרת ההסכם, הספק רשאי לגשת אך ורק למערכות המידע הבאות* (מחק את המיותר):
   3.1. [...]
   3.2. [...]

4. הספק לא יעביר וכן לא יאפשר גישה ו/או הרשאות צפייה ו/או הרשאות עיבוד כלשהן לגבי המידע המורשה לאף גורם מבלי שקיבל את אישור האוניברסיטה מראש ובכתב. לשם כך, ולצורך ביצוע השירותים המפורטים בהסכם בלבד, האוניברסיטה מאשרת לספק להתקשר עם ספקי המשנה הבאים:
   4.1. [...] העברה אך ורק לצורכי _____.
   4.2. [...]
   4.3. [...]
5. הספק מצהיר בזאת כי בעת התקשרות עם ספק משנה כאמור בסעיף 4, יחתים הספק את ספק המשנה על הסכם התקשרות התואם באופן מהותי את הוראות הסכם זה. ביחס לספקי ענן גלובליים (כדוגמת AWS, AZURE, GCP) ניתן להסתפק בהסמכה לתקני אבטחה מקובלים, כדוגמת ISO27001 או SOC2 ו\או הצגת מדיניות פרטיות מתאימה, וזאת לאחר שהספק בחן את סיכוני אבטחת המידע הכרוכים בהתקשרות ומצא את ספק המשנה מתאים ובכפוף לתקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001.
6. הספק מצהיר ומתחייב בזאת כי עם סיום ההתקשרות, מכל סיבה שהיא, ולכל היותר, בתום תקופת ההסכם, כל המידע המורשה שהגיע לרשותו במסגרת ההסכם יוחזר לרשות האוניברסיטה לפי בקשתו, ככל הניתן, יימחק מכל אמצעי המדיה שברשותו ו/או ברשות מי מטעמו. הספק יציג לאוניברסיטה תצהיר חתום על ידי מורשה החתימה של הספק המאמת ביצוע פעולות מחיקה, ביעור והשמדה כאמור.
7. הספק מתחייב לפעול על פי כל דין, לרבות הוראות חוק הגנת הפרטיות, תשמ"א-1981 (להלן: "**החוק**" או "**חוק הגנת הפרטיות**") התקנות שהותקנו לפיו, הנחיות רשם מאגרי המידע והרשות להגנת הפרטיות וכיוצא בזאת, ולפי הוראות שיתקבלו מעת לעת על ידי האוניברסיטה.
8. הספק לא יהא רשאי לעדכן ו/או להשיב לצדדים שלישיים בכל הנוגע למידע המורשה ,ובכל מקרה בו תתקבל פנייה הנוגעת למידע המורשה המוחזק במערכות הספק ,ינחה הספק את הפונה לפנות לאוניברסיטה (למעט אם קיימת חובה אחרת לפי כל דין).
9. הספק מתחייב לאפשר לאוניברסיטה ביצוע מעקב ובקרה שוטפים על קיום הוראות חוק הגנת הפרטיות והתקנות שהותקנו לפיו והוראות ההתקשרות וזאת על מנת לאפשר פיקוח על פעילותו של הספק בהתאם להוראות הדין. בכלל זאת, הספק מתחייב לאפשר לנציג האוניברסיטה לערוך ביקורת אבטחה בכל עת ובתיאום מראש.
10. הספק מתחייב להעביר דיווח מידי לאוניברסיטה בכל מקרה של חשש לדליפת המידע מהמאגר או שימוש חורג מההרשאה שניתנה לספק ו/או למי מטעמו.

<u>סודיות:</u>

11. "**מידע**", במסמך זה: כל חומר, מסמך ו/או מידע אחר הנוגע לפעילות הלקוח ו/או חבריו ו/או לקוחותיו ו/או עובדיו ו/או עסקיו אשר אינו נחלת כלל הציבור (למעט אם הפך לכזה בשל מעשה/מחדל של הספק) לרבות, מבלי לגרוע מכלליות האמור לעיל, מידע אודות משאבי הלקוח; מידע בדבר סודות מסחריים ו/או מקצועיים, הזמנות והסכמים מכל סוג ו/או מידע המוגן מכוח חוק הגנת הפרטיות ו/או בהתאם לכל דין אחר החל או עשוי לחול על הלקוח.
12. ידוע לספק כי לצורך מתן השירותים לאוניברסיטה, תהא לו גישה למידע כהגדרתו לעיל. כמו כן, ידועה וברורה לספק רגישותו המיוחדת של המידע והצורך בשמירה קפדנית על חסיונו ועל הנזק הכבד שעשוי להיגרם עקב חשיפתו על ידי או עשיית שימוש בו על כל המשתמע מכך.

13. הספק מתחייב לשמור בסודיות מוחלטת כל מידע אשר יגיע אליו ו/או למי מטעמו מתוקף מתן השירותים לאוניברסיטה או בדרך אחרת. הספק מתחייב שלא להחזיק ברשותו ולא לעשות כל שימוש, בכל מידע באשר הוא שלא לצורכי ביצוע השירותים המפורטים בהסכם. הספק מתחייב שלא לגלות מידע כזה או חלקו, במישרין או בעקיפין, לכל אדם או גוף, אלא לצורך ביצוע השירותים לפי ההסכם ובכפוף להסכמת האוניברסיטה. למעט:
    13.1. העברת מידע מוגבלת לעובדים (לרבות נותני שירות מטעם הספק) אשר להם צורך של ממש בקבלת המידע לצורך ביצוע השירותים בלבד, ובלבד שהובהר לעובדים אלה כי מדובר במידע סודי, והם חתומים כלפי הספק על כתב סודיות בנוסח דומה לכתב סודיות זה.
    13.2. על פי דרישת ערכאה מוסמכת או רשות שלטונית מוסמכת על פי דין, ובלבד שהספק יודיע לאוניברסיטה באופן מידי על קבלת דרישה למסירת המידע (ככל שלא קיימת מניעה על פי דין למתן הודעה כאמור), ויאפשר לאוניברסיטה, ככל שהדבר בידי הספק, להתגונן בפני כל דרישה כאמור והספק ימסור רק את אותו חלק של המידע הסודי ו/או המידע החסוי שנדרש במפורש למסור.
14. הספק מתחייב לפעול כך שנתונים ומידע אשר יועברו אליו בהתאם להסכם זה, יאובטחו כך שלא תתאפשר גישה, בין באופן אקטיבי ובין באופן פאסיבי, למידע ולנתונים אלו, לאיש מלבד המורשים לכך החתומים על כתב התחייבות לשמירת סודיות כלפי האוניברסיטה.
15. הספק מתחייב שלא להעתיק ו/או להרשות לאחרים ו/או לגרום לאחר לבצע במידע – שכפול, העתקה, צילום, תדפיס וכל צורת העתקה אחרת שלא למטרת השירותים.
16. על העותקים של המידע יחולו הוראות התחייבות זו וכל האמור לגבי המידע יחול גם על עותקיו.
17. הספק מתחייב כי בכל מקרה שיתעוררו ספקות כלשהן בנוגע לתוכן התחייבויותיו לפי כתב התחייבות זה, וקיומו, יפנה לאוניברסיטה בכתב לקבלת אישורו. ידוע לספק כי אין בנאמר בפסקה זו לגרוע מכל התחייבות מהתחייבויותיו המנויות בכתב התחייבות זה.
18. הספק מתחייב להודיע מיידית לאוניברסיטה בכל מקרה של פעולה שגרמה לאובדן מידע כלשהו של האוניברסיטה.
19. למען הסר ספק, מוצהר ומוסכם כי אין בעצם גילוי המידע על ידי האוניברסיטה והעברתו אל הספק כדי להעניק לספק כל זכות במידע.
20. התחייבויות הספק דלעיל תחולנה עליו אישית וכן על כל תאגיד ו/או גוף שיקים ו/או שיהיה שותף בו, ו/או בעל שליטה בו, בין כבעל מניות, ובין בכל דרך אחרת, בין במישרין ובין בעקיפין, וכן על כל עובד מטעם הספק שייתן השירות.
21. תוקפה של התחייבות זו אינו מוגבל בזמן.
22. התחייבות זו לא תחול על מידע אשר התקבל מהאוניברסיטה ואשר הספק יוכיח לגביו בכתובים כי:
    22.1. המידע היה ידוע לספק לפני קבלת המידע מהאוניברסיטה.
    22.2. המידע היה ידוע ברבים או שהיה ניתן להשגה על ידי הציבור הרחב באופן חוקי לפני יום העברתו לספק.
    22.3. המידע הפך למידע ציבורי או ניתן להשגה על ידי הציבור באופן חוקי לאחר מועד העברת המידע על ידי האוניברסיטה לספק בלא שהיה הוא אחראי או מעורב בתהליך.
    22.4. המידע הגיע לספק בדרך חוקית של רכישת זכויות או בכל דרך חוקית שהיא.
23. ידוע ומוסכם כי האוניברסיטה תהא זכאית לפיצוי מהספק בגין כל נזק שייגרם בעקבות הפרה של איזו מהתחייבויותיו לפי כתב התחייבות זה, וזאת מבלי לפגוע בכל סעד אחר המוקנה לאוניברסיטה על פי

דין ובלבד שהאוניברסיטה הודיעה לספק על התביעה ו/או הדרישה ואפשר לו להתגונן כנגדה באופן עצמאי.

<u>דרישות אבטחת מידע</u>

24. <u>הנחיות כללית:</u>

24.1. הספק מצהיר כי הוא פועל כנדרש על פי החוק, התקנות ותיקוני הגנת הפרטיות וכי הוא נוקט באמצעי אבטחה ובקרה כמתחייב מהוראות חוק הגנת הפרטיות, תיקוניו ותקנותיו והנחיות רשם מאגרי מידע.

24.2. הספק יבצע הדרכה פרונטלית על התוכנה עפ"י דרישת האוניברסיטה.

25. הספק יתקין תוכנת הגנה תקנית ומעודכנת נגד נוזקות על מחשבים המכילים מידע השייך לאוניברסיטה.

26. <u>פיתוח מאובטח:</u>

26.1. הספק אחראי לפיתוח המערכת ועדכוניה בכפוף לנוהל פיתוח מאובטח (SSDLC) המבוסס על תקן OWASP עדכני או תקן מקביל שתאושר ע"י האוניברסיטה.

26.2. שימוש בגרסאות מעודכנות ונתמכות של שפות הפיתוח.

26.3. העברת מסמך אפיון מערכת לאישור מנהל אבטחת מידע של האוניברסיטה.

26.4. פיתוח המערכת בהתאם לדרישות האפיון.

26.5. ביצוע בדיקות מסירה ע"י הספק לווידוא קיום דרישות אבטחת מידע באפיון.

26.6. מבדק חדירה למערכת לפני העברה לייצור.

27. <u>הזדהות והרשאות:</u>

27.1. אפשרות הגדרת מדיניות סיסמאות חזקה המורכבת מאותיות וספרות, אורך סיסמא מינימלי של 8 תווים, ו/או מתן אפשרות לקישור המערכת ל-Active Directory של האוניברסיטה, לבקשת האוניברסיטה.

27.2. הגדרת מנגנון לאכיפת החלפת סיסמאות- מינימום יום אחד (1), מקסימום חצי שנה (180 ימים).

27.3. הסיסמאות תוצפנה בהצפנה חד כיוונית בבסיס הנתונים.

27.4. יכולת הגדרת היסטוריית סיסמאות – לפחות 10 דורות אחורה.

27.5. יכולת הגדרת הרשאות על פי פרופיל (תפקיד) תוך מידור גישה/עדכון ברמת שדה.

27.6. יכולת הפקה יזומה של דו"ח הרשאות תקפות לפחות אחת לשנה או בהתאם לבקשת האוניברסיטה.

27.7. יישום תיעוד כל שינוי בטבלת ההרשאות.

27.8. יכולת הגדרת הזדהות רב שלבית (MFA) ולכל הפחות דו-שלבית (2FA) כגון סיסמה חד-פעמית (OTP), TOKEN וכיוב'.

27.9. גישת Admin (מנהל מערכת) תהיה באמצעות אימות רב שלבי (MFA).

28. <u>אפשרות הגדרת תיעוד בלוג:</u>

28.1. זיהוי ואימות;

28.2. נעילות משתמש;

28.3. פעולות עדכון ע"י המשתמשים כולל שמירת ערך קודם;

28.4. העלאות תכנים;

28.5. גישה מרחוק;

28.6. תיעוד כל מקרה שבו התגלה אירוע אבטחת מידע. ככל האפשר יבוסס התיעוד על רישום אוטומטי;

28.7. ממשק API למערכת ניטור מרכזית (כגון SIEM);

28.8. שמירת הלוגים באופן מאובטח למשך 24 חודשים לכל הפחות.

29. <u>בקרת קלט- פלט</u>:

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

29.2. שימוש בפרוטוקול Https בכל דפי היישום;

29.3. הגדרת רשימת ערכים וטווחים מותרים לשדות קלט (כולל הגנה על FORM באמצעות CAPTCHA);

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

29.5. 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;

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

30. <u>הפרדת סביבות</u>:

30.1. סביבת הייצור תופרד מסביבות אחרות- המערכת תותקן באופן מקומי בשרתי האוניברסיטה;

30.2. העברת המערכת/האפליקציה מסביבת פיתוח לייצור תתבצע בצורה מבוקרת;

30.3. לא יעשה שימוש בנתונים אמיתיים בסביבת הפיתוח.

31. <u>אבטחת תשתיות</u>:

31.1. מענה אנושי לטיפול באירועי סייבר.

31.2. הספק יוודא 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.

31.3. דרישות נוספות במקרה של פעילות בענן [להסרה/ עדכון טרם הפצה לחתימת הצדדים]:

31.4. במקרה של פיתוח בשירותי ענן הכולל נתוני אמת של האוניברסיטה, יוגדרו דרישות נוספות בהתאם לצורך ולסוג הפעילות.

ולראיה באתי על החתום:

שם + שם משפחה _____ תפקיד _____

תאריך _____ חתימה + חותמת _____