1. מטרה

1.1. הסדרת עקרונות למסירת עבודה לספקי מיקור חוץ עבור אוניברסיטת בר אילן (ע"ר) (להלן: "**האוניברסיטה**") הכרוכה בהתחברות מרחוק למחשבי האוניברסיטה, לצורך הגנה על שלמות המידע השמור במערכות האוניברסיטה, הגנה על המידע כהגדרתו להלן מפני חשיפה לצד ג' ו/או שימוש בידי צד ג'.

1.2. הסדרת עקרונות אבטחת המידע וסייבר באתרי ספקים חיצוניים המחזיקים מידע של האוניברסיטה.

1.3. הסדרת עקרונות אבטחת מידע וסייבר בפעולות פיתוח.

1.4. התאמת פעילות האוניברסיטה להוראות חוק הגנת הפרטיות, התקנות שהותקנו מכוח החוק ובפרט תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "**תקנות אבטחת מידע**"), הנחיות הרשם לפי החוק לגבי רישום מאגרי מידע, הנחיות מערך הסייבר הלאומי ותורת ההגנה הקיברנטית[1].

2. כללי

2.1. האוניברסיטה כפופה לחוק הגנת הפרטיות, התשמ"א-1981 (להלן: "החוק" או "חוק הגנת הפרטיות") להנחיות רשם מאגרי המידע ולתקנות שהותקנו מכוח החוק.

2.2. האוניברסיטה נעזרת בשירותיהם של ספקים וקבלנים חיצוניים (להלן: "ספקים") לצורך קבלת שירותים מסוגים שונים. כתוצאה מכך, ספקים אלה מורשים לגישה למאגרי המידע של האוניברסיטה ובכך נחשפים למידע מוגן ע"פ חוק הגנת הפרטיות ומידע רגיש של האוניברסיטה ועובדיה. כן מועבר לספקים, בהתאם לצורך ובמסגרת ההתקשרות ולצרכיה, מידע רגיש.

2.3. קיימת חשיבות רבה לנקיטת צעדים טכנולוגים ומנהליים שיצמצמו את הסיכונים הנובעים מהיות הספקים חשופים למידע כאמור, לרבות בתהליך הכרוך בסיום התקשרות עם גורמי מיקור חוץ.

2.4. נוהל זה מפרט את חובות האוניברסיטה לעניין התקשרות עם מיקור חוץ בהתאם לדרישות החוק, תקנות אבטחת מידע ותקני אבטחת מידע מקובלים בעולם. במידת הצורך ובהתאם לשיקול דעת האוניברסיטה, הגורמים המנויים בנוהל זה יעזרו בתקנה 15 לתקנות אבטחת מידע.

2.5. מנהל אבטחת מידע יוכל להחריג ספק או אוכלוסיית משתמשים מתחולת הנוהל לפי שיקול דעתו ובכפוף להנחיות הרשות להגנת הפרטיות והדין לאחר התייעצות מוקדמת עם הממונה על הגנת הפרטיות.

---

[1] 'תורת ההגנה הקיברנטית' - מסמך שפרסם מערך הסייבר הלאומי המסייע לארגונים למפות את סיכוני הסייבר שהם חשופים אליהם ולהגדיר אמצעי הגנה בהתאם. תורת ההגנה מהווה עקרונות best practice לאבטחת מידע - https://www.gov.il/he/Departments/Guides/cyber_security_methodology_for_organizations_test?chapterIndex=1

3. הגדרות

3.1 **"סייבר"** – משמש ככינוי למרחב הקיברנטי. מרחב ה"סייבר" מורכב משלושה רבדים:

3.1.1. רובד פיזי – הכולל את כלל מרכיבי המחשוב והתקשורת.

3.1.2. רובד לוגי – המכיל את הקוד המפעיל את רכיבי המחשוב וכיצד יפעלו.

3.1.3. רובד אנושי – הכולל את כלל האנשים המשתמשים ברשת.

3.2 **"ספקים וקבלנים חיצוניים"** – גורמים חיצוניים אשר מספקים שירות ו/או טובין לאוניברסיטה, בין אם במשרדיה בין אם מרחוק, ונחשפים למידע אישי ממאגרי מידע.

3.3 **"ספקים מהותיים" -** ספקים החשובים לפעילות האוניברסיטה ו/או אלה החושפים אותה לסיכוני סייבר ואבטחת מידע פוטנציאליים גבוהים, שבהתממשותם ניתן יהיה לתקוף את האוניברסיטה או לפגוע בפעילותה.

3.4 **"עובד ספק"** - עובד של ספק או קבלן חיצוני, ו/או איש שירות מטעמו, שנחשף למידע ממאגרי המידע של האוניברסיטה, בין במשרדי האוניברסיטה ובין מרחוק ממשרדי הספק/הקבלן החיצוני.

3.5 **"נספח אבטחת מידע עם ספק/קבלן חיצוני"** – נספח להסכם ההתקשרות בין האוניברסיטה לספק/קבלן. שמסדיר, ביו היתר, את דרישות אבטחת המידע, הפרטיות והסודיות מהספק.

3.6 **"אבטחת מידע"** - כלל האמצעים הטכנולוגיים והארגוניים הננקטים לשם צמצום סיכוני השימוש במערכות טכנולוגיית המידע בתחומי חשאיות המידע, אמינותו, שלמותו וזמינותו, לרבות מסמכי נייר.

3.7 **"מאגר מידע"** – כהגדרתו בחוק הגנת הפרטיות, התשמ"א-1981.

3.8 **"מנהל אבטחת מידע"** – עובד שימונה ע"י סמנכ"ל תקשוב ואשר תפקידו יהא לטפל בכל הקשור לנושאי אבטחת מידע וכן לגיבוש, עיבוד ופרסום הנהלים הפנימיים הקשורים לאבטחת המידע באוניברסיטה, ביצועם ואכיפתם.

3.9 **"ממונה על הגנת הפרטיות"** – מי שמונה על ידי מנכ"ל האוניברסיטה להיות אחראי על הטמעה ויישום ההוראות החלות על האוניברסיטה מכוח חוק הגנת הפרטיות ותקנות האיחוד האירופי-GDPR.

3.10 **"מחזיק מאגר מידע"** - ספק שמנהל את תשתיות מערכות מאגרי מידע או מחזיק במערכות מאגר מידע או מבצע פעולות במערכת מאגר מידע דרך קבע והוא רשאי לעשות בהם שימוש.

3.11 **"אירוע אבטחת מידע"**- הינו אירוע מכל סוג, אשר פוגע, או עלול לפגוע בסודיות, בשלמות ובזמינות המידע ברשת המחשוב של האוניברסיטה, ו/או לפגוע, לשבש או לקטוע תהליכי עבודה תקינים באוניברסיטה. כגון:

3.11.1. חשיפה בלתי מורשית של מידע רגיש ממערכות המידע של האוניברסיטה.

3.11.2. התקפות מניעת שירות על מערכות האוניברסיטה (Denial Of Service).

3.11.3. פריצה למערכות המידע באוניברסיטה (ע"י תוקף חיצוני או פנימי).
3.11.4. פגיעת וירוס בתשתיות המחשוב של האוניברסיטה.
3.11.5. שינוי פני אתרים ואפליקציות (Defacement).
3.11.6. מעילה, שימוש לא מורשה בהרשאות במערכת מידע.
3.11.7. השחתה או גניבת ציוד מחשבים במשרדי האוניברסיטה.
3.11.8. שימוש במערכות מידע לפעילות לא חוקית (גניבת תוצרת גמורה, מלאי בתהליך, וכו').

3.12. **"אירוע אבטחה חמור"** – כהגדרתו בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017:

א. במאגר מידע שחלה עליו רמת אבטחה גבוהה – אירוע שנעשה בו שימוש במידע מן המאגר, בלא הרשאה או בחריגה מהרשאה או שנעשתה פגיעה בשלמות המידע.
ב. במאגר מידע שחלה עליו רמת אבטחה בינונית – אירוע שנעשה בו שימוש בחלק מהותי מן המאגר, בלא הרשאה או בחריגה מהרשאה או שנעשתה פגיעה בשלמות המידע לגבי חלק מהותי מן המאגר;

3.13. **"מידע רגיש"** - כהגדרתו בחוק הגנת הפרטיות התשמ"א-1981 בתקנות, הנחיות רשם מאגרי מידע ובצווים שהוצאו מכוחו.

3.14. **"הגורם המזמין"** – היחידה באוניברסיטה שמבקשת להתקשר עם ספק חיצוני לצרכי היחידה.

4. <u>הנחיות כלליות</u>

4.1. <u>התקשרות עם ספק חיצוני יכולה להתבצע בשני אופנים:</u>

א. התקשרות בעקבות מכרז או בעקבות מתן פטור ממכרז על ידי וועדת מכרזים/וועדת תשומות של האוניברסיטה- ראה סעיף 5.3 לנוהל.
ב. התקשרות באמצעות הזמנת רכש, בהתאם לנוהלי האוניברסיטה.

4.2. יחידה מזמינה המעוניינת להתקשר עם ספק מיקור חוץ, הכרוך בגישה למאגר מידע של האוניברסיטה (בין אם באמצעות הרשאות במערכות ובין אם באמצעות העברת מידע), תפנה תחילה למנהל אבטחת מידע לשם קבלת אישור להתקשרות.

4.3. מנהל אבטחת מידע יבחן בטרם היציאה למכרז או בטרם ההתקשרות, לפי העניין את הסיכונים הכרוכים בהתקשרות עם הספק לצורך מתן שירות לאוניברסיטה הכרוך במתן גישה למאגרי המידע של האוניברסיטה. באחריות הגורם המזמין להגדיר את דרישות אבטחת המידע בהתאם לסוג הספק ולנספחים המצורפים לנוהל זה, ובמידת הצורך תוך התייעצות עם מנהל אבטחת המידע ו/או הממונה על הגנת הפרטיות.

4.4. מנהל אבטחת מידע יגדיר תכנית בדיקה שנתית אצל הספקים המהותיים, על מנת לוודא יישום דרישות אבטחת המידע הרלוונטיות בנסיבות העניין, וידאג לבדוק את יישומה.

4.5. מחלקת הרכש תחתים ספקים קיימים על הנספחים המצורפים לנוהל זה לפי העניין: נספח א'- לספק שאינו ספק תוכנה ו/או מחזיק מאגר; נספח ב'- לספק תוכנה ונספח ג' - לספק מארח/מחזיק מאגר מידע הכוונה רק לספקים רלוונטיים לא לכלל הספקים של בר-אילן-לא נוכל להחתים את כולם.

5. שיטה

5.1. תקשורת והצפנה

5.1.1. מנהל אבטחת מידע יגדיר את דרישות הצפנת התקשורת.

5.1.2. מנהל אבטחת מידע יוודא מימושן של דרישות ההצפנה בתקשורת מול מערכות המחשב של האוניברסיטה, כאשר הגישה היא באמצעות האינטרנט.

5.2. התקשרות עם ספק חיצוני שלא באמצעות מכרז

5.2.1. בעת התקשרות עם ספק שלא באמצעות מכרז, על הגורם המזמין להזין בקשה במערכת ה-ERP לאישור התקשרות עם ספק. במסגרת הבקשה, הגורם המזמין יציין האם הספק ייחשף למידע ממאגרי המידע של האוניברסיטה בצורה כלשהיא. הבקשה תיבחן על ידי מחלקת הרכש ותאושר על ידה.

5.2.2. אישור ההתקשרות עם ספק חיצוני הכרוכה במתן גישה למאגרי המידע של האוניברסיטה, יינתן רק לאחר היוועצות עם מנהל אבטחת מידע של האוניברסיטה ביחס לסיכוני אבטחת המידע ועם ממונה על הגנת הפרטיות ביחס לדרישות רגולטוריות בהיבטי אבטחת מידע והגנת הפרטיות. .

5.2.3. לאחר אישור הבקשה, תחתים מחלקת הרכש או הגורם המזמין, לפי העניין, את הספק על נספח אבטחת מידע, בהתאם לסוג הספק. במידת הצורך, מחלקת הרכש או הגורם המזמין ייוועצו עם ו/או מנהל אבטחת מידע ו/או הממונה על הגנת הפרטיות, לצורך סיווג נכון של הספק.

5.3. מכרז / הסכם התקשרות

5.3.1. התקשרות עם ספק חיצוני מתבצעת בהתאם לנוהל התקשרויות של האוניברסיטה. כאשר ההתקשרות מתבצעת באמצעות מכרז, באחריות מחלקת הרכש לכלול את הנושאים המפורטים בסעיף 5.3.2 במסמכי ההתקשרות לשם קביעת הנדרש מחלקת הרכש במנהל אבטחת המידע ו/או בממונה על הגנת הפרטיות.

5.3.2. דרישות האבטחה יכללו לכל הפחות <u>את הנושאים הבאים:</u>

5.3.2.1. המידע שהספק רשאי לעבד ומטרות השימוש המותרות בו לצורכי ההתקשרות.

5.3.2.2. מערכות המאגר שהספק רשאי לגשת אליהן.

5.3.2.3. סוג העיבוד או הפעולה שהספק רשאי לעשות.

5.3.2.4. אחריות לטיפול באירועי אבטחת מידע אשר מתרחשים במערכות המאגרים שברשותם. בכלל זה, תיעוד האירועים

ודיווח למנהל אבטחת מידע של האוניברסיטה וכן לרשם מאגרי מידע בקרות אירוע אבטחה חמור.

5.3.2.5. משך ההתקשרות, אופן השבת המידע לידי האוניברסיטה בסיום ההתקשרות, השמדתו מרשותו של הספק ודיווח על כך למנהל אבטחת המידע של האוניברסיטה.

5.3.2.6. אופן יישום החובות בתחום אבטחת המידע שהמחזיק חייב בהן לפי תקנות אבטחת מידע וכן הנחיות נוספות לעניין אמצעי אבטחת מידע שהוגדרו בנוהל זה ובנספח אבטחת מידע.

5.3.2.7. חובתו של הספק להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק לפי האמור בהסכם ההתקשרות וליישם את אמצעי אבטחת המידע הקבועים בנספח אבטחת מידע, לרבות פיקוח על ביצוע ההוראות על ידי עובדיו.

5.3.2.8. במקרה בו האוניברסיטה התירה לספק לתת את השירות באמצעות גורם נוסף, אזי חובתו של הספק החיצוני לכלול, בהסכם עם הגורם הנוסף, לכל הפחות את כל הנושאים המפורטים בסעיף זה, אשר צריכים להיכלל בהסכם ההתקשרות.

5.3.2.9. סמכויות פיקוח של האוניברסיטה, ובכלל זאת הוראה כי הספק החיצוני ידווח למנהל אבטחת מידע של האוניברסיטה, אחת לשנה לפחות, אודות אופן ביצוע חובותיו לפי תקנות אבטחת המידע וההסכם, ואודות אירועי אבטחת מידע.

5.3.2.10. האוניברסיטה רשאית להתקשר עם ספק חיצוני לצורך מתן שירות הכרוך בגישה למספר מאגרי מידע בהסכם אחד לעניין כל המאגרים, ובלבד שכל המאגרים באותה רמת אבטחת מידע.

5.3.3. נספח אבטחת מידע יהיה בהתאם לדוגמאות הבאות, כאשר סטיה אפשרית לפי העניין ובהתייעצות עם מנהל אבטחת מידע:

נספח א'- לספק (שאינו ספק תוכנה ו/או מחזיק מאגר)

נספח ב'- לספק תוכנה

נספח ג'- לספק מחזיק /מארח מאגר.

5.4. **<u>הגדרת ספקים במערך המחשוב של האוניברסיטה</u>**

5.4.1. אגף התקשוב יגדיר לספק שיזדקק במהלך עבודתו לבצע פעילויות במערך המחשוב של האוניברסיטה, זיהוי משתמש אישי (User-Id) בסביבת המחשוב שבה יעבוד לתקופה מוגבלת (הרשאה לשנה או למשך העסקתו אם נמוך משנה). זיהוי זה יקבע על פי על פי הוראות הממונה הישיר ואישור מנהל אבטחת מידע. זיהוי זה יחשב כהרשאה למאגר מידע על פי חוק הגנת הפרטיות.

5.4.2. אגף התקשוב יגדיר לספק הרשאות ברמה המינימלית להן הוא נזקק במהלך עבודתו ולצורך ביצוע עבודתו בלבד, בהתאם להנחיות מנהל אבטחת מידע ובהתאם לנוהל משתמשים והרשאות.

5.4.3. אגף התקשוב יתעד ויתייק את ההרשאות שיינתנו לספק מיקור חוץ.

5.4.4. אגף התקשוב יבצע בקרה על הרשאות הספקים, לכל הפחות אחת לחצי שנה.

5.5. **<u>בקרה ותיעוד גישה</u>**

5.5.1. ספקים חיצוניים אשר מחזיקים מאגרי מידע ומערכות מאגרי מידע של האוניברסיטה אחראים בהתאם לתקנות אבטחת מידע ולנספח ג' עליו יחתום הספק לקיום מנגנון בקרה במאגרים ובמערכות שברשותם.

5.5.2. מנגנון הבקרה יאפשר תיעוד אוטומטי וביקורת על הגישה למערכות המאגר אשר יכלול את הנתונים הבאים בלוגים: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה.

5.5.3. מנגנון הבקרה לא יאפשר, ככל האפשר, ביטול או שינוי של הפעלתו, יאתר שינויים או ביטולים בהפעלתו ויקושר לרכיב שיפיץ התראות, בין היתר, לגורמים האחראים באוניברסיטה: מנהל אבטחת מידע, יועץ המחשוב וכל גורם נוסף שיקבע על ידי מנהל אבטחת מידע.

5.5.4. מנהל אבטחת מידע יגדיר נוהל בדיקה שגרתי של הלוגים לפחות אחת לחודש, ידאג ליישומו ויערוך דו"ח של הבעיות שהתגלו והצעדים שננקטו.

5.5.5. אגף התקשוב ישמור את הלוגים של מנגנון הבקרה באופן מאובטח למשך 24 חודשים, לכל הפחות.

5.6. **<u>אירועי אבטחת מידע</u>**

5.6.1. פעולות ספקים בעלי הרשאות גישה למערכות הפנימיות של האוניברסיטה יתועדו בלוגים על ידי מחלקת המחשוב. מנהל אבטחת מידע יגדיר קבלת התראות על פעולות חריגות.

5.6.2. ספקים אשר מחזיקים מאגרי מידע ומערכות מאגרי מידע, יהיו אחראים לטפל באירועי אבטחת מידע אשר מתרחשים במערכות המאגרים שברשותם, לגבי מידע ושירותים של האוניברסיטה. כמו כן, הספקים יהיו אחראים לתעד את האירועים ולדווח עליהם למנהל אבטחת מידע של האוניברסיטה וכן דיווח גם לרשם מאגרי מידע בקרות אירוע אבטחה חמור.

5.7. **<u>סיום הפעילות</u>**

5.7.1. הגורם המזמין ידווח למנהל אבטחת מידע על סיום ההתקשרות עם הספק וכן יעביר למחלקת המחשוב טופס/ מייל לצורך ביטול ההרשאות באופן מידי.

5.7.2. אם סופק לספק ציוד מחשוב, הממונה הישיר יוודא השבתו לאוניברסיטה.

5.7.3. במקרה של מעבר ספק המחזיק מערכת מידע, יוודא מנהל אבטחת מידע כי לא נשאר מידע של האוניברסיטה במחשבי הספק עם סיום ההתקשרות, למעט מידע או גיבוי שהאוניברסיטה דרשה שיישמר.

5.8. **<u>הוראת מעבר</u>**

5.8.1. <u>ספקים אשר נותנים שירות לאוניברסיטה, אשר כרוך בגישה למאגרי המידע של האוניברסיטה או בקבלת מידע רגיש מהאוניברסיטה, ללא הסכם התקשרות בכתב</u> – מחלקת הרכש תיזום פניה לכל הספקים אשר נותנים שירות לאוניברסיטה בתחום פעילותם הכרוך בגישה למאגרי המידע של האוניברסיטה או בקבלת מידע רגיש מהאוניברסיטה, ולא מוגדר מולם הסכם התקשרות בכתב, על מנת להגדיר נספח אבטחת מידע להסכם ההתקשרות בהתאם לנוהל זה, לכל המאוחר עד לסוף שנת 2020.

5.8.2. <u>הסכמי התקשרות קיימים עם ספקים אשר נותנים שירות לאוניברסיטה, אשר כרוך בגישה למאגרי המידע של האוניברסיטה או בקבלת מידע רגיש מהאוניברסיטה, וטרם הגיע מועד חידושם</u> – מחלקת הרכש תיזום פנייה באופן מידי לספקים אלה, בהתאם לסוג הספק, כדי שיחתום על נספח אבטחת המידע הרלוונטי לו המצורף לנוהל זה ו/או יבצע פנייה יזומה לספק לקבלת אישור בכתב אודות אופן עמידתו בתקנות אבטחת המידע.

5.8.3. <u>הסכמי התקשרות שהגיע מועד חידושם או חדשים</u> - במועד חידוש ההסכמים, מחלקת הרכש תעדכן את הסכם ההתקשרות בהתאם לנוהל זה.

6. <u>אחריות</u>

6.1 יחידות האוניברסיטה ו/או הגורם המזמין

6.2 מחלקת הרכש

6.3 מנהל אבטחת מידע

6.4 הממונה על הגנת הפרטיות

7. <u>תחולה</u>

תוקף הוראה זו מיום פרסומה.

מר זהר ינון
מנכ"ל

נספח א '

נספח אבטחת מידע לספק מקבל מידע (שאינו מחזיק מאגר ואינו ספק תוכנה)

<u>התקשרות אבטחת מידע עבור ספק מקבל מידע</u>

בהמשך להזמנת העבודה/הסכם השירותים מיום _____, (להלן: "**הזמנת העבודה**"), שנחתמה בין _____ ח.פ _____ (להלן: "**הספק**") לבין אוניברסיטת בר אילן ע"ר 580063683 (להלן: "**האוניברסיטה**") ולאור הוראות תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "**תקנות אבטחת מידע**") הצדדים מעוניינים להוסיף את התנאים הבאים להתקשרותם:

<u>הוראות כלליות:</u>

1. הספק מצהיר כי לשם מתן השירותים אשר פורטו בהזמנת העבודה, האוניברסיטה נדרשת להעביר לספק מידע ממאגרי המידע של האוניברסיטה ו/או לאפשר לספק ולעובדיו גישה למאגרי המידע ו/או למערכות המידע של האוניברסיטה;
2. במסגרת הזמנת העבודה, הספק עשוי להיחשף / לקבל גישה לסוגי המידע הבאים:
   א. [...]
   ב. [...]
   וזאת למטרת ביצוע השירותים בלבד, כפי שהוגדרה בהזמנת העבודה ("**מטרת השירות**");
3. העברת מידע בין הספק לאוניברסיטה או להיפך תתבצע באמצעות _____.
4. במסגרת הזמנת העבודה הספק אינו רשאי לגשת למערכות המידע / במסגרת הזמנת העבודה הספק רשאי לגשת אך ורק למערכות המידע הבאות (מחק את המיותר):
   א. [...]
   ב. [...]
5. הספק לא יעביר וכן לא יאפשר גישה ו/או הרשאות צפייה ו/או הרשאות עיבוד כלשהן לגבי המידע המפורט בסעיף 2 לאף גורם מבלי שקיבל את אישור האוניברסיטה מראש ובכתב. לשם כך, ולצורך ביצוע השירותים המפורטים בהזמנת העבודה בלבד, האוניברסיטה מאשרת לספק להתקשר עם ספקי המשנה הבאים:
   א. [...], אך ורק לצורכי _____.
   ב. [...]
   ג. [...]
6. הספק מצהיר בזאת כי בעת התקשרות עם ספק משנה כאמור בסעיף 5, יחתים הספק את ספק המשנה על הסכם התקשרות התואם להוראות תקנה 15 לתקנות אבטחת מידע.
7. הספק מתחייב שלא לבצע שינוי או עיבוד למידע המתקבל מהאוניברסיטה שלא בהתאם להוראות ההתקשרות בין הצדדים.

8. הספק מצהיר ומתחייב בזאת כי עם סיום ההתקשרות, מכל סיבה שהיא, ולכל היותר, בתום תקופת הזמנת העבודה/הסכם השירותים, כל המידע שהגיע לרשותו במסגרת השירותים יוחזר לרשות האוניברסיטה, ככל הניתן, ויימחק מכל אמצעי המדיה שברשותו ו/או ברשות מי מטעמו, ויציג למנהל אבטחת המידע של האוניברסיטה תצהיר חתום על ידי מורשה החתימה של הספק המאמת ביצוע פעולות מחיקה, ביעור והשמדה כאמור.
9. 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.
10. 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.
11. הספק מתחייב להעביר לאוניברסיטה דיווח מידי בכל מקרה של חשש לדליפת המידע מהמאגר או שימוש חורג מההרשאה שניתנה לספק ו/או למי מטעמו.
12. פרטי איש קשר מטעם הספק לצורך עדכון הספק כמקבל מידע ממאגר המידע:
שם מלא: _____; טלפון: _____; כתובת דוא"ל_____.

<u>סודיות:</u>

13. "**מידע**", במסמך זה: כל חומר, מסמך ו/או מידע אחר הנוגע לפעילות האוניברסיטה ו/או חבריה ו/או תלמידיה ו/או עובדיה ו/או עסקיה אשר אינו נחלת כלל הציבור (למעט אם הפך לכזה בשל מעשה/מחדל של הספק) לרבות, מבלי לגרוע מכלליות האמור לעיל, מידע אודות משאבי האוניברסיטה; 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 האוניברסיטה.
14. ידוע לספק כי לצורך המתן 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.
15. הספק מתחייב כי לא הוא ו/או מי מטעמו יגלו מידע שהגיע אליו ו/או למי מטעמו בתוקף תפקידו כעובד, כמנהל או כמחזיק של מאגר מידע, אלא לצורך מטרת השירות או לביצוע החוק או על פי צו בית משפט בקשר להליך משפטי וכי ידועות לו הוראות סעיף 16 לחוק הגנת הפרטיות והוראות סעיף 19 לתקנות אבטחת מידע.
16. הספק מתחייב שלא לעשות כל שימוש, בכל מידע באשר הוא שלא לצורכי ביצוע מטרת השירות.
17. הספק מתחייב כי העברת מידע תהא מוגבלת לעובדים 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.

18. 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.
19. 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.
20. על העותקים של המידע יחולו הוראות התחייבות זו וכל האמור לגבי המידע יחול גם על עותקיו.
21. 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.
22. הספק מתחייב להודיע מיידית לאוניברסיטה בכל מקרה של אובדן מידע כלשהו של האוניברסיטה.
23. למען הסר ספק, מוצהר ומוסכם כי אין בעצם גילוי המידע על ידי האוניברסיטה והעברתו אל הספק כדי להעניק לספק כל זכות במידע.
24. 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.
25. **תוקפה של התחייבות זו אינו מוגבל בזמן.**
26. התחייבות זו לא תחול על מידע אשר התקבל מהאוניברסיטה ואשר הספק יוכיח לגביו בכתובים כי:
    א. המידע היה ידוע לספק לפני קבלת המידע מהאוניברסיטה.
    ב. המידע היה ידוע ברבים או שהיה ניתן להשגה על ידי הציבור הרחב באופן חוקי לפני יום העברתו לספק.
    ג. 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.
    ד. המידע הגיע לספק בדרך חוקית של רכישת זכויות או בכל דרך חוקית שהיא.
27. 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 ואפשרה לו להתגונן כנגדה באופן עצמאי.

<u>דרישות אבטחת מידע</u>

28. הספק יבטיח, בין היתר, שימוש נכון בזיהוי המשתמש ובסיסמא, בהרשאות הגישה למידע, בהגנת משאבי מערכות המחשב והמידע ומערכות התקשורת המכילות מידע השייך לאוניברסיטה, ובאבטחה הפיזית של המידע ומערכות המידע והתקשורת
29. הספק מתחייב לגרוס או להעביר לגריסה מאובטחת מסמכי נייר.
30. הגישה למערכות המחשוב / תיקיות המחזיקות מידע של האוניברסיטה תתאפשר רק תוך שימוש בזיהוי חד ערכי של בעל ההרשאה ושימוש בסיסמאות אישיות וחסויות. הסיסמאות תהיינה ידועות רק למשתמשים בלבד ותוחלפנה לפחות כל 180 יום.

31. משתמש יינעל אוטומטית לאחר 5 ניסיונות גישה כושלים רצופים בהקשת הסיסמא. השחרור יוכל להתבצע רק ע"י משתמש בעל הרשאות ניהול רשת או לאחר שעה.
32. ייושם מידור פנימי בשרת בגישה לספריות וקבצים של האוניברסיטה. הגישה לספריות וקבצים אלה תתאפשר רק למי שעבודתם ותפקידם אצל הספק מחייבים זאת.
33. הספק יתקין תוכנת הגנה תקנית ומעודכנת כנגד נוזקות וקודים זדוניים במחשבים המיועדים לעבודה מול האוניברסיטה, ויעדכנה על פי דרישות היצרן.
34. הספק מתחייב לקיים הגנה נאותה בגלישה באינטרנט ובתקשורת מול גורמי חוץ.
35. הספק מתחייב ליישם הגנה פיזית ובקרת גישה למחשבים, לשרתים ולרכיבי התקשורת.
36. תקשורת הנתונים מול האוניברסיטה תהיה מוצפנת מקצה לקצה באמצעות פרוטוקול TLS 1.2 או פרוטוקול אחר שיאושר על ידי מנהל אבטחת המידע של האוניברסיטה.
37. גיבויים יבוצעו בצורה מסודרת וישמרו במקום סגור ונעול עם גישה לאחראי על הגיבויים בלבד. כמו כן, הספק יגדיר נוהל גיבויים אשר יכלול, לכל הפחות, גיבוי יומי ושמירת גיבויים ולוגים באופן מאובטח, למשך 24 חודשים לכל הפחות.
38. הספק יגדיר תהליך להעברת מידע פיזי באופן מאובטח לאוניברסיטה וממנה.

ולראיה באתי על החתום:

שם + שם משפחה _____ תפקיד _____

תאריך _____ חתימה + חותמת _____

נספח ב'

נספח אבטחת מידע לספק תוכנה

<u>התקשרות עם ספק תוכנה</u>

בהמשך להזמנת העבודה/הסכם השירותים מיום _____, (להלן: "**הזמנת העבודה**"), שנחתמה בין _____ ח.פ _____ (להלן: "**הספק**") לבין אוניברסיטת בר אילן ע"ר 580063683 (להלן: "**האוניברסיטה**") ולאור הוראות תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "**תקנות אבטחת מידע**") הצדדים מעוניינים להוסיף את התנאים הבאים להתקשרותם:

<u>הוראות כלליות:</u>

1. הספק מצהיר כי לשם מתן השירותים אשר פורטו בהזמנת העבודה, האוניברסיטה נדרשת להעביר לספק מידע ממאגרי המידע של האוניברסיטה ו/או לאפשר לספק ולעובדיו גישה למאגרי המידע ו/או למערכות המידע של האוניברסיטה;
2. במסגרת הזמנת העבודה, על הספק לעבד רק את סוגי המידע הבאים:
   א. [...]
   ב. [...]
   וזאת למטרת ביצוע השירותים בלבד, כפי שהוגדרה בהזמנת העבודה ("**מטרת השירות**");
3. העברת מידע בין הספק לאוניברסיטה או להיפך תתבצע באמצעות _____
4. במסגרת הזמנת העבודה הספק אינו רשאי לגשת למערכות המידע / במסגרת הזמנת העבודה הספק רשאי לגשת אך ורק למערכות המידע הבאות *(מחק את המיותר)*:
   א. [...]
   ב. [...]
5. הספק לא יעביר וכן לא יאפשר גישה ו/או הרשאות צפייה ו/או הרשאות עיבוד כלשהן לגבי המידע המפורט בסעיף 2 לאף גורם מבלי שקיבל את אישור האוניברסיטה מראש ובכתב. לשם כך, ולצורך ביצוע השירותים המפורטים בהזמנת העבודה בלבד, האוניברסיטה מאשר לספק להתקשר עם ספקי המשנה הבאים:
   א. [...] העברה אך ורק לצורכי _____.
   ב. [...]
   ג. [...]
6. הספק מצהיר בזאת כי בעת התקשרות עם ספק משנה כאמור בסעיף 5, יחתים הספק את ספק המשנה על הסכם התקשרות התואם להוראות תקנה 15 לתקנות אבטחת מידע.
7. הספק מצהיר ומתחייב בזאת כי עם סיום ההתקשרות, מכל סיבה שהיא, ולכל היותר, בתום תקופת הזמנת העבודה/הסכם השירותים, כל המידע שהגיע לרשותו במסגרת השירותים יוחזר לרשות האוניברסיטה, ככל הניתן, ויימחק מכל אמצעי המדיה שברשותו ו/או ברשות מי מטעמו, ויציג

למנהל אבטחת המידע של האוניברסיטה תצהיר חתום על ידי מורשה החתימה של הספק המאמת ביצוע פעולות מחיקה, ביעור והשמדה כאמור.

8. הספק מתחייב לפעול על פי כל דין, לרבות הוראות חוק הגנת הפרטיות, תשמ"א-1981 (להלן: "החוק"), התקנות שהותקנו לפיו, הנחיות רשם מאגרי המידע והרשות להגנת הפרטיות וכיוצא בזאת, ולפי הוראות שיתקבלו מעת לעת על ידי האוניברסיטה.
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 לאוניברסיטה דיווח מידי 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 האוניברסיטה ו/או חבריה ו/או תלמידיה ו/או עובדיה ו/או עסקיה אשר אינו נחלת כלל הציבור (למעט אם הפך לכזה בשל מעשה/מחדל של הספק) לרבות, מבלי לגרוע מכלליות האמור לעיל, מידע אודות משאבי האוניברסיטה; 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 האוניברסיטה.
12. ידוע לספק כי לצורך המתן 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 שלא לעשות כל שימוש, בכל מידע באשר הוא שלא לצורכי ביצוע מטרת השירות.
14. הספק מתחייב כי העברת מידע תהא מוגבלת לעובדים 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.
15. 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.
16. 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.
17. על העותקים של המידע יחולו הוראות התחייבות זו וכל האמור לגבי המידע יחול גם על עותקיו.
18. 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.
19. הספק מתחייב להודיע מיידית לאוניברסיטה בכל מקרה של אובדן מידע כלשהו של האוניברסיטה.

20. למען הסר ספק, מוצהר ומוסכם כי אין בעצם גילוי המידע על ידי האוניברסיטה והעברתו אל הספק כדי להעניק לספק כל זכות במידע.
21. 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.
22. **תוקפה של התחייבות זו אינו מוגבל בזמן.**
23. התחייבות זו לא תחול על מידע אשר התקבל מהאוניברסיטה ואשר הספק יוכיח לגביו בכתובים כי:
    א. המידע היה ידוע לספק לפני קבלת המידע מהאוניברסיטה.
    ב. המידע היה ידוע ברבים או שהיה ניתן להשגה על ידי הציבור הרחב באופן חוקי לפני יום העברתו לספק.
    ג. 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.
    ד. המידע הגיע לספק בדרך חוקית של רכישת זכויות או בכל דרך חוקית שהיא.
24. 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 הודיע לספק על התביעה ו/או הדרישה ואפשרה לו להתגונן כנגדה באופן עצמאי.

<u>דרישות אבטחת מידע</u>

25. **הנחיות כללית:**
    א. 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.
    ב. הספק יבטיח, בין היתר, שימוש נכון בזיהוי המשתמש ובסיסמא, בהרשאות הגישה למידע ובהגנת משאבי מערכות המחשב והמידע ומערכות התקשורת המכילות מידע השייך לאוניברסיטה או המשמשים להתחברות לאוניברסיטה ו/או למידע של האוניברסיטה המאוחסן בשירותי ענן.
    ג. הספק יבצע הדרכה פרונטלית על התוכנה עפ"י דרישת האוניברסיטה.
    ד. הספק יתקין תוכנת הגנה תקנית ומעודכנת נגד נוזקות על מחשבים המכילים מידע השייך לאוניברסיטה.

26. **פיתוח מאובטח:**
    א. שימוש בתקן OWASP או תקן מקביל שיאושר ע"י האוניברסיטה.
    ב. שימוש בגרסאות מעודכנות ונתמכות של שפות הפיתוח.
    ג. העברת מסמך אפיון מערכת לאישור מנהל אבטחת מידע של האוניברסיטה.

ד. פיתוח המערכת בהתאם לדרישות האפיון.

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

ו. מבדק חדירה למערכת לפני העברה לייצור.

27. הזדהות והרשאות:

א. שימוש במדיניות סיסמאות חזקה המורכבת מאותיות וספרות, אורך סיסמא מינימלי של 8 תווים, ו/או מתן אפשרות לקישור המערכת ל-AD של האוניברסיטה, לבקשת האוניברסיטה.

ב. הסיסמאות תוחלפנה לפחות כל 6 חדשים.

ג. הסיסמאות תוצפנה בהצפנה חד כיוונית בבסיס הנתונים.

ד. היסטוריית סיסמאות – לפחות 10 דורות אחורה.

ה. יכולת להגדיר הרשאות על פי פרופיל ולמדר גישה/עדכון ברמת שדה.

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

ז. יישום תיעוד לכל שינוי בטבלת ההרשאות.

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

28. תיעוד בלוג:

א. זיהוי ואימות;

ב. נעילות משתמש;

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

ד. העלאות תכנים;

ה. גישה מרחוק;

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

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

29. בקרת קלט- פלט:

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

ב. שימוש בפרוטוקול Https בכל דפי היישום.

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

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

ה. 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.

ו. 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. הפרדת סביבות:

א. סביבת הייצור תופרד מסביבות אחרות.

ב. העברת אפליקציה מסביבת פיתוח לייצור תתבצע בצורה מבוקרת.

ג. לא יעשה שימוש בנתונים אמיתיים בסביבת הפיתוח.

31. אבטחת תשתיות:

א. מענה אנושי לטיפול באירועי סייבר.

ב. 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.

32. דרישות נוספות במקרה של פעילות בענן:

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 _____

נספח ב'

נספח אבטחת מידע לספק מחזיק מאגר

<u>התקשרות עם ספק מחזיק מאגר מידע</u>

בהמשך להזמנת העבודה/הסכם השירותים מיום _____, (להלן: "**הזמנת העבודה**"), שנחתמה בין _____ ח.פ _____ (להלן: "**הספק**") לבין אוניברסיטת בר אילן ע"ר 580063683 (להלן: "**האוניברסיטה**") ולאור הוראות תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "**תקנות אבטחת מידע**") הצדדים מעוניינים להוסיף את התנאים הבאים להתקשרותם:

<u>הוראות כלליות:</u>

39. הספק מצהיר כי לשם מתן השירותים אשר פורטו בהזמנת העבודה, האוניברסיטה נדרשת להעביר לספק מידע ממאגרי המידע של האוניברסיטה ו/או לאפשר לספק ולעובדיו גישה למאגרי המידע ו/או למערכות המידע של האוניברסיטה;
40. במסגרת הזמנת העבודה, על הספק לעבד רק את סוגי המידע הבאים:
    א. [...]
    ב. [...]

    וזאת למטרת ביצוע השירותים בלבד, כפי שהוגדרה בהזמנת העבודה ("**מטרת השירות**");
41. העברת מידע בין הספק לאוניברסיטה או להיפך תתבצע באמצעות _____
42. במסגרת הזמנת העבודה הספק אינו רשאי לגשת למערכות המידע / במסגרת הזמנת העבודה הספק רשאי לגשת אך ורק למערכות המידע הבאות (מחק את המיותר):
    א. [...]
    ב. [...]
43. הספק לא יעביר וכן לא יאפשר גישה ו/או הרשאות צפייה ו/או הרשאות עיבוד כלשהן לגבי המידע המפורט בסעיף 2 לאף גורם מבלי שקיבל את אישור האוניברסיטה מראש ובכתב. לשם כך, ולצורך ביצוע השירותים המפורטים בהזמנת העבודה בלבד, האוניברסיטה מאשרת לספק להתקשר עם ספקי המשנה הבאים:
    א. [...] העברה אך ורק לצורכי _____.
    ב. [...]
    ג. [...]
44. הספק מצהיר בזאת כי בעת התקשרות עם ספק משנה כאמור בסעיף 5, יחתים הספק את ספק המשנה על הסכם התקשרות התואם להוראות תקנה 15 לתקנות אבטחת מידע.
45. הספק מצהיר ומתחייב בזאת כי עם סיום ההתקשרות, מכל סיבה שהיא, ולכל היותר, בתום תקופת הזמנת העבודה/הסכם השירותים, כל המידע שהגיע לרשותו במסגרת השירותים יוחזר לרשות האוניברסיטה, ככל הניתן, יימחק מכל אמצעי המדיה שברשותו ו/או ברשות מי מטעמו, ויציג למנהל

אבטחת המידע של האוניברסיטה תצהיר חתום על ידי מורשה החתימה של הספק המאמת ביצוע פעולות מחיקה, ביעור והשמדה כאמור.

46. 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.
47. 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.
48. הספק מתחייב להעביר דיווח מידי לאוניברסיטה בכל מקרה של חשש לדליפת המידע מהמאגר או שימוש חורג מההרשאה שניתנה לספק ו/או למי מטעמו.
49. הספק מתחייב לדווח לאוניברסיטה, אחת לשנה לפחות, על אופן ביצוע חובותיו לפי תקנות אבטחת מידע ולפי הסכם זה.
50. פרטי איש קשר מטעם הספק לצורך עדכון הספק כמחזיק במאגר המידע: שם מלא: _____ ; טלפון: _____ ; כתובת דוא"ל_____.

סודיות:

51. "**מידע**", במסמך זה: כל חומר, מסמך ו/או מידע אחר הנוגע לפעילות האוניברסיטה ו/או חבריה ו/או תלמידיה ו/או עובדיה ו/או עסקיה אשר אינו נחלת כלל הציבור (למעט אם הפך לכזה בשל מעשה/מחדל של הספק) לרבות, מבלי לגרוע מכלליות האמור לעיל, מידע אודות משאבי האוניברסיטה; 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 האוניברסיטה.
52. 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.
53. הספק מתחייב כי לא הוא ו/או מי מטעמו יגלו מידע שהגיע אליו ו/או למי מטעמו בתוקף תפקידו כעובד, כמנהל או כמחזיק של מאגר מידע, אלא לצורך מטרת השירות או לביצוע החוק או על פי צו בית משפט בקשר להליך משפטי וכי ידועות לו הוראות סעיף 16 לחוק הגנת הפרטיות והוראות סעיף 19 לתקנות אבטחת מידע.
54. הספק מתחייב שלא לעשות כל שימוש, בכל מידע באשר הוא שלא לצורכי ביצוע מטרת השירות.
55. הספק מתחייב כי העברת מידע תהא מוגבלת לעובדים 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.
56. 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.

57. 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.
58. על העותקים של המידע יחולו הוראות התחייבות זו וכל האמור לגבי המידע יחול גם על עותקיו.
59. הספק מתחייב כי בכל מקרה שיתעוררו ספקות כלשהן בנוגע לתוכן התחייבויותיו לפי כתב התחייבות זה, וקיומו, יפנה לאוניברסיטה בכתב לקבלת אישורה. ידוע לספק כי אין בנאמר בפסקה זו לגרוע מכל התחייבות מהתחייבויותיו המנויות בכתב התחייבות זה.
60. הספק מתחייב להודיע מיידית לאוניברסיטה בכל מקרה של אובדן מידע כלשהו של האוניברסיטה.
61. למען הסר ספק, מוצהר ומוסכם כי אין בעצם גילוי המידע על ידי האוניברסיטה והעברתו אל הספק כדי להעניק לספק כל זכות במידע.
62. 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.
63. **תוקפה של התחייבות זו אינו מוגבל בזמן.**
64. התחייבות זו לא תחול על מידע אשר התקבל מהאוניברסיטה ואשר הספק יוכיח לגביו בכתובים כי:
    א. המידע היה ידוע לספק לפני קבלת המידע מהאוניברסיטה.
    ב. המידע היה ידוע ברבים או שהיה ניתן להשגה על ידי הציבור הרחב באופן חוקי לפני יום העברתו לספק.
    ג. 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.
    ד. המידע הגיע לספק בדרך חוקית של רכישת זכויות או בכל דרך חוקית שהיא.
65. 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 ואפשרה לו להתגונן כנגדה באופן עצמאי.

<u>דרישות אבטחת מידע</u>

66. תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "**התקנות**" או "**תקנות אבטחת מידע**")[2] חלות הן על בעל מאגר מידע (האוניברסיטה), והן על מחזיק מאגר מידע (הספק).
67. מנהל אבטחת המידע של האוניברסיטה רשאי להחמיר או להקל באחד או יותר מהסעיפים הבאים לפי שיקול דעתו, ובהתאם למידע הקיים או מעובד אצל הספק.
68. **הנחיות כללית:**

א. בהתקיים חובה חוקית לפי התנאים המפורטים בסעיף 17ב לחוק הגנת הפרטיות, הספק ימנה ממונה על אבטחת המידע (להלן: "**הממונה**"). הממונה יבטיח, בין היתר, שימוש נכון בזיהוי המשתמש ובסיסמא, בהרשאות הגישה למידע ובהגנת משאבי מערכות המחשב והמידע

[2] https://www.nevo.co.il/law_html/law01/501_600.htm

ומערכות התקשורת המכילות מידע השייך לאוניברסיטה. במידה שלא חלה חובה חוקית למינוי ממונה, הספק ימנה גורם מטעמו שיהיה אחראי לאבטחת המידע וסייבר.

ב. הספק יגדיר נוהל אבטחת מידע, כמפורט בתקנה 4 לתקנות אבטחת המידע.

ג. הספק יגדיר מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי מעודכנת של מערכות המאגר, הכל בהתאם למפורט בתקנה 5 לתקנות אבטחת המידע.

ד. הספק יבצע סקר סיכונים ומבדק חדירה למאגרי מידע שחלה עליהם רמת אבטחה גבוהה, אחת ל-18 חודשים לכל הפחות.

69. אבטחה פיסית וסביבתית:

א. הספק ישמור את מאגרי המידע וכן את התשתיות והמערכות המשמשות את המאגרים, במקום מוגן, המונע חדירה וכניסה אליו ללא הרשאה והתואם את אופי פעילות המאגר ורגישות המידע.

ב. הספק יבצע בקרה ותיעוד של הכניסה והיציאה מאתרים בהם מצויות מערכות המידע וכן בקרה ותיעוד של הכנסה והוצאת ציוד אל מערכות המאגר ומהן, וישמור תיעוד זה למשך 24 חודשים לכל הפחות.

70. אבטחת מידע בניהול כוח אדם:

א. הספק יחתים את בעלי ההרשאות מטעמו על הצהרות סודיות הכוללות, בין היתר, התחייבות לשמירה מוחלטת על סודיות המידע של האוניברסיטה, שימוש במידע רק בהתאם לאמור בהסכם ההתקשרות בין הספק לאוניברסיטה ויישום אמצעי האבטחה הקבועים בהסכם ההתקשרות, לרבות נספח זה.

ב. הספק ייתן וישנה הרשאות גישה למידע המצוי במאגר המידע רק לאחר נקיטת אמצעים סבירים, המקובלים בהליכי מיון ושיבוץ עובדים.

ג. הספק יקיים הדרכות לבעלי הרשאות גישה למידע מטעמו המצוי במאגרי המידע, בטרם מתן ההרשאות או בטרם שינוי ההרשאות הקיימות. ההדרכות יעסקו בחובות לפי חוק הגנת הפרטיות, תקנות אבטחת המידע ומסירת מידע אודות חובות בעלי ההרשאות לפי החוק ולפי נוהל האבטחה של הספק.

ד. הספק יקיים הדרכה תקופתית לבעלי ההרשאות מטעמו למאגרי המידע של האוניברסיטה בנושא מסמך הגדרות המאגר, נוהל האבטחה של הספק והוראות אבטחת המידע לפי החוק ותקנות אבטחת המידע ובדבר החובות של בעלי ההרשאות לפיהם. ההדרכה תיערך לכל הפחות אחת לשנתיים ובהסמכה של בעל הרשאה לתפקיד חדש, סמוך ככל האפשר למועד הסמכתו.

71. הזדהות וניהול הרשאות:

א. הספק יוודא מתן הרשאות גישה לבעלי הרשאות מטעמו למאגרי המידע ולמערכות המאגרים, בהתאם להגדרות התפקיד ובמידה הנדרשת לביצוע התפקיד בלבד, לרבות מידור גישה / עדכון ברמת שדה.

ב. הספק יבצע בקרת הרשאות לכל הפחות אחת לשנה לבעלי ההרשאות מטעמו. במידה שהספק יפתח מערכת עבור האוניברסיטה, הספק יוודא יכולת הפקה יזומה של דו"ח הרשאות תקפות עפ"י דרישת האוניברסיטה.

ג. אופן זיהוי בעל הרשאה במחשבי הספק, המשמשים גישה למידע של האוניברסיטה ו/או מכילים מידע של האוניברסיטה, יעמוד בקריטריונים הבאים:

- ככל הניתן, אופן הזיהוי ייעשה על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה.
- שימוש במדיניות סיסמאות חזקה המורכבת מאותיות וספרות, ובעלת אורך סיסמא מינימלי של 8 תווים.
- החלפת סיסמאות לפחות כל 6 חודשים.
- הגדרת מספר ניסיונות הקשה שגויים של סיסמא בטרם נעילת המשתמש (לכל היותר 5).
- הגדרת Session Time Out לאחר פרק זמן של אי פעילות, המחייב זיהוי מחדש של המשתמש. ברירת המחדל לסיום Session תהיה 30 דקות (גם אם המערכת תנוהל מקומית).
- הצפנת הסיסמאות בהצפנה חד כיוונית בבסיס הנתונים.
- גישת אדמין (מנהל מערכת) תהיה באמצעות אימות רב שלבי (MFA).
- יישום תיעוד לכל שינוי בטבלת ההרשאות.
- הגדרת אופן טיפול בתקלות הקשורות באימות זהות.
- ביטול הרשאות לבעל הרשאה שסיים את תפקידו ובמידת האפשר שינוי סיסמאות למאגר ולמערכות המאגר, שבעל ההרשאה עשוי היה לדעת, מיד עם סיום תפקידו של בעל ההרשאה.

72. בקרה ותיעוד גישה:

א. הספק יתעד בלוג את השדות הבאים:

- זיהוי ואימות;
- נעילות משתמש;
- פעולות עדכון ע"י המשתמשים כולל שמירת ערך קודם;
- העלאות תכנים;
- גישה מרחוק;
- תיעוד כל מקרה שבו התגלה אירוע אבטחת מידע. ככל האפשר יבוסס התיעוד על רישום אוטומטי.

ב. הספק ישמור את הלוגים הנ"ל באופן מאובטח, למשך 24 חודשים, לכל הפחות.

ג. הספק יגדיר נוהל בדיקה שגרתי של הלוגים למנגנון הבקרה כולל דו"ח של הבעיות שהתגלו והצעדים שננקטו בעקבותיהן.

73. אירועי אבטחת מידע:

א. הספק יגדיר הוראות בנוהל האבטחה שלו לעניין התמודדות עם אירועי אבטחת מידע, לפי חומרת האירוע ומידת רגישות המידע, לרבות לעניין ביטול הרשאות וצעדים מיידיים אחרים

הנדרשים וכן הוראות לעניין דיווח למנהל אבטחת המידע של האוניברסיטה על אירועי אבטחה ועל הפעולות שננקטו בעקבותיהם.

ב. הספק ידווח גם לרשם מאגרי מידע אודות אירוע אבטחה חמור. הספק ישמור את התיעוד באופן מאובטח, למשך 24 חודשים לכל הפחות.

ג. הספק יקיים דיון באירועי האבטחה ויבחן את הצורך בעדכון נהלי האבטחה שלו, במאגרים שחלה עליהם רמת אבטחה בינונית, אחת לשנה לפחות. במאגרים שחלה עליהם רמת אבטחה גבוהה, אחת לרבעון לפחות.

74. ניהול מאובטח ומעודכן:

א. הספק יגביל / ימנע אפשרות חיבור התקנים ניידים וינקוט אמצעי הגנה.

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

ג. הספק יישם בקרות קלט ופלט.

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

ה. הספק יבצע הפרדה בין הנתונים של האוניברסיטה לבין נתונים של לקוחות אחרים. הפרדה כאמור יכולה להיות לוגית, תוך מתן הסבר למנהל אבטחת המידע של האוניברסיטה על אופן ההפרדה.

ו. הספק יישם הגנות על בסיס הנתונים והקשחות עפ"י הנחיות היצרן.

ז. הספק יוודא ניטור שינויים בבסיסי הנתונים והפקת דו"ח למנהל אבטחת המידע של האוניברסיטה לפי דרישתו.

ח. זמינות מרבית – הספק ידווח לאיש הקשר באוניברסיטה על כל השבתה של המערכת.

ט. הספק ישמור את המידע כל עוד נמשך השירות.

י. 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.

75. אבטחת תקשורת:

א. הספק ינקוט באמצעי אבטחה הולמים, בהתאם לרמת רגישות המידע, שימנעו חדירה מכוונת או מקרית למערכת או אל קווי התקשורת בין האוניברסיטה אל הספק (לכל הפחות Firewall- ו-IPS, הצפנה בפרוטוקול TLS 1.2 ומעלה).

ב. 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.

ג. בגישה מרחוק, באמצעות רשת האינטרנט או רשת ציבורית אחרת, הספק יעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של בעל ההרשאה שמטרת לזהות את המתקשר והמאמת את

הרשאתו לביצוע הפעילות מרחוק ואת היקפה (לדוגמה: OTP, גישה מכתובת IP קבועה, טוקן, וכיו"ב).

76. ביקורות תקופתיות:

הספק יערוך ביקורת פנימית או חיצונית, לעניין עמידתו בתקנות אבטחת מידע, אחת לשנתיים לפחות. הביקורת תיערך ע"י גורם בעל הכשרה מתאימה לביקורת בנושא אבטחת מידע, שאיננו אחראי האבטחה על המאגרים.

77. גיבויים ושחזורים:

הספק יגדיר נוהל לביצוע גיבויים ושחזורים של נתוני האבטחה, בהתאם לתקנות 17 ו-18 לתקנות אבטחת מידע.

78. דרישות נוספות במקרה של פעילות בענן:

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

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

ג. 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 פרוטוקול TLS1.2 ומעלה או פרוטוקול אחר שיאושר ע"י מנהל אבטחת המידע של האוניברסיטה.

ד. נדרשת הצפנת שדות מידע רגיש ברמת ה-DB + ניהול מפתחות הצפנה והחלפת מפתחות אחת לשנה לפחות.

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

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

ולראיה באתי על החתום:

שם + שם משפחה _____ תפקיד_____

תאריך _____ חתימה + חותמת _____