# כתב התחייבות – ספק מיקור חוץ

# אבטחת מידע והגנת הפרטיות

## רקע

כתב ההתחייבות המצורף כולל דרישות בתחום אבטחת המידע והגנת הפרטיות וחתימת הספק עליו הינו מתחייב בכדי להמשיך בהתקשרות שבין **האוניברסיטה תל אביב** לבין **ספק השירות**, תוך עמידה בדרישות הדין, החוק, ההוראות והתקנות עליהן כפופה האוניברסיטה.

## הנחיות למילוי וחתימה על כתב ההתחייבות

1. על הספק לוודא שהוא עומד בכלל הדרישות בכתב התחייבות זה לפי אופן הפעילות והשרות הניתן לאוניברסיטה על ידי הספק:
   a. **מיקור חוץ** יש למלא סעיפים 0-34
   b. **עבודה בחצרות האוניברסיטה** יש למלא סעיפים 0-9, 13, 26, 32-34
   c. **גישה מרחוק** יש למלא סעיפים 0-9, 13, 18, 20, 22, 23, 26, 32-34
   d. **טיפול במידע** יש למלא סעיפים 0-34
   e. **פיתוח תוכנה** יש למלא סעיפים 0-9, 13, 22, 27-34
2. בתחתית עמוד זה, יש למלא את פרטי הספק, מורשה החתימה מטעמו ולהוסיף את חתימת מורשה החתימה וחותמת הספק.
3. יש לשלוח עותק סרוק של כתב ההתחייבות בתוך 14 יום מקבלתו, לאחר שהספק מילא את הפרטים הנדרשים וחתם עליו, לכתובת דואר האלקטרוני: ciso@tau.ac.il מנהל תחום אבטחת מידע והגנת סייבר באוניברסיטה.

| **שם הספק** | | **ח.פ./ח.צ./ע"ר/ת.ז.** | |
|---|---|---|---|
| | | | |
| **אישור הספק** | | | |
| אנו מאשרים כי כתב התחייבות זה נחתם על-ידי מר. _____ מספר זהות _____ ביום _____ ולאחר שהסברנו לו את משמעות חתימתו על כתב התחייבות זה כלפי האוניברסיטה תל אביב והצהרתו כי הוא נציג של הספק המוסמך מטעמו לחתום על כתב התחייבות זו, חתם על כתב התחייבות זה בשם הספק, מרצונו החופשי . | | | |
| | | | |
| **שם מורשה החתימה ותפקיד** | | | **חתימה וחותמת הספק** |

חתימת גורם מוסמך מתאם הספק_____

# כתב התחייבות – ספק שירות

# אבטחת מידע והגנת הפרטיות

**0. כללי**

0.1. כתב התחייבות זה מושתת על הוראות חוק הגנת הפרטיות, התשמ"א – 1981 ("**חוק הגנת הפרטיות**"), תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017 ("**תקנות אבטחת המידע**"), תקנות נוספות מכוח חוק הגנת הפרטיות, הנחיית רשם מאגרי המידע 2/2011 – שימוש בשירותי מיקור חוץ לעיבוד מידע, הנחיות רלבנטיות נוספות של רשם מאגרי המידע ("**ההנחיות**") וכל חוק, תקנות והנחיות בקשר עם עיבוד מידע אישי במיקור חוץ, ככל שקיימים ושיהיו בעתיד (יחד – "**החוק**").

0.2. הוראות כתב התחייבות זה אינן ממעטות מהוראות החוק. מקום בו החוק מציב דרישות מהספק העודפות על הוראות כתב התחייבות זה, תחולנה הדרישות כאמור בנוסף על הוראות כתב התחייבות זה. הנספחים לכתב התחייבות זה מהווים חלק בלתי נפרד ממנו. הוראות כתב התחייבות זה גוברות על הוראות ההסכם וכל הסכם נוסף, התחייבות ומסמך אחר בעל תוקף משפטי בין הספק ומי מטעמו לאוניברסיטה ומי מטעמה.

0.3. במהלך מתן השירותים כהגדרתם בהסכם שבין הספק לבין **אוניברסיטה תל-אביב** (להלן "**האוניברסיטה**"), חברת האם, חברות בנות של האוניברסיטה וכל אוניברסיטה הקשורה אליהן, בהתאם למצוין בהסכם ("**השירותים**", "**ההסכם**", "**הספק**" ו"**האוניברסיטה**" בהתאמה), מבצע הספק פעולות ותהליכים במידע עבור האוניברסיטה.

0.4. לצורך כתב התחייבות זה, "**מידע**" הוא כל מידע, נתונים וידע, המצויים כעת ושימצאו בעתיד בידי הספק או בידי מי מטעמו, או שיש או תהיה לספק או למי מטעמו גישה למידע, נתונים וידע כאמור, הקשורים, או נוגעים לאוניברסיטה, לתפעולה, לפעילותה, לתלמידיה, עובדיה, מנהליה, ספקיה, לכל צד שלישי מטעמה ולכל אוניברסיטה, תאגיד וארגון הקשור אליה. בכלל זה, "מידע" יכלול את המונח "מידע" כהגדרתו בחוק הגנת הפרטיות.

0.5. ידוע לספק כי המידע הינו מנכסיה העיקריים והחיוניים ביותר של האוניברסיטה והוא מבין שמתן השירותים מחייב הקפדה יתרה על הוראות חוק הגנת הפרטיות, תקנות אבטחת המידע ההנחיות ושמירתו המאובטחת של המידע בתנאי אבטחת מידע, סודיות ודיסקרטיות מלאים.

לפיכך, הספק מצהיר ומתחייב כלפי האוניברסיטה, כדלקמן –

1. **<u>הצהרות והתחייבויות לאוניברסיטה לעניין קיום חוק הגנת הפרטיות:</u>**

1.1. הספק מצהיר בזאת כי הוא מקיים ויקיים את הוראות חוק הגנת הפרטיות, התשמ"א-1981 (בכתב התחייבות זה: "חוק הגנת הפרטיות") ובכלל זה כל חקיקת משנה והנחיות כפי שתהיינה מעת לעת לפי חוק הגנת הפרטיות ו/או תוצאנה על ידי רשם מאגרי המידע ו/או רשות להגנת הפרטיות.

1.2. מבלי לגרוע מכלליות האמור לעיל, הספק מתחייב לקיים הוראות כאמור כפי שתחולנה מעת לעת ביחס למחזיק כהגדרתו בחוק הגנת הפרטיות.

1.3. מבלי לגרוע מכל זכות הקיימת לאוניברסיטה, מכוח כל דין והסכם, הספק נותן בזאת את הסכמתו לאוניברסיטה להעביר לגורם מאסדר את החוזה ואת כתב התחייבות זה.

2. **<u>ממונה על אבטחת מידע והגנת הסייבר</u>**



חתימת גורם מוסמך מטעם הספק_____

2.1. הספק מצהיר כי מונה על ידיו ממונה על אבטחת מידע והגנת הסייבר, וכי יכהן אצלו ממונה כזה למשך כל תקופת ההתקשרות על פי החוזה, ובכלל זה כל תקופת הארכה, וכן במשך 90 יום לאחר סיום החוזה מכל סיבה שהיא.

2.2. הנהלת הספק תקבע את תחומי אחריותו של הממונה על אבטחת המידע והגנת הסייבר ואת הנושאים שהחלטות לגביהם טעונות התייחסותו. תחומי אחריותו יכללו, בין היתר:

2.2.1. אחריות כוללת ליישום מדיניות אבטחת המידע והגנת הסייבר אצל ספק;

2.2.2. פיתוח תוכניות אבטחת המידע והגנת הסייבר אצל הספק, מעקב אחר יישומן, ובחינה של אפקטיביות מערכות אבטחת המידע והגנת הסייבר של הספק;

2.2.3. טיפול באירועים חריגים בתחום אבטחת המידע והגנת הסייבר.

2.3. הספק יעמיד לרשות הממונה על אבטחת המידע והגנת הסייבר את המשאבים הדרושים לו לשם מילוי תפקידו.

2.4. הממונה על אבטחת המידע והגנת הסייבר יהיה בעל הכשרה מקצועית וניסיון רלוונטיים בתחום עיסוקו.

3. **<u>מטרות השימוש במידע</u>**

3.1. הספק רשאי לעשות שימוש במידע לצורך מתן השירותים, כפי שאלו הוגדרו בהסכם, בלבד.

3.2. הספק לא רשאי לדרוש מידע שאינו נדרש לצורך ביצוע השירותים.

3.3. הספק איננו רשאי לעשות כל שימוש במידע, שנמסר ל על ידי האוניברסיטה או מי מטעמה, או נאסף על ידו עבור האוניברסיטה או מי מטעמה, אלא לצורך מתן השירותים.

3.4. הספק לא יעביר את המידע לצד שלישי, ללא הסכמה מפורשת, בכתב ומראש של האוניברסיטה.

3.5. הספק לא ישמור, העתק של מידע שנמסר לו על ידי האוניברסיטה, או שנאסף עבורה או עבור מי מטעמה, אלא על פי הנחיות האוניברסיטה.

3.6. הספק לא יצור כל מאגר מידע מכל סוג שהוא מהמידע שהועבר לו על ידי האוניברסיטה.

4. **<u>איסוף מידע</u>**

4.1. אם במהלך אספקת השירותים, יעסוק הספק באיסוף מידע במישרין מנושאי מידע, אזי, מבלי לגרוע מהוראת כל דין, הספק מתחייב:

4.1.1. לקיים את חובת ההודעה כלפי כל נושא מידע שאליו נעשית פניה לאיסוף מידע, בהתאם לקבוע בסעיף 11 לחוק הגנת הפרטיות.

4.1.2. להביא את נוסח ההודעה לאישורה של האוניברסיטה קודם לאיסוף המידע.

4.1.3. להימנע לחלוטין מאיסוף מידע או מגישה למידע שלא כדין, לרבות תוך שימוש במאגרי מידע בלתי חוקיים.

5. **<u>גילוי על פי הוראת רשות מוסמכת:</u>**

5.1. במקרה בו הספק יחויב לגלות לרשות מוסמכת את מידע של האוניברסיטה המאוחסן על גבי המערכות התפעוליות של הספק, על פי הוראה של רשות מוסמכת על פי דין, הספק יהיה רשאי לגלות לרשות המוסמכת את המידע אותו חוייב לגלות כאמור, ובלבד שהספק הודיעה לרשות המוסמכת כאמור על התחייבויות הספק בכתב התחייבות זה וכן הודיעה לאוניברסיטה על קבלת הדרישה למסירת המידע, מייד עם קבלת הדרישה.

5.2. במקרה בו קיימת מניעה על פי דין למתן הודעה על ידי הספק לאוניברסיטה כאמור, תודיע הספק לאוניברסיטה על קבלת הדרישה למסירת המידע, מייד עם הסרת המניעה.

6. **<u>גישה למידע על ידי האוניברסיטה ומסירת מידע לרשויות</u>**

6.1. בכל עת במהלך ההסכם ולאחריו, כל עוד הספק מחזיק במידע עבור או מטעם האוניברסיטה, יאפשר הספק גישה לאוניברסיטה ולמי מטעמה למידע ולנתונים אודות המידע מתוך מערכות המידע של הספק ומי מטעמו, בהתאם להנחיות האוניברסיטה ביחס לאופן מתן הגישה, ובהעדר הנחיות כאמור – באמצעי גישה סבירים ומקובלים.

6.2. ידוע לספק שהאוניברסיטה עשויה להידרש למסור כל מידע, נתונים ומסמכים בקשר להסכם ולכתב התחייבות זה, לרשות להגנת הפרטיות.

7. **<u>מיפוי, ניהול נכסי מידע ונהלים</u>**

7.1. הספק יערוך, ינהל ויעדכן אחת לשנה לפחות את מסמכי מבנה מאגר והגדרות מאגר בהתאם לתקנות אבטחת המידע וכן רשימה של נכסי המידע שברשותו או בשליטתו. הספק יעביר עותק מרשימת נכסי המידע למחלקת מערכות המידע של האוניברסיטה, אחת לשנה לפחות ובהתאם לבקשת האוניברסיטה.

7.2. הספק יערוך, ינהל, יעדכן אחת לשנה לפחות ובהתאם להנחיות האוניברסיטה, ויוודא שכל מורשי הגישה מטעמו פועלים בהתאם לנהלי אבטחת מידע, הכוללים את כלל הדרישות בהתאם לתקנות אבטחת המידע ובכתב התחייבות זה.

8. **<u>אחזקת מאגרי מידע</u>**

8.1. מלוא המידע המצוי במאגרי המידע של האוניברסיטה אשר בידי הספק או שיש לספק גישה אליהם במסגרת ההתקשרות בינו לבין האוניברסיטה, הינו בבעלות האוניברסיטה על כל המשתמע מכך. הספק מתחייב שכל גישה שלו, או של מי מטעמו, למידע ולמאגר המידע, תתבצע אך ורק בהתאם להוראות האוניברסיטה ולמטרות אשר הוגדרו לו על ידי האוניברסיטה במסגרת ההתקשרות.

8.2. הספק מתחייב שהוא, או מי מטעמו, יקפיד כי כל איסוף מידע או שימוש בו יבוצע אך ורק בהתאם להוראות החוק והדין, ועל פי הנחיות האוניברסיטה.

8.3. ככל שהספק שומר מידע נוסף כלשהו מעבר למידע אשר הוגדר במפורש על ידי האוניברסיטה, עליו לבצע את השמירה ואת ההגנה על המידע בהתאם להוראות החוק, התקנות והנחיות רשות להגנת הפרטיות הרלוונטיות, לרבות בנוגע לרישום מאגרים, בהתאם לצורך.

8.4. הספק יפריד ויחצוץ לוגית במערכות המידע שלו, ככל שניתן באמצעות הפרדה לוגית, בין הפעילות שהוא מבצע עבור האוניברסיטה במסגרת מתן השירותים לבין כל פעילות עיבוד מידע אחרת שהוא מבצע עבור עצמו או עבור צדדים שלישיים.

8.5. אם הספק מחזיק במאגרי מידע של בעלים שונים, הספק יוודא שאפשרות הגישה לכל מאגר תהיה נתונה רק למי שהורשו לכך במפורש בהסכם בכתב בינה לבין בעליו של אותו מאגר.

9. **<u>אי עיסוק בסחר במידע</u>**

9.1. הספק מצהיר ומתחייב כי הוא איננו עוסק באספקת שירותי דיוור ישיר, כמשמעותם בחוק, או בכל מכירה, הפצה או סחר במידע כהגדרתם בחוק.

10. **<u>מימוש זכות העיון, תיקון ומחיקה</u>**

10.1. פנה נושא מידע לספק בבקשה למימוש זכותו בחוק לעיין, לתקן ולמחוק מידע שעליו, הנמצא בחזקת הספק, יודיע הספק למבקש אם הספק מחזיק מידע עליו וכן את שם האוניברסיטה ומענה.

10.2. הספק יודיע לאוניברסיטה בכתב על כל בקשה של נושא מידע לממש את זכותו בחוק לעיין, לתקן ולמחוק מידע שעליו הנמצא בחזקת הספק וישמע להנחיות האוניברסיטה בקשר לבקשה כאמור.

11. **<u>העברת המידע לספק</u>**

11.1. העברת נתונים פיסית –עקרונות מנחים:

11.1.1. פרטי אנשי קשר בצד מוסר המידע ומקבלו – יאושרו על-ידי האוניברסיטה.

11.1.2. צורת העברת המידע תאושר על ידי האוניברסיטה טרם ביצוע העברה - מדיה מגנטית/ניירת וכיו״ב.

11.1.3. שינוע המידע ייעשה ישירות לאתר היעד כפי שייקבע בחוזה מול האוניברסיטה בתאום ובאישור מראש על-ידי האוניברסיטה.

11.1.4. על הגורם החיצוני לאבטח את המידע המגיע מהאוניברסיטה.

11.2. תווך תקשורת –עקרונות מנחים:

11.2.1. לא תבוצע כל העברת מידע של האוניברסיטה ו/או כל חומר רגיש אחר באמצעות רשת האינטרנט ללא הצפנה (באמצעים מוגדרים ומוסכמים מראש על-ידי האוניברסיטה).

11.2.2. תצורת העבודה (העברת קבצים, מסמכים וכו') תאושר על-ידי אבטחת המידע והגנת סייבר של האוניברסיטה.

11.2.3. יתקיים זיהוי ואימות חזק של שני הצדדים המתקשרים.

11.3. אם העברת מידע מגורם החיצוני <u>אל תוך</u> האוניברסיטה תעשה באמצעות התקן נייד, נדרש לבצע הלבנה טרם הכנסתו לרשת האוניברסיטה.

11.4. לא יתקיים שיתוף מידע של האוניברסיטה בין פרויקטים שונים של הספק ללא אישור מראש של תחום אבטחת מידע והגנת סייבר באוניברסיטה.

11.5. העברת נתונים בין האוניברסיטה לבין הספק, במידה ותידרש, תתבצע בצורה מוצפנת לפי הסטנדרטים המקובלים ובהתאם להגדרות מאושרות על-ידי האוניברסיטה הכוללים VPN, נל"ן ו/או שימוש במערך הכספות.

12. **<u>שמירה והשמדת המידע</u>**

12.1. הספק מתחייב לסמן כל פלט של מידע המופק ממאגרי המידע של האוניברסיטה באמצעות כותרת עליונה בנוסח הבא : "מכיל מידע מוגן לפי חוק הגנת הפרטיות - המוסר שלא כדין עובר עבירה".

12.2. בסיום ההסכם ולבקשת האוניברסיטה בכל מועד אחר, הספק ישיב את המידע לאוניברסיטה, או יעבירו לספק אחר, בהתאם להנחיות האוניברסיטה וימחק באופן מלא, סופי ובלתי חוזר כל עותק



חתימת גורם מוסמך מטעם הספק_____

של המידע הנמצא ברשותו, יוודא שלא נשאר בידיו עותק כלשהו של המידע, לרבות על גבי מדיה נתיקה, אתרי גיבוי ושחזור מאסון, זכרונות מטמון וכיו"ב - הכל בהתאם ללוח זמנים לביצוע שתקבע האוניברסיטה, ויספק לאוניברסיטה תצהיר ערוך כדין של ממונה האבטחה או האחראי על האבטחה, אם לא מינה ואיננו מחויב על פי דין למנות ממונה אבטחה, מטעמו על השלמת פעולות המחיקה, ביעור והשמדה של המידע.

12.3. על אף האמור לעיל, ככל שיש הוראה בדין המחייבת שמירה של המידע על ידי הספק, או שהספק נדרשת לשמור מידע לצורכי התגוננות מתביעות, ישמור הספק את המידע המינימלי הנדרש, יעביר את המידע לסטאטוס של ארכוב, יאפשר גישה למידע אך ורק למטרה הנ"ל ולמורשי גישה הנדרשים לכך בלבד (כדוגמת מנכ"ל ויועץ משפטי) ויערוך נוהל מתאים לניהול המידע המאורכב ויפעל לפיו. כל עוד נותר המידע שמור בארכיב הספק, תחולנה עליו כל הוראות כתב התחייבות זה וכן הוראות בעניין סודיות המידע בהסכם.

12.4. הוראות כתב התחייבות זה תמשכנה לחול, אף לאחר סיום ההסכם מכל סיבה וכל עוד הספק, או ספקי משנה שלו, מחזיקים במידע.

13. **<u>הדרכה</u>**

13.1. כתנאי לגישת כל מורשה גישה למידע, הספק ידריך את מורשי הגישה ביחס למטרות השימוש במידע – ביחס למורשי גישה קיימים – בסמוך לאחר החתימה על ההסכם ולאחר מכן לכל מורשה גישה נוסף שהספק יאפשר לו גישה למידע.

13.2. הספק יקיים תיעוד בכתב על קיומה של כל הדרכה כאמור, בו יצוין מועד ההדרכה ומשכה, שם המדריך, העובדים הנוכחים בהדרכה ותכני ההדרכה שהועברו להם. התיעוד יאושר בחתימת המדריך ובחתימת מנכ"ל הספק. הספק יעביר לאוניברסיטה, עותק של כל תיעוד מאושר כאמור בסמוך לאחר ביצוע ההדרכה.

14. **<u>אבטחה פיסית</u>**

14.1. הספק מתחייב כי הגישה לאזורים שקיים בהם מידע וארונות התקשורת תהייה מתועדת ומבוקרת באופן המאפשר את וידוא זהות האדם הניגש לציוד הנ"ל הכולל מניעת הכחשה. רשומות הכניסה ישמרו למשך שנתיים (לתקופה שלא תפחת מ-24 חודשים) ויועברו לאוניברסיטה לפי דרישה.

14.2. בכל מקרה בו המידע נמצא ברשות הספק או מי מטעמו, הספק מתחייב לתעד הכנסה והוצאה של ציוד אל המתקנים בהם ממוקם המידע ומהם.

14.3. הספק מתחייב כי כניסת ספקים או לקוחות לאזורי חוות השרתים תהיה מבוקרת, תכלול ליווי ותירשם ביומן רישום אירועים. באופן בו תתאפשר שליטה בנכנסים על ידי מאבטח / מערכת טכנולוגית.

14.4. אמצעים לבקרת כניסה פיסית: הספק מתחייב כי השרתים והציוד המשמש לאחסון, עיבוד וגישה למידע, לשרתי הספק וליישומי הספק יוגנו על ידי אמצעים מתאימים לבקרת כניסה כדי להבטיח שרק לעובדים מורשים תותר הגישה.

15. **<u>מידע מודפס, מצעי מידע פיסיים ומדיה מגנטית</u>**

15.1. על הספק ליידע את עובדיו וכל מי שנחשף למידע במסגרת התהליכים אצל הספק על חובת יישום ההנחיות לשמירה על מידע מודפס, מצעי מידע פיזיים ומדיה מגנטית.

15.2. באזורי קבלת קהל ועל שולחנות לקבלת קהל לא יאוחסן מידע.



חתימת גורם מוסמך מטעם הספק_____

15.3. מצעי מידע פיזיים כגון: אמצעי אחסון אלקטרוני או ניירת האוגרים מידע - אין להשאירם ללא השגחה ולאחר שעות העבודה יש לאחסנם במקום נעול.

15.4. חל איסור להשאיר פלט המכיל מידע במדפסות או במכונות צילום. מדפיס או מצלם המידע לקחת לחזקתו את הפלט או החומר המודפס ולא להשאיר אותם ללא השגחה במדפסת או במכונת הצילום.

15.5. מידע אשר השימוש בו הסתיים, חייב לעבור גריסה או להיות מאוחסן בארכיון מאובטח.

15.6. אם יש צורך בהשמדה או סילוק של מדיה מגנטית כדוגמת דיסקים, קלטות גיבוי, מדיה נתיקה מכל סוג, פלט נייר וכו' שכולל מידע, הספק יבער את המידע שבמדיה בהתאם להנחיות ממונה אבטחת המידע של האוניברסיטה לאחר גיבוי המידע בהתאם לצורך והנחיותיה.

15.7. הספק מתחייב שלא להוציא מידע להתקנים ניידים למעט לצורכי גיבוי.

15.8. אם הספק מעתיק מידע לקלטות גיבוי, יודא הספק שאין עירוב של מידע מסיווגים שונים על אותו התקן.

16. **<u>ניהל הסיכונים</u>**

16.1. הספק מתחייב לבצע ניהול וזיהוי של סיכוני אבטחת מידע בכל שלב משלבי הפרויקט, יש להגיש את ניהול הסיכונים בכתב לאוניברסיטה.

16.2. הספק מתחייב לפנות לאוניברסיטה בבקשה לאישור לפני ביצוע שינויים בארכיטקטורת המערכת, או באופן מתן השירותים. הספק מתחייב שלא לבצע שינוי כלשהו ללא אישור מפורש ובכתב מהאוניברסיטה

17. **<u>הרשאות גישה ומידור</u>**

17.1. למידע המגיע מהאוניברסיטה או מלקוחותיה תתאפשר גישה רק לעובדים הכרחיים ומורשים.

17.2. הספק לא יעניק לעובד מעובדיו, או כל צד שלישי מטעמו, גישה למידע, אלא אם נוכח לדעת שבמילוי משימותיו הקודמות אצל או עבור הספק, העובד הפגין יושרה ושיקול דעת זהיר הנדרשים כדי למלא כיאות תפקיד הכרוך בגישה למידע.

17.3. הספק יבצע בדיקת מהימנות ווידוא ואימות רקע תעסוקתי לכל מועמד להעסקה כעובד או כקבלן אצל הספק, או אצל מי מטעמו, כנדרש ובהתאם למגבלות על פי דין. היקף בדיקות אימות הרקע יתאים לדרישות האוניברסיטה, לסיווג המידע שהעובד או הקבלן יהיו נגישים להם ולסיכונים הצפויים.

17.4. בכל שינוי סטאטוס של עובד ספק בעל הרשאת גישה למידע יעודכנו ההרשאות בהתאם. הספק יעדכן את האוניברסיטה בכל שינוי רלוונטי הנודע להרשאות הגישה ויקבל על-כך אישור בכתב.

17.5. הספק ינקוט בכל האמצעים המפורטים בכתב התחייבות זה כדי למנוע חשיפת מידע לכל עובד ספק אחר שאינו נמנה על מורשי הגישה ולכל צד שלישי אחר, זולת אם נתקבלה לכך הסכמה מפורשת, בכתב ומראש של האוניברסיטה.

17.6. הספק יפחית סיכוני גניבה, הונאה או שימוש לרעה או בלתי מורשה במידע באמצעות נקיטת אמצעי הגנה סבירים ומקובלים, בין היתר ובהתאם לנדרש על ידי האוניברסיטה – לרבות באמצעות שימוש במצלמות, בקרות גישה, שומר בכניסה, אזעקה, כספות, תגי כניסה וליווי מבקרים ועוד.



חתימת גורם מוסמך מטעם הספק_____

17.7. הספק ימנע מקרים בהם עובדיו או מי מטעמו ינסו לגשת למאגרים אליהם לא קיבלו הרשאה. אם עובד או מי מטעם הספק ניסה בפעם השלישית לגשת למאגר שאינו מורשה גישה אליו, על הספק למנוע ממנו כל גישה למאגרי הספק ולדווח על כך מידית לאוניברסיטה.

17.8. הספק יידע את עובדיו ומי מטעמו בדבר קיומו של מנגנון בקרה ותיעוד, הנדרש בהתאם לכתב התחייבות זה ואת היקף התיעוד המבוצע על ידו.

17.9. הספק יתיר למורשי הגישה לגשת למידע רק לאחר שחתמו איתו על כתב התחייבות לשמירה על סודיות, אבטחת מידע, הגנת סייבר ופרטיות המידע, הכולל הוראות מחמירות לפחות כמו ההוראות בכתב התחייבות זה ובכל התחייבות של הספק לסודיות מכוח ההסכם. לפי דרישת האוניברסיטה בכתב מהספק, בהתאם לרמת רגישות המידע שהספק מעבד עבור האוניברסיטה בהתאם להסכם, לפי שיקול דעת האוניברסיטה, יחתמו מורשי הגישה על התחייבות לסודיות ופרטיות במישרין כלפי האוניברסיטה.

18. **<u>זיהוי ואימות</u>**

18.1. לכל עובד מורשה גישה למידע יוקצה אמצעי זיהוי אישי וייחודי שיכלול לפחות שם משתמש ייחודי וסיסמה.

18.2. גישה למאגרי מידע בעלי רגישות גבוהה כפי שתוגדר על ידי האוניברסיטה תבוצע באמצעות מנגנון הזדהות חזקה המשלב שני מנגנוני הזדהות (2FA), על בסיס "משהו שאתה יודע" ו-"משהו שיש לך".

18.3. אמצעי זיהוי שהוקצה לעובד, לא יוקצה לעובד אחר זולתו, אף לא במועד מאוחר יותר. הספק יקיים רישום של כל זהויות המשתמשים ותפעיל אמצעי אימות לפני כל הענקת גישה למידע.

18.4. זהות משתמש שלא היתה פעילה במשך שישה חודשים, תוסר ממערכות המידע, למעט זהות משתמש שנועדה אך ורק למטרות תחזוקה ותמיכה.

18.5. משתמש מורשה שנסתיימה או הופסקה מעורבותו בביצוע הסכם זה – יוסר ממערכות המידע.

18.6. עובדים מורשים יהיו רשאים לגשת למידע רק לאחר שעברו הליך לאימות זהות המשתמש שהוקצתה להם.

19. **<u>סיסמאות</u>**

19.1. הספק יאכוף מדיניות המקטינה את הסיכון לפגיעה בסודיות הסיסמה שבשימוש עובד מורשה. סיסמאות יאוחסנו באופן מוצפן המבטיח כי הן לא יהיו קריאות ומובנות.

19.2. הספק יקבע נוהל פנימי להקצאת, הפצת ואחסון סיסמאות.

19.3. סיסמאות יכילו לפחות שמונה תווים ולא יכללו מחרוזות שניתן בקלות לייחס למשתמש המורשה (כדוגמת שמו, שם בני משפחתו, תאריכי הולדת וכיו"ב).

19.4. הספק ידריך את עובדיו המורשים על האופן בו יש לשמור על סודיות סיסמאותיהם.

19.5. זהות משתמש תיחסם באופן אוטומטי במידה ונכשלו שלושה ניסיונות אימות רצופים.

19.6. הספק ישמור היסטוריית סיסמאות עד 5 סיסמאות אחורה.



חתימת גורם מוסמך מטעם הספק_____

20. **<u>מעקב ותיעוד</u>**

20.1. הספק יישם מערכות שיערכו תיעוד ומעקב אחר כל גישה וניסיון גישה למידע.

20.2. המידע הנאסף ממערכות תיעוד ומעקב אלה יישמר למשך שנתיים (24 חודשים) לאחר קרות האירוע המתועד על-ידן.

20.3. ממונה אבטחת המידע יבחן את דוחות מערכות התיעוד והמעקב מדי חודש לשם איתור תקריות ואנומליות.

20.4. הספק ימסור לאוניברסיטה עם דרישתה כל מידע שנאסף באמצעות מערכות לבקרת גישה כאמור.

20.5. מבלי לפגוע בכלליות האמור לעיל, הספק מתחייב:

20.5.1. לנהל מנגנון תיעוד אוטומטי שיאפשר בקרה וביקורת על מערכות שניגשות למידע;

20.5.2. שבכל פניה למערכות של הספק ולמידע, יירשמו כל הנתונים הבאים: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, והאם הגישה אושרה או נדחתה;

20.5.3. תיעוד הגישה יישמר בשרתים נפרדים מהשרתים המאחסנים את המידע;

20.5.4. מנגנון הבקרה לא יאפשר, ביטול או שינוי של הפעלתו.

20.5.5. מנגנון הבקרה יאתר שינויים או ביטולים בהפעלתו ויפיץ התראות לממונה אבטחת מידע מטעם הספק ולצוות אבטחת מידע אצל הספק.

21. **<u>גישה מרחוק</u>**

21.1. גישה מרחוק לכל מערכת מחשבים בבעלות, בהחזקת או בשליטת הספק, שהינה בעלת קישוריות, ישירה או עקיפה לאמצעי המאחסן מידע ("מערכות מידע") לא תיעשה אלא בטכנולוגיה המשלבת זיהוי ואימות המשתמש בהזדהות חזקה הכוללת שני מנגנוני הזדהות (2FA), סודיות ושלמות הנתונים ומניעת הכחשה (non-repudiation).

21.2. תווך התקשורת המשמש לגישה מרחוק יהיה מוצפן אף הוא.

22. **<u>אבטחה לוגית</u>**

22.1. הספק יישם אמצעי אבטחה הולמים שימנעו חדירה מכוונת או מקרית למערכות הספק או למערכות התשתית והתקשורת.

22.2. הספק יפריד בין רשתות המאכלסות את המידע ליישומים ולכלל הרשתות (סגמנטציה).

22.3. כל אמצעי אבטחת המידע שהספק משתמש בהם יעברו הקשחות לפי המלצות היצרן.

22.4. הספק יעדכן באופן שוטף את המערכות המשמשות לשירותים, למניעת ניצול פרצות אבטחת מידע.

22.5. מידע של האוניברסיטה יישמר בספריות ייעודיות עבור האוניברסיטה בלבד. לספריות אלה, תתאפשר גישה לעובדים מורשים בלבד הרלוונטיים לביצוע הפרויקט. הגישה לספריות תתאפשר רק באמצעות סיסמה אישית.

23. **<u>אבטחת תחנות קצה</u>**

23.1. אין לשמור מידע של האוניברסיטה בתיקיות מקומיות על גבי תחנות עבודה ולמען הסר ספק חל איסור מוחלט לשמור מידע של האוניברסיטה על גבי מחשבים ניידים.

23.2. חל איסור מוחלט לשמור מידע רגיש (כהגדרתו בחוק הגנת הפרטיות) באופן מקומי בתחנת קצה של המשתמש.

23.3. יש להקשיח תחנות קצה לפי נוהגים מיטביים המקובלים בתעשייה.

23.4. יש להתקין אנטי-וירוס בכל תחנות הקצה.

23.5. יש למנוע הכנסת מדיה נתיקה (USB) לתחנות הקצה.

24. **<u>קישוריות לאינטרנט</u>**

24.1. הספק לא יחבר את מערכות המידע המשמעות לאספקת השירותים לאינטרנט, אלא אם כן קיבל את אישור האוניברסיטה לכך.

24.2. יבוצע מידור והפרדה בין המערכות המעבדות מידע הקשור לאוניברסיטה לבין ממשקים חיצוניים, בעיקר בכל הנוגע קישור לאינטרנט.

24.3. קישוריות מערכות המידע עם מידע לאינטרנט תיעשה באמצעות שרת נפרד של הספק, לצרכים עסקיים בלבד (של הספק) ותוך יישום אמצעי אבטחת מידע עדכניים ככל שיידרש אך לפחות אנטי-וירוס עדכני, מערכות לזיהוי קוד-עוין Anti-Malware/EDR), מסנני תוכן (content filtering), מערכת לאיתור ניסיונות חדירה (IDS/IPS) וחומת-אש (Firewall) ברמה תשתיתית ואפליקטיבית (WAF).

24.4. שרתים המחזיקים מידע של האוניברסיטה אצל הספק יופרדו מרשת האינטרנט של הספק באמצעות רכיב סינון תקשורתי כדוגמת חומת-אש (Firewall) .ברכיב הסינון יוגדרו רק הגורמים המורשים מטעם הספק לביצוע פעילות כמורשה גישה לשרתי האוניברסיטה.

24.5. לא תותר גישה מרחוק למידע של האוניברסיטה המאוחסן אצל הספק כמו כן לא תתאפשר גישה מרחוק של הספק לשרתים המאוחסנים באוניברסיטה עצמה.

25. **<u>אמצעי אחסון</u>**

25.1. בשימוש הספק באמצעי אחסון מבוססים ענן תקבע הספק נהלים מתאימים לנושא שימוש והגנה בסביבת רבת דיירים (Multi Tenant) הכוללת הצפנה והרשאות גישה מתאימות.

25.2. בעת אחסון מידע מחוץ לגבולות ישראל על הספק לוודא כי ספק משנה המספק לו שירותי אחסון (ושירותי נלווים אחרים כדוגמת גיבוי ושחזור מאסון) עומד ברמת ההגנה בהתאם לרגולציה של הגנת המידע של האיחוד האירופי ובתקני אבטחת מידע מוכרים כדוגמת SOC2 Type II ו – ISO27001 וכי לפי דרישת האוניברסיטה, ימסור הספק לאוניברסיטה דו"חות אבטחת מידע כדוגמת: SOC2 Report, Statement of Applicability (SOA) ו – PCI Compliance Reports.

25.3. גישתם של עובדים אלו תתועד. הספק יקיים שיטה לתיעוד אמצעי מדיה שמתקבלים אצל הספק מאת גורם אחר כלשהו ושנמסרים מהספק אל גורם אחר כלשהו. התיעוד יכלול את סוג המדיה, תאריך ושעת הקבלה/המשלוח, זהות השולח והמקבל, מספר סידורי של המדיה ותיאור תוכן המדיה. מסירת מדיה מהספק לגורם אחר תיעשה רק לאחר שבוצע תהליך נאות לאימות תוכנה ולווידוא העדרו של כל מידע העשוי להשתייר במדיה. מדיה המתקבלת מגורם אחר תיבדק לגילוי וירוסים. השמדת מדיה או ביעורה ייעשו בדרך המונעת את שחזור המידע שהושמד.

26. **<u>הצפנה</u>**

26.1. הספק יקבע נוהל לביצוע הצפנה למידע אישי בסטנדרטים מקובלים ובהתאם לרגישות הנתונים ויפעל לפי נוהל זה במהלך ביצוע הסכם זה.

26.2. גיבוי, שחזור והתאוששות מאסון

26.3. הספק יבצע גיבויים מאובטחים של המידע שברשותו.

26.4. הספק יקבע נוהל לביצוע גיבוי למידע, שבו ייקבעו, בין היתר, תדירות הגיבוי, אופן ביצועו הכולל הצפנה לפי רמת הרגישות ומקום אחסנת עותק הגיבוי. הספק יפעל לפי נוהל הגיבוי במהלך ביצוע הסכם זה.

26.5. ככל שהספק משתמש במדיות גיבוי, הוא יאחסן אותן בכספת מוגנת אש ומים הנמצאת מחוץ למתקן המחזיק את מאגרי המידע או שהספק יעשה שימוש באמצעים שיבטיחו את שלמות המידע ויבטיחו את אפשרות שחזור המידע במקרה של אבדן או הרס.

27. **<u>שימוש במחשבים ניידים</u>**:

27.1. שמירת מידע של האוניברסיטה על גבי מחשב נייד, כפופה לקבלת אישור האוניברסיטה, ממחלקת אמ"מ.

27.2. במקרה בו אישרה מחלקת אמ"מ לספק שימוש במחשב נייד, באחריות הספק ליישם הצפנת דיסק מלאה במחשב הנייד, התקנת אנטי וירוס ועדכוני גרסאות אנטי וירוס וביצוע סריקות תכופות, התקנת Personal FireWall וכל אמצעי אחר שיידרש על ידי האוניברסיטה להתקינו.

28. **<u>סביבת פיתוח</u>**

28.1. פיתוח כלים חדשים למערכות המידע, לרבות תהליכי בדיקות לכלים חדשים, ייעשו במערכות מידע נפרדות ממערכת המידע המשמשת לתפעול ועבודה שוטפת.

28.2. פיתוח הכלים יתבצע בצורה מאובטחת ובהתאם לסטנדרטים המקובלים, דהיינו בהתאם למתודולוגיית Secured Software Development Life Cycle (SSDLC) ו-Privacy By Design (PbD).

29. **<u>דיווח, מעקב ובקרה</u>**

29.1. הספק יקבע נוהל לתגובה, לדיווח ולניהול תקריות אבטחה הקשורות, או קיים חשד שקשורות במידע.

29.2. הספק יקיים רישום לכל תקרית אבטחה שהגיעה לידיעתו, ובו יתועד מועד התקרית, זהות המדווח, זהות הנמענים של הדיווח ותוצאות התקרית.

29.3. הספק ידווח, מייד לאחר שנודע לו, על כל אירוע שנעשה בו שימוש במידע, בלא הרשאה או בחריגה מהרשאה או שנפגעה שלמות המידע.

29.4. הספק יחל מייד באיתור וטיפול בגורם האירוע, יפעל בתיאום עם האוניברסיטה ביחס לניהול האירוע במישורים הטכנולוגיים, משפטיים, רגולטורים ומנהלתיים וימשיך לדווח לאוניברסיטה על כל דבר ועניין הקשור באירוע ובניהולו.

29.5. בתום האירוע ימסור הספק לאוניברסיטה דו"ח אירוע מפורט וכן ינקוט בכל הפעולות הנדרשות, לרבות יישום כלים ושיטות עבודה, ככל שנדרש כדי להימנע מאירוע דומה בעתיד.

29.6. הספק יקבע נהלים לשחזור מידע שאבד או שנפגם עקב תקרית אבטחה. נהלים אלה יחייבו תיעוד מדוקדק של פעולות השחזור שננקטו ויחייבו קבלת אישור מקדים בכתב מהאוניברסיטה לכל פעולת שחזור מידע.

29.7. הספק ידווח לאוניברסיטה מיד לאחר שנודע לו על כל תלונה שיקבל מכל צד שלישי שהוא לגבי מידע המנוהל או מוחזק על ידו או על ידי מי מטעמו, ועל כל פניה או פעולת פיקוח של רשות להגנת הפרטיות או מי מטעמה, בקשר עם ניהול ועיבוד מידע כהגדרתו בחוק הגנת הפרטיות על ידי הספק או מי מטעמו. ככל שהתלונה או פעולת הפיקוח נוגעת למידע, תשמע הספק להוראות האוניברסיטה (ככל שהדין איננו אוסר זאת) ותפעל בהתאם להנחיות ודרישות האוניברסיטה.

29.8. לפי שיקול דעת האוניברסיטה ודרישתה בכתב מהספק, הספק יספק לאוניברסיטה, או יאפשר לה להטמיע אמצעים ומערכות שנועדו לצורכי ניטור ובקרה ושיאפשרו לאוניברסיטה לפקח על פעילות הספק, עובדיו וכל מי מטעמו במידע.

29.9. הספק ישלח לאוניברסיטה דיווחים שוטפים בנוגע לאופן ניהול מאגר המידע ועיבוד המידע.

29.10. הספק יקבע ויאכוף נוהל לבחינה תקופתית של מערכות המידע, במטרה לאתר חולשות, פריצות אבטחה וכשלי אבטחה.

29.11. הבחינה התקופתית לא תפחת מפעם בחצי שנה וביצועה יתועד בכתב.

29.11.1. במידה והבחינה איתרה חולשות, פריצות אבטחה או כשלי אבטחה אחרים, הספק יערוך בהקדם האפשרי תוכנית פעולה לתיקונם ותפעל בזריזות ליישמה.

30. **<u>ביקורת</u>**

30.1. האוניברסיטה רשאית לערוך בקורת אצל הספק, בעצמה או באמצעות מבקר מטעמה, בכפוף להתחייבות המבקר שאיננו עובד האוניברסיטה לסודיות, לרבות בחצרי הספק ולבקש מהספק כל מידע הרלבנטי לפעולות במידע שמבצע הספק, מי מטעמו וספקי המשנה שלו. הביקורת תבוצע בהתראה בת שלושים (30) יום מראש לפחות, של האוניברסיטה לספק, למעט אם הביקורת נובעת מאירוע אבטחה אצל הספק, או מחשד של האוניברסיטה שהספק מפרת את הוראות החוק או



חתימת גורם מוסמך מטעם הספק_____

כתב התחייבות זה, שאז האוניברסיטה רשאית לבצע בקורת ללא התראה מראש. ככל שניתן, הביקורת תהיה בשעות העבודה הרגילות של הספק, ככל שניתן מבלי לפגוע בפעילות השוטפת של הספק. האוניברסיטה תישא בעלויותיה, לרבות עלות המבקר מטעמה. הספק יישא בעלויותיו.

30.2. האוניברסיטה רשאית לדרוש מהספק את תיקונם של כל הליקויים שיתגלו בפעולות פיקוח ובקורת, או בכל דרך אחרת והספק מתחייב לתקן על חשבונו את כל הליקויים כאמור ולהביא תיקונים אלה לאישורה של האוניברסיטה - בתוך פרק זמן סביר שהאוניברסיטה תקבע לכך. הספק מתחייב לשאת בעלות בדיקה חוזרת המיועדת לוודא כי הליקויים תוקנו כנדרש. הספק מצהיר כי ידוע לו וכי הוא מאשר שאם האוניברסיטה תבחר שלא לממש את זכות הביקורת הנתונה לה לפי הוראות כתב התחייבות זה או לא תמסור לספק את הערותיה או דרישותיה לתיקון ליקויים בעקבות פעולת הביקורת– לא יהיה בכך כדי לפטור את הספק ממילוי התחייבויותיו על-פי כתב התחייבות זה, או כדי למנוע מהאוניברסיטה כל טענה, תביעה ודרישה כלפי הספק בגין אי-מילוי הוראות כתב התחייבות זה.

30.3. הספק מאשר שהוא מודע לחובותיו כלפי רשם מאגרי המידע, לרבות סמכויות הפיקוח שלו בקשר לשירותים.

31. **<u>ספקי משנה והעברת מידע לחו"ל</u>**

31.1. הספק איננו רשאי להתקשר עם צד שלישי לצורך מתן השירותים ("**ספק משנה**") ללא אישור מראש, בכתב ובמפורש של האוניברסיטה.

31.2. הספק יכלול בהסכם עם כל ספק משנה, איתו הוא מתקשר לצורך מתן השירותים, הוראות המגנות על המידע ומסדירות את ניהולו, שאינן נופלות מהדרישות שבכתב התחייבות זה, לרבות נספחיו ובכלל זה את כלל ההוראות המופיעות בסעיף 15 לתקנות אבטחת מידע לחוק הגנת הפרטיות.

31.3. הספק לא יעביר את המידע אל מחוץ לגבולות המדינה, למעט לאתר הנמצא בתחום אחת או יותר ממדינות האיחוד האירופי, ללא אישור בכתב, מראש ובמפורש של האוניברסיטה.

31.4. הספק לא ישמור את המידע באמצעות שירותי אחסון בענן, אלא בכפוף של אישור בכתב ומראש של ממונה האבטחה של האוניברסיטה.

32. **<u>בקרה, בטוחות, סעדים ואחריות</u>**

32.1. כדי לאפשר לאוניברסיטה תגובה מהירה ויעילה להפרות הוראות החוק או כתב התחייבות זה על ידי הספק, ידווח הספק באופן מיידי לאוניברסיטה על כל חריגה מהוראות כתב התחייבות זה או הפרה של הוראות החוק.

32.2. מבלי לגרוע מהתחייבויות הספק על פי ההסכם וכתב התחייבות זה, הספק יחזיק במהלך כל תקופת ההסכם ועוד שנתיים לאחר מכן ביטוח לכיסוי אחריותו המקצועית וסיכוני סייבר. פוליסת הביטוח של הספק תכלול כיסוי מלא כנגד עילות תביעה הנובעות מהפרת חוק הגנת הפרטיות ותקנותיו, פריצות למערכות המידע שלו, הפרת סודיות וכל שימוש לרעה, או ללא רשות במידע. גבול האחריות בפוליסה לא יפחת מסך של $1,000,000 לאירוע ובסך הכל לתקופת ביטוח שנתית.

32.3. הספק ימלא אחר כל תנאי הביטוחים הנזכרים לעיל והוא מתחייב, בין היתר, לשלם את דמי הביטוח במלואם ובמועדם, לדאוג ולוודא כי פוליסות הביטוח תחודשנה מעת לעת ולפי הצורך ולא לעשות כל מעשה שיש בו כדי לצמצם או להפקיע את תוקף הביטוחים.

32.4. ביטוחי הספק יכללו תנאי מפורש על פיו הינם קודמים לכל ביטוח אשר נערך על ידי האוניברסיטה וכי המבטח מוותר על כל דרישה או טענה בדבר שיתוף ביטוחי האוניברסיטה. כמו כן, יתחייב המבטח שהפוליסות לא תצומצמנה ולא תבוטלנה אלא אם תימסר הודעה בכתב בדואר רשום לידי האוניברסיטה לפחות 60 יום מראש.

32.5. הפרת אילו מהתחייבויות הספק המפורטות בכתב התחייבות זה, או את החוק, תהווה הפרה יסודית של ההסכם שתאפשר לאוניברסיטה להשעות את פעולות עיבוד המידע על ידי הספק, בהודעה לספק עם תוקף מיידי, עד שהספק יתקן את ההפרה לשביעות רצון האוניברסיטה וכן שיאפשר לאוניברסיטה לבטל את ההסכם באופן מיידי - והכל ללא כל תשלום או פיצוי לספק ומבלי לפגוע בזכויות ובסעדים המוקנים לאוניברסיטה על פי דין.

32.6. אחריות הספק להפרת הוראות כתב התחייבות זה והחוק כלפי האוניברסיטה, מי מטעמו וכל צד שלישי, איננה מוגבלת.

32.7. הספק ישפה את האוניברסיטה ומי מטעמה, מייד עם דרישתה בכתב, בגין כל נזק, פיצוי, הפסד, קנס, עיצום כספי והוצאה, לרבות שכר טרחת עורכי דין ויועצים מקצועיים, בגין כל דרישה ותביעה של צד שלישי וכל פעולת פיקוח, אכיפה או חקירה של רשות ממשלתית, הנוגעות להפרה של הספק, מי מטעמו וכל ספק משנה של הספק, את אילו מהתחייבויות הספק לפי כתב התחייבות זה, או את החוק.

33. **<u>אנשי קשר</u>**

33.1. אנשי הקשר לצורך כתב התחייבות זה הם כדלקמן:

| | **ממונה אבטחת המידע של הספק** | **ממונה אבטחת המידע והגנת סייבר של האוניברסיטה** |
|---|---|---|
| **שם** | | אורן בן שלום |
| **כתובת דוא"ל** | | ciso@tau.ac.il |
| **מס' טלפון ישיר** | | 03-6408944 |

33.2. כל דיווח של הספק בהתאם לכתב התחייבות זה ייעשה לממונה אבטחת המידע והגנת הסייבר של האוניברסיטה.

33.3. ממונה האבטחה של הספק יהיה זמין לפניות של ממונה האבטחה של האוניברסיטה בכל דבר ועניין הקשור עם כתב התחייבות זה.

34. **עדכון כתב ההתחייבות**

34.1. הספק מכיר בכך שכתב התחייבות זה כפוף לדרישות והוראות החוק. בהתאם, האוניברסיטה רשאית לערוך תיקונים ועדכונים בכתב התחייבות זה, בהתאם לנדרש על פי דין, לפי שיקול דעתה, בהודעה בכתב לספק והספק מתחייב ליישם כל עדכון כאמור בהתאם ללוח הזמנים שהוגדר על ידי האוניברסיטה בהודעתה. אם הספק לא יעמוד בדרישות כל עדכון כאמור, לשביעות רצונה המלא של האוניברסיטה, האוניברסיטה רשאית להשעות באופן מיידי את ניהול המידע על ידי הספק וכל תשלום לספק בקשר עם השירותים, עד שיבצע את העדכון הנדרש, ליתן לספק כל הוראה אחרת בקשר עם המידע, ניהולו, מחיקתו או ניוד שלו לכל צד שלישי וכן רשאית האוניברסיטה לבטל את ההסכם, בהודעה בכתב עם תוקף מיידי. במקרה של ביטול ההסכם כאמור, ישיב הספק כל תשלום יחסי ששולם לו על ידי האוניברסיטה, בגין תקופת ההסכם שלאחר ביטולו והאוניברסיטה תשלם לספק את התשלום היחסי עד למועד הביטול, בכפוף לכל זכות קיזוז המסורה לאוניברסיטה בהתאם להסכם ועל פי דין.

35. **הגדרות**:

בכתב התחייבות זה תהיה למונחים הבאים המשמעות שלצידם:

35.1. "**מידע של האוניברסיטה**": משמעו –

כל מידע, ובכלל זה מסמך ותיעוד (פיזי או אחר), בקשר עם:

א. זהותם ו/או שמם ו/או מידע ו/או נתונים ו/או פרטים, של, או המתייחסים אל, תלמידי האוניברסיטה או מי שיש להם עם האוניברסיטה קשרים אחרים לרבות עצם הקשרים האמורים עם האוניברסיטה ו/או כל אדם שפרטים אודותיו יועברו לספק על ידי האוניברסיטה ו/או כל אדם שהספק תיחשף, בקשר עם מתן השירותים, לפרטים אודותיו, וכן

ב. זהותם ו/או שמם ו/או מידע ו/או נתונים ו/או פרטים, של, או המתייחסים אל, עובדי האוניברסיטה ו/או גמלאי האוניברסיטה בכל עת שהיא ו/או בני משפחותיהם, ו/או מי שיש לו או היו לו קשרי העסקה עם האוניברסיטה, וכן

ג. מידע ו/או נתונים ו/או פרטים המתייחסים לטכנולוגיית המידע, אבטחת מידע, תהליכים, נהלים, ציוד, חומרה, מערכות, תוכנות, תוכניות, נוסחאות ו/או שיטות הקשורים ו/או מתייחסים לתפעול האוניברסיטה ו/או לפעילות האוניברסיטה ו/או למערכות המידע שלה ו/או למערכות התפעוליות שלה ו/או לנוהלי עבודה, הנהוגים ו/או שהיו נהוגים ו/או שיהיו נהוגים באוניברסיטה מעת לעת וכן סודות מסחריים ו/או קנין רוחני של האוניברסיטה.

ד. כל הסכם או התקשרות בין הספק לאוניברסיטה ובכלל זה תוצרי השירותים שניתנו על ידי הספק לאוניברסיטה.

35.2. "**מערכות המידע של הספק**" או "**המערכות התפעוליות של הספק**": משמען –

א. המערכות, ובכלל זה חומרה ותוכנה ותשתיות מחשוב, תקשורת ואבטחת מידע, התומכות בפעילות הספק במתן השירותים לאוניברסיטה, ואשר הספק, להבדיל מהאוניברסיטה, הוא אשר מקצה את הרשאות הגישה אליהן.

ב. מערכות מידע של הספק אשר ניגשות למערכות התפעוליות של האוניברסיטה, או משמשות את הספק לביצוע עבודתו עבור האוניברסיטה, בין שהספק מתחזק אותן ובין שהאוניברסיטה מתחזקת אותן.

ג. מידע של האוניברסיטה, ככל שהוא מוחזק ו/או מאוחסן ו/או שמור ו/או מעובד במערכות ותשתיות המחשוב, התקשורת ואבטחת המידע של הספק, להבדיל ממערכות האוניברסיטה.

ד. כל מידע ומאגר מידע שהספק הוא בעליו או שהוא מחזיק בו.

35.3. "**מתקן הספק**": כל מתקן של הספק אשר מתואר בסעיף 2 לעיל כמתקן של הספק לאחסון ו/או עיבוד ו/או גיבוי מידע של האוניברסיטה.

35.4. "**תקשורת מחשבים מאובטחת**": מערכת תקשורת מחשבים מאובטחת כפי שהאוניברסיטה תודיע עליה לספק מעת לעת.

35.5. "**עובד**" או "**עובד הספק**": משמעו עובד של הספק, וכן כל מי שפועל עבור הספק או מטעמו גם אם אינו מועסק במישרין על ידי הספק.

35.6. "**מחלקת אבטחת מערכות מידע**" או "**אמ"מ**" משמעם: מחלקת האוניברסיטה לאבטחת מערכות מידע והגנת הסייבר.

35.7. "**אישור האוניברסיטה**": אישור מפורש של האוניברסיטה, מראש ובכתב, אשר יהיה ערוך על ידי האוניברסיטה על גבי מסמך ייעודי המסדיר אישור זה בלבד, ויהיה מופנה אל הספק.

35.8. **הממונה על אבטחת המידע אצל הספק**: אדם הנמנה על עובדי הספק אשר מונה על ידי הספק לתפקיד זה ואשר אחראי על אבטחת המידע הנכלל במאגרי המידע המצויים בידי הספק ועל יישום ההנחיות המופיעות במסמך זה.

35.9. **הממונה על אבטחת המידע באוניברסיטה**: אדם שמונה לתפקיד זה מטעם בעל המאגר ( מנהל פעיל ) ואשר אחראי על אבטחת המידע באוניברסיטה, ואחראי על מתן הנחיות אבטחת מידע.

35.10. **מאגר מידע**: אוסף נתוני מידע המוחזק באמצעי מגנטי או אופטי (ובכלל זה מחשב) ומיועד לעיבוד ממוחשב.

35.11. **מנהל המאגר**: מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לעניין זה;

35.12.

האוניברסיטה תהיה רשאית להימנע מלתת אישור לספק, על פי שיקול דעתה, מבלי שתהיה עליה לנמק זאת