1. כללי

1.1. באוניברסיטת בר אילן (להלן: "**האוניברסיטה**") מתבצעים מחקרים על ידי חוקרים (כהגדרתם בהמשך).

1.2. בכל ניסוי שבו מעורבים בני אדם יש להגיש בקשה מוקדמת לאישור ועדת הסקירה המוסדית (ועדת האתיקה) או לתת ועדה מטעמה (מחלקתית / פקולטית). **נוהל זה חל רק על מחקרים בהם נאסף מידע אישי על בני אדם.**

1.3. האוניברסיטה כפופה להוראות חוק הגנת הפרטיות, התשמ"א-1981 (להלן: "**חוק הגנת הפרטיות**"), לתקנות שתוקנו מכוחו ולהנחיות רשם מאגרי המידע.

1.4. כמו כן, במחקרים מסוימים בהם מעורב מידע אישי אודות נושאי מידע מהאיחוד האירופי, האוניברסיטה מחויבת לפעול בהתאם להוראות דין זר, בהן בין היתר, תקנות האיחוד האירופי לאיסוף ועיבוד מידע אישי (GDPR).

1.5. נייר עקרונות של ור"ה אשר מהווה קו מנחה לפעולת האוניברסיטה והחוקרים, יעמוד בפני ועדת הסקירה המוסדית של האוניברסיטה כמסמך הנחיות לעבודתה.

2. מטרה

2.1. קביעת הוראות ונהלי עבודה לחוקר (כהגדרתו בהמשך) בטרם תחילת המחקר, בעת המחקר ובסיומו, שיבטיחו קיום הוראות הדין החלות על האוניברסיטה, הבטחת זכויות נושאי המידע ושמירה על אבטחת המידע.

3. הגדרות

3.1. **"מנהל אבטחת מידע"** – עובד שימונה על ידי סמנכ"ל התקשוב ואשר תפקידו יהא לטפל בכל הקשור לגיבוש, עיבוד ופרסום נהלים פנימיים הקשורים לאבטחת מידע באוניברסיטה, ביצועם ואכיפתם.

3.2. **"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

3.3. **"חוקר"** – עובד המועסק מטעם האוניברסיטה בתפקיד חוקר ו/או מדען; סטודנט באוניברסיטה שנדרש לבצע מחקר בהתאם לתוכנית הלימודים שלו; וכן כל מי שמשתמש במשאבי האוניברסיטה לצורך מחקר או עושה מחקר במסגרת האוניברסיטה.

3.4. **"מחקר" -** חקירה שיטתית, כולל פיתוח, בדיקה והערכה שנועדו לפתח או לתרום לידע מדעי בר הכללה (generalizable knowledge).

3.5. **"ועדת סקירה המוסדית"–** ועדה מוסדית אשר מופקדת בין היתר על בחינת האתיקה במחקרים בהם מעורבים משתתפי אנוש או חומר או מידע ממקור אנושי, המורכבת מיו"ר הוועדה, נציגי הפקולטות ונציג ציבור. הוועדה פועלת באמצעות תתי הוועדות המחלקתיות או הפקולטטיביות מטעמה. ועדת הסקירה המוסדית ותתי הוועדות נדרשת לאשר את המחקר ולוודא עמידתו בהוראות נוהל זה והוראות הדין הרלוונטיות. שיקול הדעת האתי והמחקרי בנוגע לביצוע, התאמות ושיתוף מידע במחקר נתון לסמכות ועדת הסקירה המוסדית, כל עוד אינו סותר דין חל.

3.6. **"GDPR"** – תקנות האיחוד האירופי לעיבוד מידע אישי. General Data Protection Regulation (EU) 2016/679 of the European Parliament and the -Regulation Council of 27 April 2016.

3.7. **" מידע אישי" –** נתון הנוגע לאדם מזוהה או לאדם הניתן לזיהוי; לעניין הגדרה זו, "אדם הניתן לזיהוי" – מי שניתן לזהותו במאמץ סביר, במישרין או בעקיפין, ובכלל זה באמצעות פרט מזהה, כגון שם, מספר זהות, מזהה ביומטרי, נתוני מיקום, מזהה מקוון, או נתון אחד או יותר הנוגע למצבו הפיזי, הבריאותי, הכלכלי, החברתי או התרבותי.

3.8. **"מידע בעל רגישות מיוחדת" -** מידע אישי על צנעת חיי המשפחה של אדם, על צנעת אישיותו ועל נטייתו המינית, מידע בריאותי או רפואי, מידע גנטי, מזהה ביומטרי, מוצאו של אדם, עבר פלילי, דעות פוליטיות, אמונות דתיות, השקפת עולם, נתוני מיקום, נתוני תעבורה, שכר, פעילות פיננסית, מידע אישי שחלה עליו חובת סודיות שנקבעה בדין.

3.9. **"אנונימיזציה" או "התממה** "- המרה של נתונים מזהים לנתונים לא מזוהים, ע"י שימוש בטכניקות מתאימות אשר גורמות להפחתת היכולת לזהות את נושאי המידע שהמידע הוא אודותיהם. "מידע מקודד" אינו עונה להגדרת מידע שעבר התממה.

3.10. **"פסאודומיניזציה"** / **"מידע מקודד"** – טכניקה של החלפת מידע מזהה בערך בלתי קשור אך עדיין ייחודי, למשל החלפת שם פרטי ושם משפחה של משתתף במספר (שלום שמואלי = 123456), באופן שבו המידע אינו מזהה את המשתתף ללא שימוש במידע נוסף אשר נשמר בנפרד.

3.11. **" עיבוד / שימוש" –** כל פעולה שמבוצעת על מידע אישי, לרבות קבלתו, איסופו, אחסונו, העתקתו, עיון בו, גילויו, חשיפתו, העברתו, מסירתו או מתן גישה אליו.

3.12. **"מאגר מידע" -** אוסף פרטי מידע אישי המעובד באמצעי דיגיטלי, כהגדרתו בחוק הגנת הפרטיות, התשמ"א-1981.

3.13. **"מנהל מאגר מידע" -** מנכ"ל האוניברסיטה או מי שהמנכ"ל הסמיכו לנהל את המאגר.

3.14. **"משתתף" –** משתתף שעתיד להשתתף במחקר או נציגו החוקי של משתתף חסר כשרות

3.15. **"אבטחת מידע "-** הגנה על שלמות המידע האישי או הגנה על המידע האישי מפני עיבוד, ללא רשות כדין.

3.16. **"אירוע אבטחת מידע" –** אירוע אשר פוגע, או עלול לפגוע בסודיות, שלמות וזמינות המידע ברשת המחשוב של האוניברסיטה, ו/או לפגוע, לשבש או לקטוע תהליכי עבודה תקינים באוניברסיטה, כגון:

3.16.1. חשיפה בלתי מורשית של מידע אישי ו/או מידע בעל רגישות מיוחדת ממערכות המידע של האוניברסיטה.

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

3.16.3. פריצה למערכות המידע באוניברסיטה (ע"י תוקף חיצוני או פנימי).

3.16.4. פגיעת וירוס בתשתיות המחשוב של האוניברסיטה.

3.16.5. שינוי פני אתרים ואפליקציות (Defacement).

3.16.6. מעילה, שימוש לא מורשה בהרשאות במערכת מידע.

3.16.7. השחתה או גניבת ציוד מחשבים במשרדי האוניברסיטה.

3.16.8. שימוש במערכות מידע לפעילות לא חוקית (גניבת תוצרת גמורה, מלאי בתהליך, וכו').

3.17. **"אירוע אבטחת מידע חמור"** – עפ"י הגדרתו בתקנות הגנת הפרטיות.

3.18. **"ועדת הלסינקי"** –ועדה לאישור ניסויים רפואיים בבני אדם לפי הצהרת הלסינקי כמפורט בתקנות בריאות העם (ניסויים רפואיים בבני אדם), תשמ"א-1980.

4. <u>תהליכי העבודה</u>

4.1. <u>אישור המחקר:</u>

4.1.1. בטרם תחילת המחקר, או בכל מקרה של שינוי מטרות המחקר או פרטים שהוגדרו בפרוטוקול מחקר שאושר או במיקום בו יאוחסן המידע על החוקר להגיש בקשה לאישור/שינוי המחקר באמצעות פרוטוקול מחקר כדלקמן:

- לתת-ועדה מחלקתית או לתת-ועדה פקולטית של ועדת הסקירה המוסדית.
- במחקר שמעורב בו בית חולים/ מבטח רפואי כגון קופות החולים– גם לוועדת הלסינקי.

4.1.2. הוועדה הרלוונטית תבחן את פרוטוקול המחקר ותחליט האם להמליץ לוועדת הסקירה המוסדית לאשר את המחקר. כמו כן, הוועדה הרלוונטית תבחן את סוג והיקף ההסכמה הנדרשת לביצוע המחקר בהתאם להוראות הדין הרלוונטי ועקרונות האתיקה המקצועית. במסגרת הבקשה יפרט החוקר את טופס הסכמת הנחקר או אפוטרופוס/מורשה חתימה במקרה של משתתפי מחקר במעמד 'חסוי' (ילדים, אנשים עם דמנציה וכדומה) להשתתף במחקר, סוגי המידע הנאסף, מטרות המחקר, יכולות להתממה של המידע ובמידת הרלוונטיות, אזרחות זרה של המשתתפים במחקר, מחקרים בהם בגלל טיב המחקר אין אפשרות להסביר לנחקר מראש את מטרתו (אלא רק בדיעבד), גורמים נוספים שיסייעו במחקר (פנימיים וחיצוניים).

4.1.3. סוגיות אתיות ונושאים נוספים כמו משך שמירת המידע האישי הנאסף במסגרת המחקר לאחר סיום המחקר, הגדרת פרק הזמן הדרוש לקיום המחקר, ייבחנו בוועדה/ בוועדות הרלוונטית המאשרת את המחקר.

4.1.4. החוקר אינו רשאי להתחיל את איסוף המידע גיוס הנחקרים והחתמתם על טפסי הסכמה מדעת, טרם אישור המחקר על ידי הוועדה הרלוונטית.

4.1.5. אישור המחקר תקף לפרק הזמן המצוין בו ולאחר פרק הזמן הנקוב נדרש אשרור מחדש ו/או הארכה של המחקר על ידי הוועדה הרלוונטית.

4.2. <u>פרוטוקול המחקר:</u>

4.2.1. בטרם איסוף המידע על הנחקרים, החוקר ימלא פרוטוקול מחקר שבו יפרט את הפרטים הבאים:

- הגדרת מטרת המחקר.
- הגדרת המידע האישי שנדרש, בהתאם למטרת המחקר.
- הגדרת הזמן הנדרש לשמירת המידע, בהתאם למטרת המחקר.
- קביעת אמצעי מדידה טכנולוגיים וארגוניים שיבטיחו את אבטחת המידע. ניתן להיוועץ במנהל אבטחת מידע של האוניברסיטה.
- יידוע נושאי המידע המשתתפים במחקר על זכויותיהם.
- הגדרת בסיס חוקי לעיבוד הנתונים האישיים (לפי ה-GDPR). ראה סעיף 5.5 לנוהל.
- הגשת בקשה לאישור מחקר לוועדות הרלוונטיות ואישור הוועדות.

קבלת הסכמתו החופשית והמפורשת (הסכמה מדעת) של הנחקר או של אפוטרופוס/מורשה חתימה במקרה של משתתפי מחקר במעמד 'חסוי' (ילדים, אנשים עם דמנציה וכדומה) להשתתפות במחקר ולאיסוף ועיבוד מידע אישי אודותיו (נספח א'). היה וההסכמה תתקבל בכתב, כתב ההסכמה יישמר בעותק קשיח בתיקייה ייעודית וכן סריקתו תשמר בתיקייה ייעודית ברשת האוניברסיטה שהגישה אליה ממודרת, או באופן מאובטח על מחשבו של החוקר.

4.3. **<u>הסכמה מדעת:</u>**

4.3.1. בכפוף להחלטת וועדת הסקירה המוסדית לפני גיוס משתתף למחקר עליו חל נוהל זה, על החוקר לקבל הסכמה מדעת מהמשתתף, בהתאם לעקרונות המפורטים בנספח א'.

4.4. **<u>סודיות ואחריות אישית:</u>**

4.4.1. <u>החוקרים מחויבים לשמירה על סודיות המידע והנתונים אליהם הם נחשפים במהלך עבודתם.</u>

4.4.2. חוקר שנעזר בגורמים חיצוניים לביצוע המחקר (עוזרי מחקר, סטודנטים וכיו"ב) מחויב להחתים כל גורם כאמור על הסכם אבטחת מידע וסודיות בהתאם לנוהל דרישות אבטחת מידע מספקי מיקור חוץ. על החוקר לשמור אצלו את המסמכים החתומים ולהעביר עותק מהם לוועדה הרלוונטית, ואם הגורם הנוסף מקבל תשלום עבור עבודתו – גם למדור כ"א מחקר.

4.5. **<u>תחולת הוראות ה-GDPR:</u>**

4.5.1. הוראות ה - GDPR חלות רק כאשר מתבצע איסוף, עיבוד, ניהול או איסוף מידע אישי על אנשים באיחוד האירופי.

4.5.2. אם המחקר אינו מכיל מידע אישי, הוראות ה-GDPR לא יחולו על המחקר.

4.5.3. ה-GDPR אינו חל כאשר מדובר במידע אנונימי, שאינו מקושר למשתתף ספציפי. יחד עם זאת, הוראות ה-GDPR כן יחולו כאשר המידע עובר פסאודומיניזציה.

בכל מקרה של ספק, הוועדה הרלוונטית תתייעץ עם הממונה על הגנת הפרטיות של האוניברסיטה.

4.6. **<u>בסיס חוקי לפי ה-GDPR</u>**

4.6.1. <u>עיבוד נתונים אישיים במחקר יהיה כדין רק אם וככל שחלים **לפחות אחד** מהסעיפים הבאים:</u>

4.6.1.1. הנבדק נתן הסכמתו המפורשת לעיבוד נתוניו האישיים למטרה ספציפית אחת או יותר.

4.6.1.2. הגנת האינטרסים החיוניים של הנבדק.

4.6.1.3. ביצוע משימה שהינה לטובת הציבור או בהפעלת סמכות רשמית.

4.6.1.4. אינטרסים לגיטימיים – כל מטרה לגיטימית אחרת שלשמה נאסף המידע בהתאם לעקרונות החוק.

4.6.2. <u>במקרה והמחקר כרוך בעיבוד **מידע בעל רגישות מיוחדת** ניתן לעבד אותו רק אם **לפחות אחד** מהסעיפים הבאים חל:</u>

4.6.2.1. הנבדק נתן הסכמה מפורשת לעיבוד הנתונים האישיים למטרות מוגדרות, אחת או יותר.

4.6.2.2. העיבוד מתייחס לנתונים אישיים של המשתתף שהפכו להיות פומביים על ידי המשתתף.

4.6.2.3. הקמה, מימוש או הגנה של תביעות משפטיות או כאשר בתי משפט פועלים במסגרת תחום השיפוט שלהם.

4.6.2.4. סיבות בעלות אינטרס ציבורי משמעותי.

4.6.2.5. עניין הציבור בתחום בריאות הציבור, כמו הגנה מפני איומים חוצי גבולות על הציבור או הבטחת סטנדרטים גבוהים של איכות ובטיחות של שירותי הציבור או מוצרים רפואיים או מכשור רפואי.

4.6.2.6. למטרות ארכיב לטובת הציבור, מטרות מחקר מדעי או היסטורי, מטרות סטטיסטיות.

4.7. **<u>הערכת השפעת הגנת המידע (DPIA-Data Protection Impact Assessment)</u>**

4.7.1. החוקר נדרש לבצע הערכה של ההשפעה על הגנת המידע כאשר פעולות העיבוד עלולות לגרום לסיכון גבוה לזכויות ולפרטיות של נושאי המידע, בהתחשב באופי המידע, היקפו, הקשרו ומטרות העיבוד. סעיף זה לא יחול במקרים בהם א. המידע אנונימי לחלוטין ב. המידע אינו מכיל מידע רגיש ג. המידע אינו משלב מקורות שמאפשרים זיהוי.

4.7.2. המטרה היא להעריך את אופי וחומרת הסיכון לזכויות ולפרטיות של נושאי המידע.

4.7.3. תוצאות ההערכה תילקחנה בחשבון בעת קביעת האמצעים ההולמים הנחוצים לשמירת המידע.

4.7.4. החוקר יתייעץ עם הממונה על הגנת הפרטיות והממונה על אבטחת מידע בעת ביצוע הערכת השפעת הגנת המידע <u>(DPIA)</u>.

4.8. **<u>ניהול מאגר מידע (כאשר מדובר במחקר שכולל, בחלקו או מקצתו, מידע אישי על ישראלים בלבד)</u>**

4.8.1. בתחילת כל מחקר יתייעץ החוקר עם מנהל אבטחת מידע וממונה הגנת הפרטיות של האוניברסיטה האם המחקר מוגדר כמאגר מידע וזאת בהתאם להוראות חוק הגנת הפרטיות.

4.8.2. היה והוחלט כי מדובר במאגר מידע, נדרש יהיה לנהל את המאגר באופן פנימי באמצעות מסמך הגדרות למאגר. , האוניברסיטה תוגדר כבעלת המאגר והחוקר יוגדר כאחראי המאגר.

4.8.3. הממונה על הגנת הפרטיות יסייע לאחראי המאגר לנהל את המאגר פנימית וזאת בהתאם לנוהל הגנת הפרטיות ונוהל ניהול מאגרי מידע שמספרו 18-006.

4.9. **<u>אחריות אחראי המאגר</u>**

4.9.1. אחראי המאגר יוודא אחת לשנה, כי המידע שנשמר במאגר אותו הוא מנהל, אינו רב מן הנדרש למטרות המאגר;

4.9.2. אחראי המאגר ישתמש במאגר המידע בהתאם למטרות שהוגדרו בלבד;

4.9.3. אחראי המאגר, בשיתוף מנהל אבטחת מידע, יקפידו על האבטחה הפיזית והסביבתית של מערכות המאגר

4.9.4. אחראי המאגר יגדיר וינהל את ההרשאות למאגר ולמידע בו, כולו או מקצתו, ובכלל זה מתן הרשאות והעברת מידע, הסרת הרשאות, מחיקת המידע מרשות מקבל המידע בסיום הצורך

4.9.5. אחראי המאגר, בשיתוף מנהל אבטחת מידע, יוודאו כי קיים גיבוי למאגר המידע וכי מבוצעת בדיקת שחזור לפחות אחת לשנה;

4.9.6. אחראי המאגר ינהל רשימה של מורשי הגישה למאגר ושל הגורמים שקיבלו מידע מהמאגר

4.9.7. חל איסור מוחלט על אחראי המאגר למכור ו/או להשכיר ובכלל למסור לאחר את המידע ללא הסכמה מפורשת של רשות המחקר, ממונה על הגנת הפרטיות ונושאי המידע.

4.10. **<u>זכות העיון וזכות תיקון המידע ומחיקתו</u>**

4.10.1. למשתתף קיימת **הזכות לעיון** מכוח סעיף 13 לחוק הגנת הפרטיות. סעיף זה מקנה למשתתף את הזכות לעיין במידע המוחזק אודותיו במאגרי המידע של האוניברסיטה, בעצמו או באמצעות בא כוחו שהורשה בכתב או על ידי אפוטרופוס.

4.10.2. לצורך כך, על החוקר ליידע את המשתתף בטופס ההסכמה על זכות זו ועל פרטי ההתקשרות עם החוקר לצורך הגשת בקשה לעיון כאמור. על החוקר לבחון את הבקשה ולהחליט האם לאפשר את זכות העיון בתוך 30 יום מיום הגשת הבקשה.

4.10.3. החוקר רשאי שלא להתיר למשתתף את זכות העיון לגבי מידע המתייחס למצבו הרפואי או הנפשי אם לדעתו עלול המידע לגרום נזק חמור לבריאותו הגופנית או הנפשית של המבקש או לסכן את חייו; במקרה זה ימסור מנהל המאגר את המידע לרופא או לפסיכולוג מטעמו של המבקש. כמו כן, החוקר אינו רשאי למסור למבקש מידע שחל עליו חיסיון שנקבע לפי כל דין, אלא אם כן המבקש הוא מי שהחיסיון נועד לטובתו.

4.10.4. למשתתף קיימת הזכות לבקש **לתקן ו/או למחוק את המידע אודותיו** מכוח סעיף 14 לחוק הגנת הפרטיות. משתתף שעיין במידע אודותיו ומצא כי אינו נכון, שלם, ברור או מעודכן, רשאי לפנות לחוקר, בבקשה לתקן את המידע או למחוק אותו.

4.10.5. לצורך כך, על החוקר ליידע את המשתתף בטופס ההסכמה על זכות זו ועל פרטי ההתקשרות עם החוקר לצורך הגשת בקשה לתיקון /מחיקה כאמור.

4.10.6. בקשה לתיקון / מחיקת מידע כאמור ניתן להגיש עד לשלב תום איסוף הנתונים למחקר, שהרי לאחר מכן ייתכן ולא יהיה ניתן למלא את הבקשה.

4.10.7. החוקר יבחן את הבקשה ויחליט האם להיענות לבקשה או אם לאו:

4.10.7.1. אם הסכים החוקר לבקשה, יבצע את השינויים הנדרשים במידע שברשותו ויודיע עליהם לכל מי שקיבל ממנו את המידע בתוך 30 יום מיום הגשת הבקשה.

4.10.7.2. סירב החוקר למלא הבקשה, יודיע על כך למבקש בכתב ובתוך 30 יום מיום הגשת הבקשה.

4.10.8. על החוקר להיוועץ בממונה הגנת הפרטיות בכל בקשה כאמור (לעיון או לתיקון/מחיקה).

4.10.9. על החוקר לשמור את הבקשה והתגובה אליה וכן להעביר עותק למנהל אבטחת מידע ולממונה הגנת הפרטיות.

4.10.10. יודגש כי הזכות של משתתף לעיון ותיקון מידע כאמור חלה רק על המידע אותו מסר המשתתף לחוקר, ואינה כוללת את המסקנות, התוצאות והתרשמות החוקר מהמידע.

4.11. **<u>שמירת המידע, הצפנה ואבטחת מידע:</u>**

4.11.1. החוקר ישמור את המידע האישי באופן מאובטח וינהג על פי מדיניות אבטחת המידע של האוניברסיטה, הנהלים ויתייעץ עם מנהל אבטחת המידע בכל נושא אבטחת מידע.

4.11.2. המידע האישי יישמר במחשבים של האוניברסיטה בלבד. חל איסור על שמירת המידע במחשבים פרטיים שאינם רכוש האוניברסיטה.

4.11.3. ככל שהחוקר שומר את המידע על מחשב פרטי, החוקר יוודא כי המחשב מוגן בצורה מאובטחת וברמה המקובלת, בהתאם לנהלי האוניברסיטה. שמירת מידע על מחשבים פרטיים הינה באחריות החוקר בלבד.

4.11.4. היה וקיים צורך לשמור מידע על התקן נייד או מחשב שאינו של האוניברסיטה, על החוקר להעביר מידע זה למחשב של האוניברסיטה מיד כאשר הדבר מתאפשר ולוודא כי על המחשב מותקנת תכנת הגנה ותכנת הצפנה מאושרות.

4.11.5. הגישה למידע תהא לגורמים המורשים לעסוק במחקר בלבד, כפי שהוגדרו בבקשה למחקר.

4.11.6. מחשבים, מחשבים ניידים, כונני פלאש, טאבלטים, טלפונים ניידים וכל חומרה אחרת המיועדת לאחסון נתונים תוצפן באמצעות תוכנת הצפנה מאושרת שתותקן על המכשיר. השיטה מגנה על כל הקבצים במכשיר ודורשת סיסמא בעת הפעלתו. באחריות החוקר לוודא כי מכשיריו מוצפנים ואם אינו בטוח, יתייעץ עם מנהל אבטחת המידע.

4.11.7. הצפנת קבצים – בעת העברת קבצים המכילים מידע אישי בדוא"ל, החוקר יצפין הקבצים באמצעות סיסמא וישלח א הסיסמא לנמען במדיה אחרת.

4.11.8. אחסון בענן – במידה והחוקר שומר את המידע האישי בשירותי ענן (למשל: Dropbox, OneDrive, Google Drive) החוקר יוודא עם מנהל אבטחת המידע כי אחסון הנתונים מתבצע בצורה מאובטחת וברמה המקובלת.

4.11.9. מחשב נייד בו נשמר המידע יוצפן באמצעות תוכנת הצפנה מאושרת על ידי מנהל אבטחת מידע. לחלופין, המידע יישמר בקובץ המוגן בסיסמה.

4.11.10. בכל מחשב תותקן מערכת הגנה (אנטי וירוס). חל איסור להסיר את התוכנה. במידה והתוכנה מצאה קבצים נגועים, או שהתקבלה הודעה על אי-פעילות של התוכנה מסיבה כלשהי, על משתמש לפנות ליועץ המחשוב.

4.11.11. המשתמש יפעיל את עדכוני האבטחה בהתאם להוראות היצרן ולמנהל אבטחת מידע.

4.11.12. חל איסור על התקנת תוכנות לתחנת העבודה אלא באישור יועץ המחשוב.

4.12. **<u>שיתוף והעברת מידע</u>**

4.12.1. המידע חייב להיות מוגן בעת העברתו לגורם אחר (בפנים ומחוץ לאוניברסיטה), לכן על החוקר לוודא שמתבצעות לפחות אחת מהאפשרויות הבאות:

4.12.1.1. פרוטוקול העברת קבצים מאובטחים (SFTP) כולל SSH.
4.12.1.2. העלאת קובץ מוצפן ל OneDrive, Dropbox או Google Drive.
4.12.1.3. שליחת קובץ מוצפן בדוא"ל ושיתוף הסיסמא באופן נפרד ומאובטח.
4.12.1.4. סקירת תוכנות עם תוכנות הצפנה התומכות בהצפנה בזמן איסוף המידע והעברתו לשרת המרכזי.

4.13. **<u>אנונימיזציה ומחיקת המידע</u>**
4.13.1. החוקר נדרש להגדיר בטופס הבקשה את משך הזמן הנדרש לשמירת כל מידע אישי ו/או מידע בעל רגישות מיוחדת לפי מטרת העיבוד.
4.13.2. בסיום משך הזמן שהוגדר ו/או כאשר אין צורך לשמור את המידע האישי ו/או כאשר שמירת המידע אינה תואמת למטרת המחקר, החוקר מחויב למחוק את המידע האישי.
4.13.3. המחיקה חייבת להיות מלאה, לכן החוקר יוודא כי המידע האישי נמחק ממסדי הנתונים, גיבויים, התקנים ניידים ועוד. לחילופין, החוקר יכול לבצע אנונימיזציה של המידע האישי ולשמור אותו בצורה שאינה מאפשרת עוד לקשר ולזהות את המשתתפים במחקר.

4.14. **<u>מחשבים ניידים</u>**
4.14.1. על המשתמש לוודא כי אמצעי המחשוב הנייד נמצא בהשגחתו בכל עת.
4.14.2. אין להשאיר אמצעי מחשוב נייד ברכב או בכל מקום אחר ללא השגחה.
4.14.3. המשתמש ינעל את המחשב הנייד במקום בטוח בביתו.
4.14.4. המשתמש יוודא את נעילת אמצעי המחשוב הנייד עם סיסמה אישית, באמצעות שומר מסך מיד כשהוא מפסיק או מסיים את עבודתו על המחשב.
4.14.5. במידה ואמצעי המחשוב הנייד אבד או נגנב, ידווח המשתמש מידית ליועץ המחשוב.

4.15. **<u>אירועי אבטחת מידע</u>**
4.15.1. על החוקר לדווח למנהל אבטחת מידע ו/או ליועץ המחשוב על כל הפרה של כללי אבטחת המידע וסייבר המובאים בנוהל זה ובמסמך האחריות האישית.
4.15.2. במקרה של חשש לאירוע שעשוי להוות אירוע של אבטחת מידע וסייבר, כגון: חדירה לרשת, נעילת קבצים, דלף מידע בדוא"ל, חשיפת סיסמאות גישה, גישת גורמים לא מורשים לקבצים או למשרדי האוניברסיטה ועוד, מחובת החוקר לדווח מידית למנהל אבטחת מידע ו\או לממונה על הגנת הפרטיות.
4.15.3. בקרות אירוע אבטחה חמור, מנהל אבטחת המידע יפעל בהתאם לנוהל ניהול אירועי אבטחת מידע של האוניברסיטה.

4.16. **<u>סיום המחקר</u>**
4.16.1. בעת סיום המחקר ו/או כאשר לא קיים עוד צורך במידע ו/או בהיעדר הסכמה מהמשתתף, על החוקר לבצע את הפעולות שלהלן:
4.16.1.1. למחוק את המידע וכל עותק נוסף מרשותו ולבקש מכל גורם שקיבל את המידע למחוק מרשותו את המידע כאמור לאלתר. לחלופין, ניתן לבצע

אנונימיזציה למידע באופן שלא ניתן עוד לזהות את המשתתף וזאת בהתאם להנחיות מנהל אבטחת מידע ובאישורו.

4.16.1.2. לדווח לממונה על הגנת הפרטיות ו/או למנהל אבטחת מידע לצורך מחיקת הרישום של מאגר המידע ממסמך הגדרות המאגרים הפנימי של האוניברסיטה.

4.16.2. ככל שיעלה הצורך לעשות שימוש במידע ו/או במאגר המידע למחקר נוסף ו/או לשימוש אחר ו/או ככל שהתקבלה הסכמת המשתתף, על החוקר לקבל את אישור ועדת הסקירה המוסדית באמצעות תת הוועדה הרלוונטית מראש ובכתב, תוך הצגת הנימוקים להמשך השימוש במידע לצורך נוסף או אחר.

4.17. **<u>איסוף מידע על נושאי מידע מחוץ לישראל</u>**

4.17.1. בעת איסוף מידע על נושאי מידע מחוץ לישראל ולא באיחוד האירופי, לרבות באמצעות שירותי ענן, על החוקר לפנות לממונה הגנת הפרטיות לצורך קבלת הנחיות נוספות.

5. <u>אחריות</u>

5.1. מנהל אבטחת מידע

5.2. ממונה על הגנת הפרטיות

5.3. רשות המחקר

5.4. חוקרים ראשיים

5.5. חברי וועדת הסקירה המוסדית ותתי וועדות של הוועדה המוסדית

6. <u>תוקף</u>

תוקף הוראה זו מיום פרסומה

זהר ינון

מנכ"ל ומשנה בכיר לנשיא

<u>נספח א' – דוגמה לטופס הסכמה להשתתפות במחקר</u>

***נוסח הטופס עשוי להתעדכן מעת לעת בהתאם לצורך**

<u>נושא המחקר:</u> _____

<u>שם החוקר:</u> _____

<u>כתובת דוא"ל להתקשרות:</u> _____

<u>טל:</u> _____

אני הח"מ:

שם משפחה _____ שם פרטי _____ מס' ת.ז. _____

כתובת _____ מיקוד _____

א. מצהיר/ה בזה כי אני מסכים/ה להשתתף במחקר כמפורט במסמך זה.

ב. הנני מצהיר/ה כי נמסר לי מידע מפורט בעל פה ו/או בכתב על המחקר ובמיוחד הפרטים הבאים הקשורים: למטרות המחקר, לשיטות, למשך הזמן הצפוי, לסיכונים הטמונים הנפוצים, לאי הנוחות העלולה להיגרם ולתועלת הצפויה לי או בכלל מהמחקר.

ג. מצהיר/ה בזה כי הוסבר לי ע"י החוקר/ת כדלהלן:

1. כי החוקר/ת קיבל/ה מוועדת הסקירה של אוניברסיטת בר-אילן ו/או מתת ועדה שלה (פקולטית/מחלקתית) אליה הוא משתייך אישור לביצוע המחקר.
2. כי אני חופשי/ה לסרב לענות על השאלון או להפסיק את מילוי השאלון או השתתפות במחקר / ניסוי בכל עת בלי להינזק.
3. כי מובטחת סודיות בכל הנוגע לפרטיי האישיים ולכל פרט אחר שעלול לחשוף את זהותי.
4. ידוע לי כי האוניברסיטה עשויה לשמור את המידע האישי שלי במאגרי המידע שלה (אם תידרש לכך בהתאם להוראות הדין) וידוע לי כי במידה ויתגלה לי על הפרה לזכות

שלי לפרטיות ו/או יתקיים חשש לפגיעה במידע האישי שלי אוכל לפנות לאנשי הקשר המצוינים בסעיף 5 לטופס זה.

5. הנתונים שייאספו עשויים לשמש לצורכי פרסום אקדמי, לרבות מאמרים, מצגות וכנסים מקצועיים. כל פרסום ייעשה באופן אנונימי, ללא פרטים מזהים של המשתתפים.
6. ידוע לי כי מכוח סעיף 13 לחוק הגנת הפרטיות, התשמ"א-1981 (להלן: "**חוק הגנת הפרטיות**") קיימת לי הזכות לבקש מהחוקר לעיין במידע שלי שמסרתי לחוקר (ויודגש כי אין מדובר במסקנות החוקר ובתוצאות המחקר). החוקר רשאי לסרב לבקשתי בהתאם לתנאים המפורטים בחוק הגנת הפרטיות. כמו כן, במידה ואמצא כי המידע אודותיי אינו שלם או נכון, תהא לי הזכות, בתנאים מסוימים, לבקש מהחוקר לתקן או למחוק מידע זה.
7. ניתן לפנות ל___ לצורך הבהרות לגבי מילוי השאלון או הטיפול (שם וכתובת להתקשרות):

   _____
8. באם יתעורר צורך לשוחח עם איש מקצוע בעקבות מילוי שאלון המחקר או המחקר (שם של איש מקצוע וכתובת להתקשרות): _____

ד. הנני מצהיר/ה בזה כי את הסכמתי הנ"ל נתתי מרצוני החופשי, הבינותי את כל האמור לעיל, ואני מוכן/ה שייעשה שימוש בשאלון/ראיון/ניסוי לצורכי מחקר בלבד.

_____	_____	_____
שם משתתף/ת במחקר	חתימה	תאריך
_____	_____	_____
שם הגורם המסביר	חתימה	תאריך