



מערכת ניהול אבטחת המידע

הנחיות



אוניברסיטת רייכמן
Reichman University



אודות המסמך

א. מטרה

העלאת מודעות חוקרי האוניברסיטה העושים שימוש במידע אישי לנהלי הארגון בתחום אבטחת מידע, הגנת הפרטיות וסודיות המידע ואת חובותיהם מכוח החוק בנושאים אלו.

מעקב שינויים

גרסה	תאריך	שינויים
1.0		

ב. כתיבה

שם	כתיבה
	כותב גרסה נוכחית
	ביקורת גרסה נוכחית

ג. אישור ותוקף

פירוט	תהליך אישור
	הועבר לעיון ועדת היגוי
	אישור
	כניסה לתוקף
	בתוקף עד

ד. תפוצה ושימוש

- 1) חוקרי אוניברסיטת רייכמן, לרבות עמיתי מחקר (להלן כולם ביחד ולחוד: "החוקר") הכפופים לתקנון אתיקה ונוהל מחקרים בבני אדם של האוניברסיטה.
- 2) **כל הזכויות שמורות** © מסמך זה והידע הכלול בו הינם קניינה הבלעדי של אוניברסיטת רייכמן ואינם ניתנים לשימוש ו/או לפרסום ו/או לגילוי ו/או להפצה ו/או להעתקה ו/או בחלקו, במישרין, ו/או בעקיפין ללא הסכמה מראש ובכתב של אוניברסיטת רייכמן.

ה. נספחים

שם	תיאור
נספח א'	אישור קריאת הנוהל
נספח ב'	טופס הסכמה מדעת למשתתף

1. כללי

- 1.1. מטרת הנוהל היא להביא לידיעת חוקר באוניברסיטה, העושה שימוש במידע אישי במסגרת מחקרו, את נהלי האוניברסיטה בתחום אבטחת מידע, הגנת הפרטיות וסודיות המידע ואת חובותיו עפ"י חוק בנושאים אלו.
- 1.2. נוהל זה חל על מחקרים העושים שימוש במידע אישי, כהגדרתם בתקנון אתיקה ונוהל מחקרים בבני אדם של האוניברסיטה.
- 1.3. אוניברסיטת רייכמן רואה חשיבות רבה שמחקר הנערך על ידי חוקריה ו/או בהשתתפותם ו/או מחקר הנערך במימונה ו/או בניהולה ו/או המיוחס לה ו/או על-ידי מי מטעמה, יתקיים בהתאם לכל הוראות הדין.
- 1.4. נוהל זה מוגש כשירות לציבור החוקרים באוניברסיטה וכולל המלצות ליישום הדינים הישראליים החלים לגבי מידע אישי והפניות להמשך העמקה בהוראות הדין. האוניברסיטה שומרת לעצמה את הזכות לשנות את הנוהל בכל עת.
- 1.5. יודגש, למען הסר כל ספק, כי נוהל זה נועד לסייע לחוקר בהכרת החובות המוטלות עליו עפ"י דין, אולם-
 - 1.5.1. אין בו כדי לקבוע כי המחקר הינו בהתאם להוראות כל דין, נוהל, אישור, חוזה או צו של רשות מוסמכת (לרבות, מבלי לגרוע, הוראות הגנת הפרטיות ו/או דינים של מדינות אחרות, בפרט דיני האיחוד האירופי או ארצות הברית), ו/או כי המחקר מקיים או עומד בדרישת הוראות כאמור.
 - 1.5.2. אין בו כדי להסיר מאחריות החוקר לביצוע המחקר ולתוצאותיו וכל הכרוך בו, לרבות לפי נוהל זה ו/או לפי כל דין, נוהל, אישור, חוזה או צו של רשות מוסמכת, ככל שחלים ולפי העניין.
 - 1.5.3. אין בו כדי להטיל כל אחריות על אוניברסיטת רייכמן, ו/או על מי מטעמה ו/או נציגיה, ביחס למחקר המבוצע ו/או ביחס לכל היבט הנוגע בו ו/או לאופן יישומו ו/או לפרשנות של נוהל זה או של הוראות כל דין או צו רלוונטיים אחרים, וזאת - הן כלפי החוקרים, הן כלפי המשתתפים במחקר והן כלפי כל צד שלישי כלשהו.
- 1.6. האחריות להגנת זכויותיהם של המשתתפים היא של החוקרים המבצעים את המחקר ועליהם בלבד, ולפיכך עליהם לנהוג בהתאם להוראות נוהל זה, הוראות נהלים רלוונטיים אחרים באוניברסיטת רייכמן וכן לפי כל דין, לרבות (מבלי לגרוע) הוראות לעניין הגנת הפרטיות.
- 1.7. נוהל זה בא להוסיף על כל נוהל אבטחת מידע וכל נוהל אחר של האוניברסיטה ולא לגרוע ממנו.
- 1.8. ככל שיובא לידיעת נציגי האוניברסיטה כי חוקר הפר את הוראות הדין כמפורט להלן או כי אירע אירוע אבטחת מידע חמור המחייב בדיווח לרשות להגנת הפרטיות, האוניברסיטה תדווח על כך לרשות להגנת הפרטיות.
- 1.9. גרסה עדכנית של מסמך זה ניתנת לצפייה בכל עת באתר האוניברסיטה.

2. תחולה

הנוהל חל על כל אדם המבצע מחקר וקשור באוניברסיטת רייכמן כעובד, איש סגל אקדמי או סטודנט, כהגדרתו בתקנון אתיקה ונוהל מחקרים בבני אדם של האוניברסיטה.

3. אחריות לביצוע הנוהל

חוקרי האוניברסיטה, כהגדרתם בתקנון אתיקה ונוהל מחקרים בבני אדם של האוניברסיטה.

4. רקע

4.1. הזכות לפרטיות מוכרת כזכות יסוד חוקתית ומוגנת בדין הישראלי בחוק הגנת הפרטיות, התשמ"א, 1981.

4.2. בין היתר, החוק מגדיר פגיעה בפרטיות במקרים הבאים: שימוש בשם אדם, כינוי, תמונתו או קולו לשם מטרת רווח; הפרה של חובת סודיות שנקבעה בדין או שנקבעה בהסכם מפורש או משתמע לגבי ענייני הפרטיים של אדם; שימוש בדיעה על ענייני הפרטיים של אדם או מסירתה לאחר שלא למטרה שלמה נמסרה; פרסומו של עניין הנוגע לצנעת חייו האישיים של אדם.

4.3. מידע אישי כולל נתונים על הכשרתו המקצועית, דעותיו ואמונתו של אדם. בנוסף, ייחשב כמידע אישי כל מידע שניתן לזהות באמצעותו, במישרין או בעקיפין, אדם באופן אישי (כגון: תמונה, כתובת מגורים, ת.ז., טלפון, דוא"ל וכו').

4.4. מידע אישי רגיש מוגדר כנתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצב הכלכלי, דעותיו ואמונתו.

4.5. הפרת פרטיות עלולה להיחשב הן לעבירה פלילית והן לעוולה אזרחית (המאפשרת לנפגע לתבוע בגינה).

זכור! איסוף ושמירת מידע מזהה ורגיש יוצר מאגר מידע אישי המטיל חובות בדין על החוקר, כפי שיפורט להלן. לכן, מומלץ לשקול בכובד ראש מהו המידע הנדרש למחקר, לצמצם למינימום האפשרי את המידע הנאסף, להתמים את הנתונים, ולהימנע מאיסוף מידע מיותר שאינו זרוש לתכליות המחקר.

4.6. לפי הגדרתו בסעיף 7 ל- חוק הגנת הפרטיות, מאגר מידע הוא: אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט – (1) אוסף לשימוש אישי שאינו למטרות עסק; או (2) אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר אפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף.

4.7. להלן הוראות הדין העיקריות החלות על מאגר מידע:

א. **רישום המאגר ברשם המאגרים** ברשות להגנת הפרטיות לפי החוק -

מידע נוסף ניתן למצוא באתר הרשות להגנת הפרטיות - הרשות להגנת הפרטיות

ב. תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז - 2017. התקנות מבחינות בין מספר סוגי מאגרים.

להלן פירוט המאגרים הרלוונטיים בד"כ למחקרים באקדמיה:

(1) מאגר המנוהל בידי יחיד - כאשר מתקיימים התנאים הבאים-

- המידע כולל מידע מזהה ונתונים על מעמדו האישי של האדם (דוגמת סטטוס משפחתי), הכשרתו המקצועית.
- יש הרשאת גישה לחוקר (בעל המאגר) ול-2 נוספים לכל היותר.
- להלן קישור למידע נוסף מאתר הרשות להגנת הפרטיות אודות אופן שמירת אבטחת המידע: מדריך תקנות הגנת הפרטיות (אבטחת מידע) לעצמאים ולעסקים קטנים

2) מאגר עליו חלה רמת אבטחה בינונית – המידע המזוהה במאגר הינו לפחות אחד מהבאים: רפואי; נפשי; כלכלי; עבר פלילי; נתוני תקשורת מסוימים (דוגמת מיקום); ביומטרי; גנטי; דעות פוליטיות; אמונות דתיות; הרגלי צריכה שניתן ללמוד מהם על אישיותו של אדם, אמונתו ודעותיו.

במקרה זה, חלות הוראות החוק הבאות - המדריך המלא ליישום תקנות הגנת הפרטיות (אבטחת מידע)

5. המלצות לשימוש במידע אישי במסגרת מחקרית

5.1. שלב כריית המידע

5.1.1. תכנון המחקר

- הגדר במדויק את המידע שייאסף מהמשתתפים בהתאמה לתכליות המחקר. במסגרת פרוטוקול המחקר, ציין תכלית ברורה ומנומקת לכל פריט מידע (שאלה או מידע אישי) בדגש על מחקרים העוסקים במידע מגדרי, נטייה מינית, השתייכות דתית ודעות פוליטיות, הנאסף במסגרת המחקר והמנע מאיסוף מידע עודף שאינו משרת את תכליות המחקר.
 - **צמצם את המידע האישי הנאסף מהמשתתף למינימום הנדרש** לצורך השגת תכליות המחקר. הגדר במדויק מהם פריטי המידע הנדרשים ונמק לצד כל פריט כיצד הם מסייעים לקידום המחקר. הסר בקשות לפריטי מידע שאינן חיוניות.
 - **המנע ככל האפשר מאיסוף מידע מזהה**. במידה והינך מגיע למסקנה כי יש צורך בפריטי מידע מזהים, יש לבצע צעדים להתממת המידע ולהימנע ככל הניתן מאיסוף מידע מדויק, כל זמן שאין בכך פגיעה בתכליות המחקר. דוגמאות-
 - גיל רצוי לציין טווח גילאים, למשל: גיל 30-35.
 - ככל שנדרש הגיל המדויק, יש לציין את גיל המשתתף ולא תאריך לידה מלא.
 - כתובת מגורים: יש להסתפק בזיהוי גיאוגרפי כללי (דוגמת עיר או אזור).
 - שם: שימוש בשמות בדויים או מספרים סידוריים.
- ככל שהינך סבור כי יש חשיבות לשמירת המידע המזהה (לדוגמה לצורך ביצוע מחקר המשך) מומלץ לשמור "מפתח זיהוי" בנפרד ממסמכי המחקר, הכולל את פרטי המשתתפים והשם הבדוי שניתן להם במחקר. יש לוודא כי הגישה למפתח ההצפנה מאובטחת ולהגדיר מורשה גישה יחיד.

זכור! שמירת רשימה מזהה הכוללת מידע רגיש מחייבת ברישום מאגר. לכן, מומלץ לתכנן את המחקר באופן יסודי על מנת להימנע מאיסוף מידע מיותר ומהצורך ביצירת קשר נוסף עם המשתתפים לביצוע מחקרי המשך, דבר אשר יחייב שמירת מפתח זיהוי.

5.2. ביצוע המחקר

- 5.2.1. במסגרת פרטוקול המחקר, תכנן מראש את אופן איסוף המידע.
- 5.2.2. ככלל, לביצוע המחקר, נדרש לעשות שימוש באמצעות משאבי המחשוב המאובטחים של האוניברסיטה.
- 5.2.3. במידה ונדרש לבצע מחקר באמצעות משאבים אחרים, יש לאשר הצורך מול מנהל אבטחת-המידע של האוניברסיטה, ובכפוף לקיום מערכות והגדרות אבטחה בסיסיות במחשב או במערכות "ענן" (בהתאם לסעיף 6 בהמשך).
- 5.2.4. במידה והנכם אוספים מידע מזהה, השיטה הטובה למזעור הפגיעה בפרטיות המשתתפים והגנת המידע הנאסף הינה איסוף מידע באמצעות מפגש אישי עם המשתתף, בו נאסף כל החומר הדרוש תוך הקלדת המידע המחקרי ישירות למחשב וצמצום מינימלי של שימוש בניירת. לשם כך, מומלץ לתכנן מראש את איסוף המידע, לקבוע מפגש אישי עם המשתתף במקום ציבורי בו יש מרחב פרטי לשיחה, ולתעד את המחקר במתן מספר סידורי לכל משתתף.
- 5.2.5. איסוף מידע באמצעות פלטפורמות מקוונות (אבטחת מידע)
- 5.2.5.1. איסוף מידע באמצעים דיגיטליים המותקנים במכשירים פרטיים, דוגמת: שיחות וידאו, העברת סקרים ושמירת תוצאות בתוכנות לא מאובטחות (לרבות כאלו העושות שימוש משני במידע הנאסף או מבצעות שירותי גיבוי), טומן בחובו סיכונים פרטיות והגנת מידע רבים, ולפיכך בין היתר מומלץ לאסוף המידע באמצעות מפגש אישי כמפורט לעיל.
- 5.2.5.2. במידה והחוקר בוחר לעשות שימוש בפלטפורמה מקוונת, יש לנקוט באמצעי הזהירות הבאים: בחירת החלופה המתאימה ביותר בהתאם לרגישות המידע שנאסף; היכרות עם סיכונים אבטחת המידע של המערכת ויישום ההמלצות למניעתם (למשל הימנעות משימוש בשירותי גיבוי פרטיים בענן);
- 5.2.5.3. בנוסף, יש לקבל את הסכמת המשתתף מראש לגבי אופן איסוף המידע ולציין בפניו את המהלכים שבוצעו למזעור הסיכונים.
- 5.2.5.4. שמירת הפרטיות- במידה והמחקר מבוצע באמצעות שיחת וידאו, יש לתכנן מראש עם המטופל את מתכונת הריאיון: לקבוע מראש בשעה ומועד בהם ניתן לקיים את השיחה ללא הפרעות ללא מאזינים נוספים ברקע; במידה והמשתתף מבצע את הריאיון מביתו, לבקש מהמשתתף להציב את המצלמה באופן שאינו חושף את סביבתו שלא לצורך.

5.2.5.5. צילום / הקלטת מפגשים - ככלל, חל איסור על ביצוע צילום מפגשים עם

משתתפים. יש להימנע מהקלטת המפגשים עם המשתתפים, שכן הדבר יחייב את החוקר באמצעי אבטחה מחמירים לרישום ושמירת מאגר תמונות. ככל שהחוקר בוחר להקליט את המפגשים, עליו:

- א. לאשר פרטנית את הצורך מול מנהל הגנת הפרטיות וגם מול מנהל אבטחת-המידע של האוניברסיטה.
- ב. עליו לקבל הסכמה מפורשת מראש מהמשתתפים ולעמוד בכל הוראות הדין.

5.2.6. קבלת הסכמה מדעת מהמשתתף חתומה וערוכה כדין-

5.2.6.1. על החוקר להכין טופס הסכמה מדעת הכולל: הסבר מפורט אודות שלבי השימוש

במידע: אופן האיסוף; התכליות; המידע הנאסף; מקורות המידע לאיסוף (לדוגמה האם ייאסף מידע אודות המשתתף מהאינטרנט); מורשי הגישה למידע; אופן עיבוד המידע (כולל התוכנות); אופן השימוש במידע והצלבתו עם מקורות מידע אחרים; אופן ותקופת שמירת המידע; הזכות לעיון במידע האישי ובקשה לתיקון ומחיקת מידע ואיסור המשך השימוש בו במסגרת תקופת שמירת המידע; אופן פרסום המידע. (מצ"ב בנספח ב' פורמט כדלקמן)

5.2.6.2. בנוסף, ההוראות החלות על טופס ההסכמה מדעת וההקפדה על כללי הפרסום

המחקריים, כמפורט בנהלי ועדת האתיקה, תקפות גם לשימוש במידע אישי בהתאם לדיני הפרטיות ונוהל זה.

5.3. שלב עיבוד המידע

5.3.1. נדרש לבצע את עיבוד המידע במשאבי המחשוב המאובטחים של האוניברסיטה (מחשב או "ענן").

5.3.2. ככל וקיים צורך לבצע עיבוד מידע במשאבי מחשוב שאינם של האוניברסיטה, השימוש מותנה באישור מנהל אבטחת-המידע של האוניברסיטה ובכפוף להצגת מתווה לאנונימיזציה מלאה של הנתונים, בהתאם לכללי ההתממה שהוגדרו בסעיף 5.1.

5.3.3. יעשה שימוש בתוכנות בעלות רישיון חוקי בלבד, בהתאם למחשב המחקר עליו מבוצע העיבוד.

5.3.4. שימוש בתוכנות Freeware ייעשה בכפוף לווידוא אל מול תנאי ההסכם של התוכנה, שאינה דורשת שיתוף נתונים מול יצרן/כותב התוכנה. יש לשים דגש לנושא בשימוש ב-GNU GPL.

5.4. שלב שמירת המידע

5.4.1. היקף המידע הנשמר

5.4.1.1. בהיבטי פרטיות הרלוונטיים למחקר, יש להבחין בין 2 סוגי מידע:

- מידע גולמי - המידע שנאסף מהמשתתף, ועשוי להכיל פרטים מזהים או כאלו העשויים להוביל לזיהוי, כפי שהוסבר לעיל.

- מידע מעובד - המידע שנוצר ע"י החוקר במסגרת מחקרו, וכולל מידע אנונימי, מיצרפי (אגרטיבי) ע"י הקבצה של פריטי המידע הגולמי.
למשל: המחקר בוצע בקרב 30 תלמידים בשנה א'.

5.4.1.2. יש לשמור את המידע המחקרי, בפרט טפסי ההסכמה מדעת, בהתאם לכללים המקובלים בעולם המחקר ביחס לסוג המחקר (לדוגמה- עבודת סמינריון, עבודת תזה וכו') ובהתאם לכללי הפרסום האקדמי.

5.5. שלב סיום המחקר - מחיקת המידע

5.5.1. יש להימנע משמירת מידע גולמי עודף שאינו משרת את תכליות המחקר ולמחוק אותו מיידית ככל שנאסף. יש להקפיד למחוק את המידע גם ממערכות הגיבוי, מהענן ומסל המחזור.

5.5.2. בסיום המחקר, ככל שהדבר עולה בקנה אחד עם כללי המחקר המקובלים הרלוונטיים למחקר, מומלץ למחוק את המידע הגולמי על מנת למזער את סיכוני פרטיות ואבטחת מידע. יש לתכנן מראש בפרוטוקול המחקר מהו המידע שישמר בסיומו, ולעדכן את המשתתף בתקופת השמירה הצפויה בטופס ההסכמה.

5.5.3. כל זמן שהמידע הגולמי שמור באופן הניתן לזיהוי אצל החוקר, זכאי המשתתף לזכות העיון, התיקון והמחיקה של המידע האישי שלו. ככל שהחוקר שומר מפתח זיהוי או מידע מזהה, עליו לעדכן את המשתתף בטופס הסכמה בדבר זכותו. במידה והחוקר אינו שומר את המידע מזהה, יש לציין זאת בטופס ההסכמה ולהבהיר כי לא ניתן יהיה לתקן או לעיין במידע.

6. הנחיות אבטחת-מידע נוספות לשמירת מידע מחקרי

6.1. מערכות אבטחה נדרשות:

6.1.1. מחשב ארגוני מנוהל – יקבל את מערכות ההגנה של הארגון, כל זמן שמחובר לרשת הארגון.

6.1.2. מחשב לא-ארגוני – המחשב יעמוד בתנאי אבטחת-המידע הבסיסים כדלקמן:

א. מחשב עליו נשמר מידע אישי רגיש ומזוהה יהיה מוצפן באמצעות תוכנות הצפנה מוכרות, כגון BitLocker של מיקרוסופט.
ב. על המחשב תותקן תוכנת הגנה (ראו נספח ב') הכוללת לפחות את התוכנות הבאות:

- Anti-Virus (חובה)
- Mail Protection (חובה)
- Anti-Ransomware (חובה)
- Web Security (חובה)
- Firewall (חובה)
- Anti-Phishing (מומלץ)
- Network Attack Protection (מומלץ)

- תוכנת ההגנה תהיה עם אפשרות עדכון של לפחות ברמה החד-יומית
- תוגדר ביצוע בדיקה על כלל המחשב לפחות פעם בשבוע.
- ג. גישה למחשב תהיה באמצעות סיסמה ארוכה מורכבת באורך 12 תווים לפחות או בגישה ביומטרית.
 - 6.1.3. "ענן" ארגוני (של רשת האוניברסיטה) – בהתאם למדיניות האוניברסיטה.
 - 6.1.4. "ענן" לא-ארגוני (מחוץ לרשת האוניברסיטה) – יש לוודא הגדרת סיסמה מורכבת/לא פשוטה בת 10 תווים לפחות + הפעלת הזדהות רב-שלבית.
- 6.2. שמירת המידע
 - א. מערכות ארגוניות מאובטחות –
 - ככלל, עדיפות לשמירה בתיקיות הרשת של האוניברסיטה.
 - בכונן המחשב – במידה והמחשב עבר הצפנה מאושרת (כגון הצפנת BitLocker של מיקרוסופט)
 - כונן "ענן" של רשת האוניברסיטה – ללא מגבלה. במקרה של שיתוף יש לשתף רק גורמים תוך-ארגוניים בצורה מפורשת. לצורך שיתוף גורמי חוץ יש להתייעץ עם מנהל אבטחת-המידע של האוניברסיטה.
 - ב. מערכות חיצוניות לרשת האוניברסיטה:
 - מחשב - במידה והמחשב עבר הצפנה מאושרת (כגון הצפנת BitLocker של מיקרוסופט) ובנוסף הותקנו בו מערכות אבטחה כפי שהוגדר בנוהל.
 - "ענן" - מידע מותמם בלבד בהתאם להנחיות הרשומות בסעיף 5.1. יש לוודא הפעלת הזדהות רב-שלבית בגישה ל"ענן".
- 6.3. שמירת סודיות
 - 6.3.1. חוקר ישתף במידע אישי רק גורם אשר הוגדר כ"עמית מחקר" והגיש הצהרת חוקר לוועדת האתיקה.
 - 6.3.2. על החוקר לפעול לצמצום חשיפת המידע לעמיתי המחקר למינימום הנדרש והרלוונטי לצורך עבודתם.
 - 6.3.3. יש להשתמש במידע רק לתכלית המחקר המוגדרת, ואשר לשמה התקבל אישור ועדת האתיקה והסכמת המשתתפים.
 - 6.3.4. על החוקר להקפיד לשמור על סודיות המידע האישי גם במצבים הבאים:
 - מסכי מחשב, מסמכים מודפסים או ציוד מחשב המכילים מידע אישי כלשהו או מידע חסוי יוצבו, יישמרו וינעלו כך שהמידע לא ייחשף לגורמים לא מורשים והחוקר יקפיד למנוע מגורמים לא מורשים עיון במידע החסוי ובמידע האישי.
 - יש לגרוס כל מסמך המכיל מידע אישי או לתייק אותו במידה שיש צורך מחקרי המחייב בשמירה.
 - 6.3.5. החוקר, לרבות עמית המחקר, מחויב:
 - א. לשמור על מידע אישי אליו נחשף במסגרת המחקר בסודיות מוחלטת;

- ב. לא לגלות המידע אישי לכל גורם אחר אשר אינו מעורב במחקר.
- ג. לא לגלות אותו לכל גורם מחוץ לאוניברסיטה אלא בהסכמת המשתתף במחקר (נושא המידע) או כשהדבר מחויב על פי דין;
- ד. לשמור על המידע האישי מפני דליפה, בין היתר על ידי קיום עקרונות אבטחת המידע המפורטים בנוהל זה, בנוהלי האוניברסיטה ובהתאם לדרישות הדין.
- 6.4. הוצאת מידע מאוניברסיטת רייכמן
- 6.4.1. חל איסור להוציא מידע מחקרי אל מחוץ לאוניברסיטה ו/או להעביר מידע לגורמים חיצוניים למעט במקרים שאושרו מראש ע"י ועדת האתיקה, ובכפוף לנוהל זה ובאישור מראש ובכתב של מנהל הגנת הפרטיות והממונה על אבטחת המידע.
- 6.4.2. מידע יועבר, לאחר קבלת האישור, בצורה מאובטחת ומוצפנת בלבד, בהתאם לתנאים המפורטים באישור.
- 6.5. אבטחת מידע במחשב ובעמדת העבודה
- 6.5.1. יש להקפיד על שמירת ניירת או מדיה המכילים מידע אישי או מידע חסוי במיקום מאובטח (ארון נעול, מגירה נעולה או כספת).
- 6.5.2. אין להשאיר מחשב נייד ללא השגחה ברכב נעול ובמקומות ציבוריים כגון: בתי קפה, מלונות, שדות תעופה וכדומה
- 6.5.3. יש לנעול המחשב בעת עזיבת העמדה (ע"י פקודת WINKEY+L / CTRL+ALT+DEL).
- 6.5.4. יש לוודא כי המחשב מוגדר עם סיסמה לפתיחה והגדרת נעילה לאחר זמן אי-שימוש של 30 דקות.
- 6.5.5. אין לפתוח הודעות דואר אלקטרוני או קבצים מצורפים אשר מקורם אינו מוכר.
- 6.6. שם משתמש וסיסמא
- 6.6.1. חל איסור מוחלט למסור את שם המשתמש ו/או הסיסמא שלך לאדם אחר או להשתמש בשם משתמש וסיסמא של אדם אחר.
- 6.6.2. יעשה שימוש בסיסמא מורכבת בהתאם למדיניות אבטחת-המידע העדכנית לעת ביצוע המחקר. לחילופין ניתן להשתמש בפתרונות זיהוי ביומטרי.
- 6.6.3. יש להימנע משמירת הסיסמא במקום בו היא עלולה להיחשף.
- 6.6.4. בכל מקרה של חשיפת הסיסמא או חשד לחשיפתה, יש להחליף את הסיסמא מיידית ולדווח למנהל אבטחת המידע אודות המקרה.
- 6.7. שימוש במדפסות, בסורקים ובמכשירי פקס
- 6.7.1. החוקר אחראי לאסוף את החומר ששלח להדפסה והכולל מידע אישי או מידע חסוי מהמדפסת מיד לאחר שליחתו להדפסה, על מנת לוודא כי החומר המודפס לא ייקרא או יילקח ע"י גורם לא מורשה.

6.7.2. על חוקר המבצע סריקה של חומרים הכוללים מידע אישי או מידע חסוי לוודא כי בסיום הסריקה החומר הסרוק הגיע ליעד הנכון וכי הוא אסף את החומרים אותם סרק.

6.8. גישה לרשת האינטרנט

- 6.8.1. אין להמשיך לגלוש באתר כאשר הדפדפן / תוכנת האבטחה מתריעה על סכנת אבטחת מידע.
- 6.8.2. אין לשתף מידע אישי וחסוי ברשתות חברתיות.
- 6.8.3. אין להעלות כל מידע אישי לכונני אינטרנט (Drop Box, Google Drive וכדומה). בכל מקרה של צורך עסקי להעברת נפח מידע גדול לגורם צד ג', יש להתייעץ עם מנהל אבטחת המידע.

6.9. תחזוקת מחשב

בכל מקרה של צורך בביצוע החלפת כונן קשיח במחשב המחקר יש להתייעץ עם ממונה אבטחת המידע באוניברסיטה, לפני ביצוע התיקון.

7. דיווח - יש לדווח למנהל אבטחת המידע של האוניברסיטה במקרים הבאים:

- 7.3.1. חשיפה או חשד לחשיפה של מידע אישי או פרטי לגורם לא-מורשה.
- 7.3.2. חשיפה או חשד לחשיפה סיסמת המחשב לגורם לא-מורשה.
- 7.3.3. אובדן המחשב או כל מדיה שעליה שמור מידע רגיש.
- 7.3.4. גילוי וירוס או פוגען אחר במחשב.
- 7.3.5. אי-עמידה בכל אחת מההנחיות כפי שפורטו במסמך זה.

8. האוניברסיטה שומרת לעצמה את הזכות לבצע בקרות בנושאי אבטחת-מידע והגנת הפרטיות במחשבי המחקר.

נספח א'

אל:

8.3.1. ועדת אתיקה

8.3.2. מנהל אבטחת מידע

8.3.3. מנהל הגנת הפרטיות

הנדון: הנחיות אבטחת המידע לעובד באוניברסיטת רייכמן

הנני מאשר/ת שקראתי והבנתי את ההנחיות שבנדון, ומתחייב לנהוג על פיהן:

שם החוקר: _____

ת.ז.: _____

שם המחקר: _____

פרטי יצירת קשר: _____

חתימה: _____

תאריך: _____

הבהרה: כל גורם המשתתף במחקר, דוגמת עמית מחקר או עוזר מחקר מחויב בחתימה על הנספח.

נספח ב'

רשימת תוכנות אבטחה להתקנה על מחשב שאינו מנוהל

הרשימה מתאימה למחשבים מבוססי מערכת-הפעלה Windows ומערכת-הפעלה MacOS:

1. Bitdefender Antivirus

2. Intego

3. TotalAV

4. Panda