תוכן עניינים

פרק א' – מבוא 2
רקע 2
מטרה 2
מקורות משפטיים 2
הגדרות ומושגים כלליים 3
פרק ב' – בעלי התפקידים 3
פרק ג' – עקרונות 4
פרק ד' – איסוף ואגירת מידע 5
פרק ה' העברת מידע לגורמים אחרים 5
פרק ו' – זכות עיון, תיקון והתנגדות 6
פרק ז' – שקיפות 6
פרק ח' – סודיות ואבטחה 7
פרק י"ד – תעוד, פיקוח ובקרה 8
פרק ט"ו – תלונות 8
פרק ט"ז – שינוי ועדכון 9
פרק י"ז - אחריות 9
נספחים 10

פרק א' – מבוא

רקע

במאי 2018 נכנסו לתקפן תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן "התקנות הישראליות"), המפרטות את אופן יישומה של חובת אבטחת המידע המוטלת בחוק הגנת הפרטיות הישראלי על כל גורם המחזיק, מנהל או מעבד מאגר של מידע אישי. הרשות להגנת הפרטיות (להלן: "הרל"פ") מונתה כגוף המפקח על יישומן של התקנות, שמטרתן הפיכת אבטחת המידע לחלק משגרת ניהול הארגון.

באותו חודש נכנסה לתוקף גם רגולציית ההגנה על הפרטיות (General Data Protection Regulation) (להלן "GDPR") המהווה אוסף של הוראות מחייבות שהוסדרו על ידי הפרלמנט האירופי, מועצת האיחוד האירופי והנציבות האירופית. הרגולציה מתייחסת לאיסוף, שמירה והעברה של נתונים אישיים של אנשים פרטיים, נתיני האיחוד האירופי, וקובעת כללים וסטנדרטים אחידים לאבטחת מידע אישי. הרגולציה נועדה בעיקר לאפשר לכל תושב באיחוד האירופי שליטה מרבית על הפרטים שנשמרו אודותיו בחברות פרטיות, ציבוריות וגופים עסקיים וממשלתיים. הרגולציה חלה על כל ארגון וכל אדם, גם אם אינם פועלים בטריטוריה של האיחוד האירופי, ובלבד שהם מעבדים נתונים של נושאי מידע שהנם תושבי האיחוד האירופי. במסגרת זו חלים איסורים ומגבלות על העברת מידע אל מחוץ לטריטוריית האיחוד, בשל החשש להפרות שעלולות להתרחש באזורים בעולם בהם הפרטיות אינה מוגנת כראוי.

מסמך זה נועד לתת מענה הן לתקנות הישראליות והן לרגולציית ה-GDPR. במסגרת החוק הישראלי נדרשת אוניברסיטת חיפה (להלן "האוניברסיטה") ליישם כללים הנוגעים להבטחת הפרטיות והגנת המידע האישי. בנוסף, מחוייבת האוניברסיטה לעמידה בהנחיות הפרטניות שפרסמה הרל"פ.
כמו כן, נדרשת האוניברסיטה לקבל עליה את תקנות ה-GDPR בכל אותם מקומות בהם מעורבת פעילות של תושבי/נתיני האיחוד האירופי (סטודנטים תושבי האיחוד, מחקרים אודות תושבי האיחוד וכד').

מטרה

1. קביעת מדיניות בנושא הבטחת הפרטיות והגנה על מידע אישי באוניברסיטה.
2. מיפוי מאגרי המידע המכילים מידע אישי באוניברסיטה.
3. קביעת נהלי העבודה הנדרשים על מנת להגן על מידע אישי באוניברסיטה.
4. קביעת האחראים ליישום מדיניות ההגנה על הפרטיות באוניברסיטה, כולל מנגנוני הטמעה, פיקוח ובקרה.
5. קביעת תהליכי אישור ועדכון של מסמך זה.

מקורות משפטיים

מסמך זה יורש את תוקפו מ:

1. חוק הגנת הפרטיות, התשמ"א—1981 (להלן: "החוק") והתקנות שנקבעו על פיו ובפרט תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 .
2. חוק התקשורת (בזק ושידורים), התשמ"ב – 1982 (להלן: "חוק התקשורת").
3. חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח – 2007.
4. הוראות הרשות להגנת הפרטיות (להלן: "הוראות הרל"פ").
5. רגולציית ההגנה על הפרטיות (General Data Protection Regulation - GDPR).

הגדרות ומושגים כלליים

- **"נושאי המידע"** (בהקשר האוניברסיטה): עובדי האוניברסיטה (בכל סוגי הסגלים כולל גמלאים), מועמדים, מתעניינים, סטודנטים ובוגרים, ספקים ובעלי עניין נוספים, אנשים שהינם מושא מחקרים, עובדי אגודת הסטודנטים, ארגוני העובדים וחברת "כרמל" – תוצר של הסכמים מול האוניברסיטה, אשר לגביהם קיים מידע פרטי באוניברסיטה כהגדרתו להלן.
- **"מידע אישי"** - כל מידע אודות נושא מידע מזוהה או ניתן לזיהוי באמצעים סבירים; כגון: שמו של אדם, כתובתו, פרטי התקשרות עמו, מספר תעודת זהות וכד'.
- "**מידע רגיש"** - מידע המתייחס לצנעת חייו האישים של נושא מידע, ציוניו באוניברסיטה, מצבו הרפואי או הנפשי, דעותיו הפוליטיות ואמונותיו הדתיות, נטיותיו, הרגליו ומעשיו המיניים, מידע גנטי ,מידע כלכלי, לרבות מידע אודות הרגלי הצריכה של אדם, מידע אודות עברו הפלילי של אדם וכד'.
- **"מידע פרטי"** – מידע אישי ו/או רגיש.
- "**מאגר מידע"** - אוסף נתוני מידע פרטי לגבי נושאי המידע, המוחזק באמצעי דיגיטלי והמיועד לעיבוד ממוחשב ואשר חשיפתו מהווה פגיעה בפרטיות לגבי נושאי המידע הנכללים בו.
- **"עיבוד מידע"** - איסוף, אחזקה, שימוש, העברה, מחיקה או השמדה של מידע פרטי.
- **"אירוע אבטחת מידע"** – חשיפת בלתי מבוקרת של מידע פרטי, פגיעה בזדון בשלימות המידע והפרעה זדונית לזמינות מערכות המידע באוניברסיטת חיפה.

פרק ב' – בעלי התפקידים

- ## הממונה על הגנת הפרטיות – DPO (להלן: "DPO")

1. ה-DPO ימונה על ידי סגן נשיא ומנכ"ל האוניברסיטה.
2. באחריות ה-DPO לבקר את קיום האמור במסמך מדיניות זה ולהבטיח את ההגנה על הפרטיות והמידע האישי באוניברסיטה בהתאם לכללי התקנות הישראליות ה-GDPR.
3. ה-DPO ישמש כנציב פניות בענייני הגנת הפרטיות עבור נושאי המידע.
4. כ-DPO מונה מר נדב אזולאי. להלן פרטי הקשר:

   נדב אזולאי
   אגף מחשוב ומערכות מידע – אוניברסיטת חיפה
   טלפון: +972-4-8240223 | דוא"ל: nazoulay@univ.haifa.ac.il

- ## ממונה על אבטחת מידע

1. הממונה על אבטחת המידע ימונה על ידי סגן נשיא ומנכ"ל האוניברסיטה.
2. באחריות הממונה על אבטחת המידע:
   - כתיבת נוהל אבטחת המידע ומדיניות ההגנה על הפרטיות.
   - יישום מדיניות אבטחת מידע ומדיניות ההגנה על הפרטיות.
   - ביצוע סקר סיכונים ופערים תקופתי וגזירת תכנית העבודה בהתאם לתוצרי הסקר.
   - ביצוע מבדקי אבטחת מידע לתיקוף יעילות ההגנות הקיימות באוניברסיטה.
   - הטמעת מדיניות אבטחת המידע וההגנה על הפרטיות באוניברסיטה.
   - טיפול באירועים החשודים כאירועי אבטחת מידע.
   - איתור אמצעים להגנה מפני אירועי אבטחת מידע ובקרה על הטמעתם באוניברסיטה.
3. הממונה על אבטחת מידע באוניברסיטה הוא:

נדב אזולאי
אגף מחשוב ומערכות מידע – אוניברסיטת חיפה
טלפון: +972-4-8240223 | דוא"ל: nazoulay@univ.haifa.ac.il

- **נאמני אבטחת מידע באגף מחשוב ומערכות מידע**

מנהל המחלקות ומנהלי המדורים באגף מחשוב ומערכות מידע משמשים כנאמני אבטחת מידע בכל הקשור לעמידה בנהלי אבטחת המידע ומדיניות הגנת הפרטיות בנושאים המקצועיים אשר עליהם הם אמונים.

- **נאמני אבטחת מידע בפקולטות וביחידות האוניברסיטה**

ראשי צוותי המחשוב בפקולטות וביחידות האוניברסיטה משמשים כנאמני אבטחת מידע ביחידותיהם ובכל הקשור למערכות המידע והמחשוב שתחת אחריותם. מתפקידו של נאמן אבטחת המידע בפקולטה ו/או ביחידה לוודא עבודה לפי הנהלים וההנחיות, כפי שיפורסמו מעת לעת ע"י הממונה על אבטחת המידע באוניברסיטה, ולהתריע בפניו על כל חריגה או חשד לאירוע אבטחת מידע.

פרק ג' – עקרונות

1. **עיבוד הוגן וחוקי** - האוניברסיטה מעבדת מידע אישי באופן חוקי והוגן, אוספת מידע אישי רק בהסכמה של נושא המידע או ממקורות הפועלים כדין.
2. **הגבלת מטרה** - האוניברסיטה מעבדת מידע אך ורק למטרות שלשמן נמסר לה המידע על-ידי נושאי המידע.
3. **העברת נתונים לגופים צד שלישי** – האוניברסיטה לא תעביר מידע פרטי לצד שלישי ללא הסכמתו של נושא המידע, למעט מקרים שבהם היא מחויבת על פי חוק. עם זאת, עושה שימוש בשירותי מיקור חוץ לעיבוד מידע. במקרה כזה, חותם הספק בפני האוניברסיטה על הסכם סודיות ומשמש כזרוע תפעולית של האוניברסיטה.
4. **שקיפות** - האוניברסיטה מפרטת בפני נושאי המידע את מטרות השימוש במידע שנאסף וכן מציינת בפניו כי עומדות לו זכויות עיון, תיקון והתנגדות כמפורט להלן.
5. **זכות עיון, תיקון והתנגדות -** האוניברסיטה מעניקה לנושאי מידע זכות לעיין במידע אישי אודותיהם; לתקנו במידה שנמצא לא מדויק או מעודכן; ולהתנגד לשימוש בו למטרות דיוור ישיר.
6. **סודיות ואבטחה** - האוניברסיטה שומרת על סודיות מידע אישי ומיישמת מנגנונים טכנולוגיים וארגוניים נגד אובדנו, פגיעה בשלמותו, גישה אליו ללא הרשאה או שינויו שלא כדין. מידע רגיש יזכה לדרגת אבטחה גבוהה והגישה אליו תחייב תהליכי זיהוי או אימות זהות הולמים.
7. **אחריות** - האוניברסיטה מיישמת תהליכים ארגוניים להבטחת האחריות של החברה, מנהליה, עובדיה, וספקיות שירותים עימם היא עובדת - לקיום המדיניות והעקרונות המוגדרים במסמך זה.
8. **אנונימיות** – במחקר הכולל מידע פרטי, תהיה העדפה לשמירת המידע באופן אנונימי, כך שלא תתאפשר זיהוי נושאי המידע. מפתח הזיהוי ישמר בנפרד מהנתונים.

פרק ד' – איסוף ואגירת מידע

1. בכל איסוף של מידע אישי, האוניברסיטה תודיע לבעל המידע או למי שמסר את המידע (במקרה של קבלת המידע מצד שלישי), ובכתב, מהן מטרות איסוף המידע, למי יועבר המידע, וכל מידע אחר הנדרש בהתאם להוראות החוק או כל דין.

2. במוקדים הטלפוניים של האוניברסיטה, בהם מתבצעת הקלטת שיחות רציפה או אקראית, תושמע בתחילת השיחה הודעה המציינת את העובדה כי חלק מהשיחות מוקלטות ומשמשות לשיפור השירות.
3. בעת איסוף מידע פרטי לצרכי שיווק ודיוור, יאשר הפונה את הסכמתו לשימוש במידע למשלוח מסרים שיווקיים. האוניברסיטה תעמיד כלים שיאפשרו לנושא המידע לממש את זכותו להימחק מרשימת התפוצה גם אם הביע את הסכמתו בעבר.
4. כל תהליך חדש של איסוף מידע פרטי, יאושר מראש על ידי הממונה על אבטחת המידע באוניברסיטה. האישור יתייחס לפרטי המידע הצפוי, המטרות להן יועד המידע וכן אישור תוכנית ניהול הנתונים שתכלול גם את הגדרת התשתית המחשובית באמצעותה ייאסף המידע, אמצעי האבטחה והבקרות על הגישה למידע.
5. בכל מחקר המכיל מידע פרטי, יחתום החוקר על מסמך אבטחת פרטיות שיכלול את תכנית ניהול הנתונים כמפורט בסעיף 4 לעיל. חתימת החוקר תהיה טרם תחילת איסוף הנתונים.
6. חוקר המעוניין לשלב מידע פרטי בשירותי ענן ציבורי (פלטפורמה, שירות או תכנה), יוכל להתקשר רק עם ספקי ענן המאושרים על ידי הממונה על אבטחת המידע באוניברסיטה וזאת במסגרת תוכנית ניהול הנתונים של המחקר. במידה וחוקר מעוניין להפעיל שירות ענני שאינו ברשימת ספקי הענן המאושרים, יגיש בקשה לאישור הספק/השירות טרם השימוש. במידת הצורך יממן החוקר מבחן חדירה לשירות המבוקש.
7. מידע פרטי המשמש את הסגל המנהלי לצורך עבודתו, יישמר על שרתי האוניברסיטה. עובדי האוניברסיטה יימנעו, עד כמה שניתן, מגזירת נתונים מתוך מאגרי המידע המרכזי אל תוך עמדות הקצה או שליחת המידע הפרטי בדואר אלקטרוני. במידה וחיוני לשלוח מידע פרטי בדואר אלקטרוני, יתבצע הדבר באמצעות קישור לקובץ בשרתי האוניברסיטה או באמצעות שליחת קובץ מוצפן כשסיסמת הקובץ תועבר באמצעי אחר. בכל מקרה לא יישמרו הנתונים מעבר לזמן קצוב וקצר ויימחקו על ידי העובד שגזר את הנתונים בתום השימוש. חל איסור לשמור נתונים פרטיים על מחשבים אישים פרטיים.
8. חוקרים ומורים מן החוץ המבקשים לשמור מידע פרטי על מחשבים שמחוץ לרשת האוניברסיטה, ישמרו את המידע באמצעות קבצים מוצפנים. במידה וניתן, יקודדו הפרטים האישיים של נושאי המידע. באחריות החוקר להתקין במחשבים אילו אנטי וירוס מעודכן ורכיבים למניעת אנומליות.
9. פרסום מידע מזוהה כל שהוא כמו: רשימות סטודנטים, ציונים וכד' יעשה אך ורק באופן מאובטח ובאמצעים המקובלים, אין לשתף מידע כזה על גבי אתרי אינטרנט ציבורי, שיתוף דרך שירותי קבצים ועוד. כמו יש להימנע עד כמה שניתן מפרסום מידע מזוהה באתרים פנימיים ובקמפוסנט.

פרק ה' העברת מידע לגורמים אחרים

1. העברת מידע לצד שלישי מתבצעת על ידי האוניברסיטה מתוקף חוק ו/או רגולציה, לצרכי התפעול השוטף של האוניברסיטה (ספקי שירותים ומיקור חוץ) או למטרות רווחה בהסכמת נושא המידע.
2. כל התקשרות עם ספק חיצוני, שכוללת בתוכה העברת מידע, או מתן גישה למידע שבאחריות האוניברסיטה, תעשה רק לאחר קבלת אישור הממונה על אבטחת מידע או סגן נשיא ומנכ"ל האוניברסיטה.
3. בכל מקרה של העברת מידע פרטי, או מתן גישה למידע שכזה, יש לוודא כי הגורם המקבל ייחשף למינימום המידע הנדרש לביצוע המשימה שבעטיה אושרה העברת המידע. כמו כן, יחויב מקבל המידע/הגישה לחתום על הסכם שמירת סודיות המידע האישי ואבטחתו, ולא לעשות בו כל שימוש למעט המטרה שלשמה נמסר.
4. האוניברסיטה תעביר מידע פרטי לספקי שירות / מיקור חוץ רק לאחר עריכת בדיקות נאותות, כולל קבלה החתמתם על הסכם שמירת סודיות המידע ואבטחתו על ידי ספקית השירות ועובדיה

שייחשפו למידע. האוניברסיטה תקיים בדיקות נאותות תקופתיות על מנת לוודא את איכות אבטחת המידע בקרב ספקי השירות / מיקור החוץ.

5. בעת העברת מידע לגוף ציבורי (כדוגמת ביטוח לאומי, רשויות המס וכד'), האוניברסיטה תיישם את "נוהל העברת מידע" וסדרי העברת המידע בין גופים ציבוריים, אשר נקבעו בתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו – 1986.

פרק ו' – זכות עיון, תיקון והתנגדות

1. על פי התקנות הישראליות וה-GDPR, זכאי כל אדם לעיין במידע הפרטי אודותיו, המוחזק בידי האוניברסיטה.
2. האוניברסיטה תאפשר לנושא מידע לעיין במידע אישי אודותיו לאחר פנייה בכתב ל-DPO, באמצעות אתר האוניברסיטה, וזאת בליווי תשלום כדין וכל עוד לא קיימת עילה שבדין לדחיית הבקשה.
3. נושא מידע זכאי להגיש בקשה בכתב לתיקון מידע פרטי שאינו נכון, שלם, ברור או מעודכן, והאוניברסיטה תתקן את המידע האישי כל עוד לא קיימת עילה לדחיית הבקשה.
4. נושא מידע, נתין/תושב האיחוד האירופי, זכאי להגיש בקשה בכתב למחיקת מידע פרטי אודותיו. האוניברסיטה תפעל למימוש בקשתו כל עוד לא קיימת עילה שבדין לדחיית הבקשה.
5. נושא מידע זכאי לדרוש בכתב שמידע אישי אודותיו יימחק ממאגר מידע המשמש לדיוור ישיר או שמידע אישי אודותיו המוחזק במאגר מידע המשמש לשירותי דיוור ישיר, לא יימסר לאדם, לסוג בני אדם או לאנשים מסוימים, גם אם הביע הסכמתו בעבר. כל דיוור ישיר יכלול גם פסקה המאפשרת מחיקה לאלתר ממאגר הדיוור הישיר.
6. ייבנה מנגנון דיוור ישיר אחוד לכל האוניברסיטה. לא ייעשה שימוש ברשימות תפוצה עצמאיות ביחידות ובפקולטות.
7. מועמדים, בוגרים או גמלאים, המבקשים להימחק ממאגרי הדיוור הישיר, יגישו בקשה באמצעות טופס הנמצא באתר האוניברסיטה. כתובת הדואר האלקטרונית של הפונה תימחק באופן אוטומטית ממנגנון הדיוור הישיר האחוד.

פרק ז' – שקיפות

1. כל עובד באוניברסיטה (גם עובדים קיימים וגם עובדים חדשים) יחתום על מסמך הסכמות דיגיטלי במסגרתו הוא מאשר את הכנסת פרטיו האישיים למאגר, את העברת המידע לנותני שירותים ומיקור חוץ, את הסכמתו לביצוע עיבודים סטטיסטיים אישיים וכלליים על נתוניו האישיים וכן יחתום האם מאשר את העברת פרטיו האישיים לארגוני העובדים הרלוונטיים.
2. כל מועמד המוסר פרטים ליצירת קשר (ליד) יחתום על מסמך הסכמות דיגיטלי במסגרתו הוא מסכים שפרטיו ייכללו במאגר המועמדים של האוניברסיטה, וכי המידע יכול להיות מעובד על ידי ספקי שירותים / מיקור חוץ חיצוניים ויכולים לשמש גם לעיבודים סטטיסטיים. בעת מסירת הפרטים יאשר/לא יאשר המועמד את הסכמתו להיכלל ברשימת הדיוור.
3. בעת הרשמה ללימודים באוניברסיטה, יחתום על מסמך הסכמות דיגיטלי במסגרתו הוא מסכים שפרטיו ייכללו במאגר הסטודנטים של האוניברסיטה, וכי המידע יכול להיות מעובד על ידי ספקי שירותים / מיקור חוץ חיצוניים ויכולים לשמש גם לעיבודים סטטיסטיים. בעת מסירת הפרטים יאשר/לא יאשר המועמד את הסכמתו להיכלל ברשימת הדיוור. הזכות שלא להיכלל ברשימת הדיוור תקפה כל עוד הינו בסטטוס מועמד. לסטודנט פעיל לא עומדת האפשרות להימחק מרשימת הדיוור.

פרק ח' – סודיות ואבטחה

1. האוניברסיטה מתחייבת לשמור על סודיות המידע הפרטי המופקד בידיה. כל עובד אוניברסיטה או ספק שירות, בעלי גישה למידע פרטי שברשות האוניברסיטה, יוחתמו על כתב סודיות דיגיטלי המתייחס לשמירה על סודיות מידע פרטי ועל הגבלת השימוש בו במסגרת תפקידם בלבד.
2. עובדים הנגישים למידע רגיש יעברו תהליכי סינון הכוללים היבטי אמינות וזאת בהתאם למוגדר בחוק.
3. עובדי האוניברסיטה יעברו מעת לעת הדרכות ריענון בתחום אבטחת המידע וההגנה על הפרטיות.
4. האוניברסיטה מיישמת מנגנונים טכנולוגיים וארגוניים על מנת למנוע אובדן מידע, פגיעה בשלמותו, גישה אליו ללא הרשאה או שינויו שלא כדין, והכל בהתאם למסמך "**מדיניות אבטחת מידע באוניברסיטת חיפה**".
5. מסמך מדיניות אבטחת מידע יכלול, בין היתר, את מנגנוני אבטחת המידע הבאים:

- מיפוי מערכות מידע וסקר סיכונים תקופתי.
- אבטחה פיסית וסביבתית של מאגרי המידע, כולל תיעוד מלא של הניגשים פיסית לשרתים המארחים את מאגרי המידע ו/או את המערכות המאפשרות גישה למאגרי המידע.
- קיום מגבלות בגישה אל נתוני מאגרי המידע ומימוש מנגנוני הרשאות והגבלתן בהתאם לעקרון ה"צורך לדעת".
- ניהול סיסמאות – האוניברסיטה מיישמת מדיניות סיסמאות מחמירה, בה כל הסיסמאות הינן סיסמאות חזקות אשר מוחלפות אחת לחצי שנה.
- עובדים באגף מחשוב ומערכות מידע ובצוותי מחשוב בפקולטות וביחידות האוניברסיטה, אשר במסגרת תפקידם הינם חשופים למידע פרטי רוחבי, יזדהו אל מול המערכות במנגנון של הזדהות כפולה.
- בכל המערכות המכילות גישה למידע פרטי יש מדיניות של נעילת משתמש לאחר 5 ניסיונות כושלים של כניסה למערכת.
- הפרדה רשתית באמצעות חומת אש בין חוות השרתים ושאר רשת האוניברסיטה.
- כל תחנות הקצה מהן מתבצעות פעולות הכוללות גישה למידע אישי, יהיו מנוהלות, ומוגנות ע"י האמצעים המוגדרים באוניברסיטה מעת לעת (אנטי וירוס, אמצעים להגנה בפני אנומליות וכד').
- כל פעילות הגישה לנתונים במאגרי המידע (קריאה, עדכון, מחיקה) יתועדו באופן שוטף בכלל המערכות (ובפרט במערכות ה-SAP, המערכת הכספית ומערכת ה-Moodle) כולל זיהוי הגורם אשר ביצע את הגישה לנתונים.
- תוגדר אמנת שירות פרטנית לכל מערכת ומאגר מידע למימוש גיבוי תקופתי רב דורי של המידע והטמעת נהלים ומנגנונים להבטחת שיחזור המידע בעקבות אירועים של אובדן, הרס או שיבוש.
- בהשתלטות מרחוק על עמדות קצה של סגל מנהלי תיושם הפרדה מוחלטת כך שלא ניתן יהיה לשתף משאבים (כוננים, מדפסות וכד') בין המחשב הנשלט למחשב המשתלט.
- כל עמדות הקצה (הן של סגל מנהלי והן של סגל אקדמי) החשופות למידע פרטי ישירות מתוך מאגרי האוניברסיטה (ובכלל זה כלל העמדות המריצות SAP), ביחידות המנהל ובפקולטות, יהיו מנוהלות.
- על כל עמדות הקצה (הן של סגל מנהלי והן של סגל אקדמי) החשופות למידע פרטי ישירות מתוך מאגרי המידע של האוניברסיטה תיושם מדיניות של נעילת מסך אוטומטית לאחר 30 דק' של העדר פעילות.
- בכל עמדות הקצה (הן של הסגל המנהלי והן של הסגל האקדמי) החשופות למידע פרטי ביחידות המנהל ובפקולטות יותקנו כל אמצעי ההגנה המקובלים באוניברסיטה, במידע וקיים

קושי טכני ביישום, יגובש פתרון חלופי על דעת הממונה על אבטחת מידע טרם חשיפת התחנה למידע פרטי.

- עם כניסתו של עובד לתפקיד חדש, יוגדרו עבורו ההרשאות הנדרשות לביצוע תפקידו במסגרת "הצורך לדעת". האוניברסיטה תממש טופס טיולים ממוחשב למעבר בין תפקידים או סיום תפקיד (עזיבת האוניברסיטה או יציאה לגמלאות). במסגרת זו יימחקו כל ההרשאות שהעובד נדרש להם במסגרת תפקידו הקודם. בטופס זה יוגדר האם יישמרו לעובד שירותי דואר אלקטרוני. הטופס יכלול הצהרת העובד לפיה אין ברשותו חומר פנימי או סודי לרבות מידע פרטי ויתחייב למחוק חומר כזה במידה וקיים ברשותו.

פרק י"ד – תעוד, פיקוח ובקרה

1. כל ארוע של אבטחת מידע ידווח לנאמן אבטחת מידע יחידתי או לממונה על אבטחת המידע באוניברסיטה, יש להקפיד לדווח סמוך ככל האפשר למועד התרחשות האירוע, הדווח הראשוני יכלול מידע על המערכות שנפגעו (הושבתו או נחשפו), המידע שאוכסן במערכות אלה תוך מתן דגש על מידע פרטי והוא ינחה לגבי המשך הטיפול באירוע, במידת האפשר יש לנתק את המכונה מהרשת.
   הממונה על אבטחת המידע מצידו, מידי ריבעון יזום דיון בהשתתפות בעלי התפקידים במאגרים וכן גורמים נוספים על פי הצורך.
2. אגף מערכות מידע ככלל, וממונה אבטחת מידע בסיוע נאמני אבטחת מידע בפרט, יפקחו וידווחו על קיום המדיניות לממונה על הגנת הפרטיות. הממונה על הגנת הפרטיות יערוך ביקורות, כולל ביקורות פתע, כדי לוודא קיומם של העקרונות והמדיניות במחלקות העסקיות השונות. במידה שנתגלו מקרים של הפרות ו/או אי קיום המדיניות, ישתף הממונה על הגנת הפרטיות פעולה עם המחלקה הרלוונטית לפתרון הבעיה ומעקב אחרי יישומו. הממונה על הגנת הפרטיות ישתף פעולה עם רשם מאגרי המידע במידה שזה יערוך ביקורת או פיקוח על נהלי הפרטיות והגנת המידע ואופן יישומם.
3. מידי 18 חודש יתבצע סקר סיכונים וביקורת אבטחת מידע. הסקר יתבצע על ידי גורם בעל הכשרה מתאימה לביקורת בנושא אבטחת מידע.
4. תוכנית העבודה השנתית של הממונה על אבטחת המידע תכלול גם בקרה שוטפת על העמידה בדרישות החוק, תוכנית ביצוע מבחני חדירה למערכות המתפעלות מאגרי מידע בעלי רמת אבטחה גבוהה.
5. אחת לשנה, יעדכן הממונה על הגנת הפרטיות את מיפוי מערכות ותזרימי המידע האישי על מנת להבטיח כי כל מידע אישי באוניברסיטה משויך לאחד ממאגרי המידע ומטופל בהתאם לנהלים הקבועים לאותו מאגר מידע.
6. הממונה יגיש, מעת לעת, ולפי הצורך, דין וחשבון לראש אגף מחשוב ומערכות מידע בנושא מימוש המדיניות, חריגות והפרות, וצעדים נחוצים להבטחת יישומה המיטבי בעתיד.

פרק ט"ו – תלונות

- נושא מידע המעוניין להתלונן על אופן יישום המדיניות על-ידי האוניברסיטה או מי מעובדיה, יפנה בכתב אל הממונה להגנת הפרטיות, שיחקור את התלונה. אם הגיעה תלונה מרשם מאגרי המידע ,ישתף עמו הממונה על הגנת הפרטיות פעולה בחקירת התלונה. במידה שנגרם לנושא המידע נזק ,ישתף הממונה על הגנת הפרטיות מידע עם היועץ המשפטי במטרה לאפשר את פיצויו של נושא המידע באופן הוגן. במידה שהטיפול של הממונה על הגנת הפרטיות אינו משביע את רצונו של נושא המידע, זכאי נושא המידע לפנות בתלונה אל רשם מאגרי המידע.

פרק ט"ז – שינוי ועדכון

1. ראש אגף מחשוב ומערכות מידע יבחן מדי שנתיים את המדיניות שנקבעה, ויעדכנה במידת הצורך.
2. כל שינוי או עדכון של המדיניות יפורסם באתר האינטרנט של האוניברסיטה ויימסר לעובדים בהודעת אימייל או בפרסום בלוח המודעות הממוחשב.
3. במידה שחל שינוי מהותי במדיניות, תוצב גם הודעה במקום בולט באתר האינטרנט של האוניברסיטה.

פרק י"ז – אחריות

1. האחריות לביצוע נוהל זה חלה בראש וראשונה על המשתמש עצמו, הן סגל אקדמי והן סגל מנהלי.
2. מנהל היחידה, או כל אדם אחר שהוסמך על ידו, אחראי לגבי אנשי יחידתו, כולל עובדי קבלן המועסקים על-ידו.
3. ראש אגף מחשוב ומערכות מידע אחראי ליישום נוהל זה.
4. הממונה על אבטחת המידע .
5. הממונה על הגנת הפרטיות DPO.
6. נאמני אבטחת מידע באגף מחשוב ומערכות מידע ובפקולטות ויחידות האוניברסיטה.
7. ראש אגף מינהל תלמידים.
8. ראש אגף משאבי אנוש.

נספחים

1. נספח א'- לוח עדכונים

נספח א

לוח עדכונים

סידורי	מהות	תאריך

מסמך זה תקף ומבוקר רק בגרסתו במחשב, בתיקיית נהלי האוניברסיטה, בפורטל הארגוני