7/7/2019

מדיניות אבטחת מידע וסייבר

אוניברסיטת תל אביב

גירסה	תאריך	עורכים	תפקיד	הערות
2	28/07/2019	אורן בן שלום	CISO	אושר בוועד מנהל

תוכן עניינים

0. רקע

0.1. אוניברסיטת תל אביב (להלן – "האוניברסיטה") הינה מוסד מוכר להשכלה גבוהה, כמשמעותו בחוק המועצה להשכלה גבוהה, תשי"ח-1958, שמטרתה היא יצירת ידע, שימורו והנחלתו לטובת הציבור לדורותיו. לפיכך, האוניברסיטה אמונה על קיום ופיתוח ההוראה והמחקר בכל שטחי המדע והתרבות, תוך התבססות על עקרון החופש האקדמי. המידע הוא נכס חיוני לאוניברסיטה כארגון מונע ידע, שבו מידע קשור ללמידה והוראה, מחקר, קניין רוחני הנובע ממחקר, ייעוץ וניהול.

0.2. מערכות מידע ממוחשבות הן מרכיב מרכזי וחשוב בתשתית הארגונית באוניברסיטה אשר תומכות בפעילותה המחקרית והציבורית. מערכות המידע, הנתונים והמידע הממוחשב של האוניברסיטה מהווים נכס חיוני שיש להגן עליו מפני חשיפות ו/או נזקים העלולים לפגוע במטרות, ביעדים ובניהולה השוטף של האוניברסיטה או לפגוע בפרטיותם של נשואי המידע.

0.3. במדיניות זאת: מידע – הוא כל נתון הנוגע ו/או קשור לפעילותה הארגונית של האוניברסיטה ונמצא על גבי מצעים פיזיים ודיגיטליים לא כולל מידע מחקרי שאינו מידע המזהה או יכול לזהות אדם; מידע רגיש – הוא מידע השייך לאוניברסיטה אשר חשיפתו או פגיעה בו עלולים לגרום נזק לפעילותה השוטפת של האוניברסיטה.

0.4. אבטחת המידע והגנת סייבר הם מכלול הפעולות והאמצעים שיש לנקוט וליישם במטרה להגן על המידע מפני חדירה, דליפה, פגיעה, הרס, חשיפה ו/או שינוי מידע לא מאושר במזיד או בשוגג. פעולות אבטחת המידע והגנת הסייבר נועדו להבטיח את סודיות, שלמות, אמינות וזמינות המידע, לרבות - שמירה על חסיון המידע של עובדי האוניברסיטה, תלמידיה וספקיה ושל כל אדם אחר שהמידע אודותיו מצוי במערכות מידע של האוניברסיטה, מזעור סיכונים תפעוליים, מניעת נזקים כספיים ונזקי מוניטין, עמידה בדרישות הדין ואבטחת רצף פעילות האוניברסיטה, וזאת תוך שמירה על עקרונות החופש האקדמי וחירות המחקר.

1. מטרה

1.1. מטרת המסמך היא קביעת מדיניות לאבטחת מערכות המידע והמידע הממוחשב של האוניברסיטה, הגדרת יעדי האבטחה, תהליכים ניהוליים, אמצעים למימוש, עקרונות בסיסיים ליישום האבטחה, ומתן הכוונה ותמיכה בנושא אבטחת מידע והגנת סייבר.

1.2. להלן הנושאים העיקריים המפורטים במדיניות זו:

1.2.1. הצגת תפיסת האוניברסיטה ומחויבותה לנושא אבטחת המידע והגנת הסייבר.

1.2.2. קביעת עקרונות מנחים ליישום אבטחת המידע באוניברסיטה ולהעלאת מודעות של כל הגורמים באוניברסיטה לנושאי אבטחת המידע והגנת הסייבר.

1.2.3. קביעת תפקידים, סמכויות, אחראיות, מסגרת תהליכית וארגונית, והקצאת משאבים עבור פעילות אבטחת מידע והגנת הסייבר באוניברסיטה.

2. תחום

המדיניות מחייבת את כלל קהילת האוניברסיטה, לרבות אנשי הסגל האקדמי והסגל המנהלי, תלמידים, וספקי שירות חיצוניים, לרבות קבלנים, קבלני משנה וספקי מיקור חוץ. המדיניות חלה על כלל המערכות הממוחשבות המשמשות את האוניברסיטה, לרבות שרתים, מסדי נתונים וכל אמצעי מחשוב ותקשורת אחר שבניהול האוניברסיטה, בבעלותה ו/או בשליטתה.

3. הצהרת הנהלה לאבטחת מידע והגנת הסייבר

3.1. עקרונות המדיניות הקבועים במסמך זה גובשו על ידי ממונה אבטחת מידע והגנת הסייבר באוניברסיטה ואושרו על ידי ההנהלה.

3.2. בכל מקרה של שינוי בכללי המדיניות או שינוי שאינו זניח בסביבה הטכנולוגית יש לבצע אישור נוסף למסמך המדיניות.

3.3. מסמך המדיניות יועבר לוועדת ההיגוי להגנת הפרטיות והסייבר לצורך עיון, ואחת לשנה יעבור תהליך בחינה מחדש לצורך דיון וריענון.

3.4. לאחר אישור ועדכון המדיניות יש ליידע את כלל הגורמים הרלוונטיים (הנהלה, עובדים, ספקים וכו') על השינויים שבוצעו.

4. יעדי אבטחת המידע

אבטחת המידע והגנת הסייבר היא גורם הכרחי להגנה על מידע אישי שבידי האוניברסיטה, למזעור הסיכונים התפעוליים, להפחתת נזקים כספיים ונזקי מוניטין, לבקרה על שיתוף בנתוני מחקר ולעמידה בדרישות הדין והרגולציה, ובין היתר:

4.1. חוק הגנת הפרטיות, התשמ"א-1981, התקנות לפיו (ובפרט, תקנות הגנת הפרטיות (אבטחת מידע) התשע"ז-2017) והוראות הרשות להגנת הפרטיות;

4.2. חוק המחשבים, תשנ"ה-1995;

4.3. חוק התקשורת (בזק ושידורים), התשמ"ב-1982;

4.4. חוק זכויות החולה, התשנ"ו-1966;

4.5. התקנות הכלליות להגנת מידע אישי של האיחוד האירופי (General Data Protection Regulation - GDPR).

5. עקרונות מדיניות אבטחת מידע והגנת הסייבר

5.1. איסוף מידע, אחסונו, משך תקופת ההגנה עליו ואופן השימוש בו יעשו בכפוף לדרישות הדין והרגולציה החלות על האוניברסיטה.

5.2. רמת ההגנה על המידע האגור במערכות המחשוב של האוניברסיטה תיקבע על פי אופיו של אותו מידע סיווגו, והסיכון הנגזר ממנו.

5.3. הגנה על מאגרי מידע כנדרש בחוק, בהתאם למפורט במדיניות הגנת הפרטיות ועפ"י הוראות הממונה על הפרטיות.

5.4. האוניברסיטה תיישם אמצעים, שיטות ונהלים סבירים ומקובלים לשמירת זמינות המידע והגנתו מפני הרס, פגיעה ו/או שינוי לא מוסמך, ולצמצום סיכוני אבטחת מידע וסייבר והכל כמתחייב מהוראות כל דין.

5.5. בכפוף למחויבותה של האוניברסיטה לחופש אקדמי, לעקרונות של מידע פתוח ולהוראות כל דין, הגישה למידע תהיה מורשית רק לגורמים אנושיים וממוחשבים במידה הנדרשת לביצוע תפקידם אשר הורשו לכך במפורש על-ידי מנהלי מאגרי מידע כהגדרתם בחוק. מנהלי מאגרי מידע, חוקרים ומנהלי יחידות ינהלו את הגישה למידע אשר בחזקתם כמפורט בנוהל הרשאות גישה של האוניברסיטה.

5.6. אבטחת מידע והגנת הסייבר תיושם על-פי עקרון ההגנה בשכבות (DiD) – כל הגנה בשכבה תהיה בלתי תלויה בהגנה של שכבה אחרת. כך, ייושמו מספר הגנות אבטחת מידע וסייבר בעלות יכולות שונות ומגוונות לאבטחת שכבות התקשורת/מערכות הפעלה/אפליקציות וכו׳.

6. תחומי אבטחת מידע והגנת הסייבר

6.1. האמצעים ליישום מדיניות אבטחת מידע והגנת הסייבר באוניברסיטה כוללים הגדרת תפקידים, סמכויות, תחומי אחריות, אכיפת נהלים והנחיות לשימוש בכלים טכנולוגיים, הטמעה ויישום אבטחת מידע והגנת הסייבר בהיערכות למצבי חירום.

6.2. אבטחת מידע והגנת הסייבר כוללת:

6.2.1. אבטחת מידע פרטי, אישי ו/או רגיש אודות עובדי האוניברסיטה, מידע אישי או רגיש במחקרים, מידע אקדמי, ספקים, מבקרים ותלמידים, באחסנה, בתעבורה או בשימוש.

6.2.2. אבטחה פיזית של ציוד מחשוב, תקשורת, כבלים וכל אמצעי אחסון של מידע, אבטחת כניסות ויציאות למתחמים בהם נמצאות מערכות המחשוב ואמצעי התקשורת.

6.2.3. אבטחת עמדות קצה, תחנות עבודה, מחשבים ניידים, ציוד תקשורת וכל ציוד אחר, לרבות אמצעי הפלט לסוגיו (נייר, מגנטי ואופטי), הנושא מידע בצורה דיגיטלית.

6.2.4. אבטחה לוגית של תוכנות, תהליכים, אפליקציות, מסדי נתונים, שרתים, תעבורת תקשורת ומאגרי מידע.

6.2.5. בקרת גישה של משתמשים ו/או גורמים חיצוניים למערכות מידע ומאגרי מידע.

6.2.6. בקרה על העברת מידע לגורמים חיצוניים.

6.2.7. אבטחת מידע בניהול כוח אדם.

7. סמכויות, אחריות וניהול אבטחת מידע והגנת סייבר באוניברסיטה

7.1. הנהלת האוניברסיטה

הנהלת האוניברסיטה מחויבת לקדם את מטרות האוניברסיטה על ידי הגנה יעילה על נכסי המידע, הבטחת שלמות ואמינות המידע, שמירה על זמינות מערכות המידע, יישום בקרות אבטחה בכפוף לרגולציה ובהתאם לסיכונים, שמירה על מוניטין האוניברסיטה על-ידי קיום עקרונות הסודיות, שלמות, אמינות וזמינות מאגרי המידע הנמצאים ברשותה. הקצאת משאבים להקמת מערכות אבטחה ובקרה לצורך הפעלתן בתדירות קבועה, תחזוקתן ושיפורן המתמיד. הנהלת האוניברסיטה תמנה ועדת משנה קבועה אשר תפעל כוועדת היגוי לאבטחת מידע והגנת הסייבר (להלן – **"ועדת היגוי"** או **"הוועדה"**).

7.2. ועדת ההיגוי

הוועדה תהווה מסגרת ניהולית עליונה מטעם הנהלת האוניברסיטה לתאום וקבלת החלטות בנושאי אבטחת מידע והגנת הסייבר באוניברסיטה. הוועדה אחראית בין השאר על תחזוקה ועדכון של מסמך מדיניות זה, החלטותיה והנחיותיה, לכל הפחות אחת לשנה. הוועדה תתכנס לכל הפחות אחת לרבעון, על-פי קביעת יו״ר הוועדה. הרכב הוועדה יהיה כדלקמן: מנכ״ל האוניברסיטה – יו״ר, מנהל הגנת הפרטיות (DPO), סמנכ״ל מחשוב וטכנולוגיות מידע, סמנכ״ל כספים, מנהלת ראשות מחקר, שני נציגים מהסגל האקדמי הבכיר שהנם חוקרים פעילים התחומים המעורבים עם מאגרי מידע, יועץ משפטי וממונה אבטחת המידע וסייבר (CISO). במידת הצורך ובהתאם לנושאים המתוכננים לדיון במסגרת הוועדה, הוועדה תזמן ותעסיק גורמים רלוונטיים נוספים, לרבות מומחים ויועצים חיצוניים.

האוניברסיטה מחויבת להגנת הפרטיות הן מכוחם של חוקים ותקנות, ובעיקר ממחויבותה לערכים ולזכויות אדם. יכולתה של האוניברסיטה להבטיח הגנת הפרטיות נובעת גם מקיומם של מנגנוני אבטחת מידע וסייבר. כדי להבטיח התמודדות נאותה עם הצורך באבטחת מידע וסייבר ובהגנת הפרטיות, תוך שימור וכיבוד החופש האקדמי ועקרון פתיחות המחקר, הוחלט שוועדת ההיגוי תהיה משותפת לשני הנושאים.

אחריות ומשימות ועדת ההיגוי:

7.2.1. פיקוח ומעקב אחר שמירת מדיניות אבטחת המידע והגנת הסייבר.

7.2.2. אישור תכנית העבודה ליישום ההוראות אבטחת מידע והסייבר, נהלים והנחיות אבטחת מידע כלל אוניברסיטאיים ומעקב אחר ביצועה.

7.2.3. הוועדה תקיים דיון בתכנית העבודה השנתית בנושאי אבטחת מידע והגנת הסייבר ותאשרה כתכנית מקובלת ליישום, לרבות הקצאת משאבים נדרשים.

7.2.4. קבלת הערכות הסיכונים מממונה אבטחת מידע וסייבר והמלצתם להתמודדות עם הסיכונים אלה.

7.2.5. הוועדה תדון באירועי סייבר משמעותיים ובאירועי אבטחת מידע, ובהמלצות הגורמים המקצועיים להתמודדות עם אירועים אלה. הוועדה תחליט בדבר יישום ההמלצות למניעת התרחשות אירועים אלה בעתיד.

7.2.6. הוועדה תדון בהמלצות גורם מקצועי לסיווג המידע על-פי סעיף 10 במסמך זה ותאשר את ביצוע תיוג מידע זה בהתאם לרמת הסיווג.

7.2.7. קבלת דיווחים ומעקב אחר ביצוע פעילות אבטחת המידע והגנת הסייבר.

7.3. ממונה אבטחת מידע והגנת הסייבר

ממונה אבטחת מידע והגנת הסייבר יפעל בכפוף לסמנכ"ל מחשוב וטכנולוגיות מידע ויישא באחריות ביצוע של כלל נושאי אבטחת מידע והגנת הסייבר באוניברסיטה, במידת הצורך יוכל לפנות לקבלת עזרה מגורמים מקצועיים חיצוניים שונים (יועצים ומומחים כפי שיידרש).

עיקרי תפקידיו ומשימותיו של ממונה אבטחת מידע והגנת הסייבר:

7.3.1. הכנה ויישום תכנית עבודה שנתית ורב שנתית ליישום דרישות אבטחת המידע והגנת הסייבר, בהתאם לדין והרגולציה.

7.3.2. הכנה ויישום תכנית שנתית להדרכת העובדים באוניברסיטה, הסגל והמנהלה, ולהעלאת המודעות בנושאי אבטחת מידע, והגנת הסייבר.

7.3.3. הגדרת הדרישות בכלל מערכות ומרכבי המידע באוניברסיטה, ומערכותיה הממוחשבות.

7.3.4. הצעת אסטרטגיה ומסגרת ממשל תאגידי להתמודדות עם אבטחת מידע והגנת סייבר כחלק מתפיסת האוניברסיטה.

7.3.5. הכנה ויישום נהלי אבטחת מידע והגנת הסייבר, ושילוב סטנדרטים, הוראות והנחיות אבטחת מידע בנהלי האוניברסיטה.

7.3.6. פיקוח ובקרה על יישום מדיניות ונהלי אבטחת מידע, ובחינת אפקטיביות מערך אבטחת המידע והגנת הסייבר.

7.3.7. ביצוע הערכה שוטפת של סיכוני אבטחת מידע והגנת הסייבר וייזום סקרי סיכונים, מבדקי חוסן, מבדקי חדירות, סקרי סייבר, לכל הפחות אחת ל-18 חודשים אשר ישקפו סיכונים עדכניים למערכות המידע והמחשוב של האוניברסיטה.

7.3.8. טיפול שוטף באישורי העברת מידע לגורמי חוץ או קבלת מידע מהם.

7.3.9. טיפול באירועים חריגים בתחום אבטחת מידע והגנת הסייבר.

7.3.10. הנחיית נאמני אבטחת מידע בפעילות האוניברסיטאית בנושא אבטחת מידע והגנת סייבר.

7.3.11. ביקורת אבטחת מידע בכל סביבות העבודה.

7.3.12. הכנת מסמכי עבודה, חוות דעת ומסמכי מטה אחרים בנושאי אבטחת מידע והגנת הסייבר.

7.3.13. שילוב מערכות אבטחה, אמצעים טכנולוגיים ותהליכים לטובת אבטחת מערכות האוניברסיטה.

7.3.14. ביצוע כל מטלה אחרת המוטלת על הממונה על אבטחת מידע בהתאם להוראות כל דין.

7.3.15. ממונה אבטחת מידע והגנת הסייבר יציג בפני הוועדה לכל הפחות אחת לחציון, את הנושאים הבאים:

7.3.15.1. סטאטוס התקדמות תכנית העבודה השנתית של אבטחת מידע והגנת הסייבר בהתאם ליעדים שנקבעו.

7.3.15.2. לקויים ברמת סיכון גבוהה שהתגלו במהלך סקרי סיכונים ומבדקי חוסן, אשר טופלו במהלך שישה חודשים, ובכלל זה בתוך כמה זמן טופלו מחשיפתם, וכן ליקויים שלא טופלו.

7.3.15.3. חשיפות מהותיות אם קיימות ואופן הטיפול בהן.

7.3.15.4. אירועי אבטחת מידע וסייבר, דוחות האירועים, תיעוד מסקנות ולקחים שהופקו מאירועים אלה בתקופה המדווחת.

7.4. נאמן אבטחת מידע

7.4.1. נאמן אבטחת מידע – הוא ראש צוות מתאמי מחשוב אשר אחראיים על נושאי מחשוב בפקולטות, יחידות ובתי הספר באוניברסיטה או מי מטעמו אחראי לנושא אבטחת מידע ומשמש כנציגות אבטחת המידע במקום.

7.4.2. תפקידו של הנאמן הוא הטמעה ואכיפת נהלי אבטחת המידע ביחידה, בהנחיה מקצועית של ממונה אבטחת מידע והגנת הסייבר הארגוני, העלאת המודעות לאבטחת מידע בפקולטה או ביחידה בה הוא נמצא.

7.4.3. נאמני אבטחת מידע יעברו הכשרה מתאימה בנושא אבטחת מידע והגנת הסייבר.

7.5. אחריות קהילת האוניברסיטה

7.5.1. כל עובד אוניברסיטה מחויב לנושא אבטחת המידע והגנת הסייבר כחלק בלתי נפרד מאחריותו המקצועית מכורח תפקידו.

7.5.2. בעלי תפקידים יקפידו על יישום ואכיפת נהלי אבטחת המידע, עידוד מודעות העובדים בנושא והבעת תמיכה בפעילות נאמני אבטחת המידע.

7.5.3. האוניברסיטה דורשת מכל אחד מעובדיה , ספקיה, קבלנים וספקי השירות (קבועים או מזדמנים) מחויבות לנושאי אבטחת המידע, אחריות אישית ליישום כללי המדיניות בתחומי תפקידם, ודיווח מיידי על גורמי סיכון ואירועים המתרחשים בהיבט אבטחת המידע והגנת הסייבר.

7.5.4. כל עובד וספק הנותן שירות חיצוני באוניברסיטה יחתמו על טופס התחייבות לשמירת סודיות וקיום הוראות אבטחת המידע.

7.5.5. מחויבות בעלי תפקידים תכלול בין היתר את אלה:

7.5.5.1. שימוש אישי בלבד בחשבון המשתמש שלו במחשב.

7.5.5.2. שימוש במידע הארגוני רק לצורך מילוי תפקידו.

7.5.5.3. שמירה על חיסיון אמצעי הזיהוי המשמשים לצורך גישה למערכות האוניברסיטה.

7.5.5.4. דיווח על חריגות אבטחה.

7.5.5.5. שמירה מאובטחת של מסמכים ורשומות.

7.5.5.6. אבטחת סביבת העבודה.

8. הערכת סיכוני אבטחת מידע והגנת הסייבר

8.1. האוניברסיטה תקיים תהליך הערכת סיכוני אבטחת מידע וסייבר במערכות המידע, מערכות התקשורת והממשקים הכולל בתוכו זיהוי, מזעור או מניעה של סיכוני האבטחה העלולים להשפיע על המידע.

8.2. תהליך זה יתבסס על סיווג נכסי מידע, איומי אבטחת המידע ואופי העבודה במערכות האוניברסיטה השונות.

8.3. תוצר הערכת הסיכונים ינחה את הנהלת האוניברסיטה בהפניית משאבים נאותים להטמעת אמצעי אבטחה, בקרות ומיקוד סקרי סיכוני האבטחה במערכות האוניברסיטה השונות ויספק מדרג רגישות של מערכות השונות באוניברסיטה, המתבסס בין היתר על סיווג המידע.

8.4. ממונה אבטחת מידע והגנת הסייבר יבצע הערכת סיכונים כל 18 חודשים ובעת שינוי מהותי כמפורט.

9. נהלי אבטחת מידע

9.1. פעילות אבטחת המידע והגנת הסייבר באוניברסיטה תהא מושתת על מערכת נהלי אבטחת ומערכות המידע שיאושרו על-ידי וועדת היגוי.

9.2. נהלי אבטחת המידע ותהליכי העבודה הם נגזרת של מדיניות אבטחת מידע והגנת הסייבר המפרטת את תפיסת ההנהלה לגבי אבטחת המידע והגנת הסייבר באוניברסיטה והעקרונות המנחים ליישומה.

9.3. לכל תהליך באוניברסיטה המטפל בניהול, הכנסה, תפעול, תחזוקה, גיבוי, העברה והוצאה של מידע ייכתב נוהל אבטחת מידע מפורט.

9.4. הנהלים יופצו לכלל העובדים או המשתמשים הרלוונטיים ויעברו תהליך בדיקה ועדכון בהתאם לצורך, עם שינוי משמעותי בסביבה הטכנולוגית או לאחר אירוע אבטחת מידע, ולכל הפחות אחת לשנתיים.

10. סיווג מידע

לאוניברסיטה, בהיותה מוסד אקדמי המבוסס על עקרון החופש האקדמי, מחויבות לאפשר לחוקריה ,ואף לעודדם, לשתף פעולה עם עמיתים בארץ ובעולם ולפרסם את תוצאות מחקריהם בפרסומים ובכנסים מדעיים. עם זאת, על מנת למנוע העברת מידע בצורה שאינה מבוקרת ולהבטיח בקרה נאותה, ממונה אבטחת מידע והגנת הסייבר יסייע לבעלי המידע לקבוע את רמת סיווג המידע שנמצא באחריותם לפי ארבעה קריטריונים:

10.1. מידע אקדמי – מידע הקשור למחקר אקדמי באופן ישיר המנוהל ע"י חברי סגל אקדמי בכיר (PI). שיקול הדעת לגבי התנאים לשיתוף מידע כזה הינו של ה PI, בכפוף לנהלי האוניברסיטה הרלבנטיים (נהלי קניין רוחני, פרטיות וכד').

10.2. מידע ציבורי – מידע שאינו אקדמי שאין בחשיפתו כדי לגרום נזק לאוניברסיטה, לעובדיה ולבעלי העניין בו, כגון מסמכים כלליים, הפתוחים לידיעת הציבור. מסמכים אלה עשויים להיות חשופים

ו/או מועברים לאנשים מחוץ לשטחי האוניברסיטה. על מידע מסוג זה אין הגבלות חוקיות, רגולטוריות ו/או אחרות.

10.3. מידע פנימי/קנייני – מידע פנימי של האוניברסיטה, אשר מיועד לשימוש פנימי בלבד, על מידע זה חלות הגבלות מפני חשיפתו לגורמים חיצוניים. גילויו לגורמים חיצוניים ילווה באישור ההנהלה. פגיעה בסודיותו של מידע זה עלול לגרום נזק מהיבטים כספים, תדמיתיים ו/או משפטים.

10.4. מידע חסוי/ רגיש/ פרטי – מידע רגיש ובעל ערך רב, הן קנייני והן אישי. אין לחשוף מחוץ לאוניברסיטה ללא אישור מפורש של הנהלת האוניברסיטה. מידע מסווג מהיבטי צנעת הפרט לפי חוק הגנת הפרטיות התשמ"א 1981, הקובע בצורה מרחיבה כי כל שימוש ו/או פרסום של ענייניו הפרטיים של אדם מהווה פגיעה בפרטיותו. כגון: פרטים על מצב נפשי, פרטים רפואיים רגישים, פרטי כרטיס אשראי וכדומה.

כברירת המחדל כל מידע מינהלי יסווג כפנימי, אלא אם כן נקבע אחרת. מערכות תומכות בהם קיים מידע יסווגו לפי מידת הנזק העלול להיגרם למידע כתוצאה מהרס, פגיעה בזמינותו, שינוי בלתי מוסמך או חשיפתו.

11. יישום אבטחת מידע והגנת הסייבר

11.1. יישום בקרות אבטחת מידע יתבצע על פי נהלי אוניברסיטה (נספח א') בהתאם לניהול סיכוני אבטחה וסייבר באחריות אגף המחשוב ובפיקוח ממונה אבטחת המידע והגנת הסייבר.

11.2. נהלי אבטחת המידע וסייבר יכללו לכל הפחות את כל הנושאים הבאים:

11.2.1. אבטחה פיזית ובטיחות

11.2.2. אבטחת מצעים נושאי מידע ועמדות העבודה

11.2.3. אבטחה לוגית וייושמית

11.2.4. אבטחת שרתים ומערכות הפעלה

11.2.5. אבטחת תשתיות תקשורת

11.2.6. אבטחת מידע בשינוי ופיתוח מערכות מידע ותשתיות מחשוב

11.2.7. הצפנה

11.2.8. הגנה מפני פוגענים, נוזקות וקוד זדוני/עוין

11.2.9. זיהוי משתמשים והרשאות גישה כולל הרשאות-על (גבוהות)

11.2.10. העברת מידע לגורמים חיצוניים

11.2.11. דואר אלקטרוני ואינטרנט

11.2.12. שימוש באמצעי מחשוב ניידים ומדיה נתיקה

11.2.13. בקרת גישה מרחוק

12. בקרה ומעקב

באחריות ממונה אבטחת המידע והגנת הסייבר לבקר את הפעילויות הממוחשבות המתבצעות באוניברסיטה, בכדי לוודא שהמידע מנוהל באופן המבטיח את שלמות, אמינות, חיסיון וזמינות המידע והשימוש המבוקר בו.

13. איתור וטיפול באירועים חריגים

ממונה אבטחת המידע והגנת הסייבר יפיק דוחות בקרה מהמערכות השונות, המציינים ניסיונות כושלים ומוצלחים בעת הכניסה לכל מערכת ו/או הפעלה חריגה של פעילויות נוספות היכולות להצביע על בעיית

אבטחה. ממונה אבטחת מידע והגנת הסייבר יבחן את הדוחות ויקבע האם היו אירועים חריגים וידווח למנהל הרלוונטי וליו"ר ועדת היגוי ברגע גילוי אירוע חמור. ממונה אבטחת מידע והגנת הסייבר יגבש נוהל "תגובה לאירועי אבטחת מידע והגנת הסייבר" בו יפרט אופן התמודדות עמם.

14. חובת דיווח

חובתו של כל משתמש לדווח לממונה אבטחת מידע והגנת הסייבר על כל ניסיון או שימוש בזיהוי המשתמש שלו, שלא על ידיו ועל כל חשש לפגיעה באבטחת מידע. אירוע חמור ידווח לגורמים רלוונטיים מחוץ לאוניברסיטה על פי הוראות הדין.

15. המשכיות עסקית

על יחידות האוניברסיטה לקבוע נהלים ומדיניות לגיבוי ושחזור נתוני היחידות על מנת להבטיח כי תהליכי גיבוי ויכולות שחזור תומכים בתהליך ההמשכיות העסקית והתאוששות מאסון כפי שנקבע במדיניות ה-BCP של האוניברסיטה.

16. עדכון המדיניות

16.1. מדיניות אבטחת המידע תסקר לכל הפחות אחת לשנה על-ידי ממונה אבטחת המידע והגנת הסייבר, כדי להבטיח שמירה, תיקוף, עדכניות, והתאמות נאותות ואפקטיביות של המדיניות.

16.2. השינויים יובאו לאישור הוועדה ויועברו לאישור ההנהלה/ועד מנהל.

16.3. עדכונים טכניים במדיניות יובאו לידיעת ההנהלה בדיעבד ללא חובת אישורם.

17. נספח א' – רשימת נהלי אבטחת המידע וסייבר

17.1. נוהל מחזור חיים של הרשאות המשתמש

17.2. נוהל מחזור חיים של מידע

17.3. נוהל פיתוח מאובטח

17.4. נוהל ניהול סיכונים

17.5. נוהל תגובה ודיווח על אירועי אבטחת מידע וסייבר

17.6. נוהל אבטחה וטיפול במאגרי מידע

17.7. נוהל התקשרות עם ספקי שירות / מיקור חוץ

17.8. נוהל הקשחת מערכות

17.9. נוהל אבטחת רשת ותקשורת