



## הנחיות אבטחת מידע לעובדי אוניברסיטת בר – אילן

עדכון 05-2023

### 1. אחריות אישית

- 1.1. במהלך עבודתכם יתכן שתיחשפו למידע מסוגים שונים, לרבות מידע סודי של האוניברסיטה ומידע רגיש אודות עובדים אחרים / סטודנטים / ספקים וכיו"ב.
- 1.2. עליכם להפעיל שיקול דעת לפני כל פעולה במחשב העלולה לגרום נזק. זכרו, אם יש ספק – אין ספק! עדיף להתייעץ מראש ולשאול טרם ביצוע הפעולה.
- 1.3. טלפון חכם (Smart Phone), הינו מחשב לכל דבר ועניין ולכן יש לנהוג בו בזהירות כפי שנוהגים במחשב.
- 1.4. אין ללחוץ על קישורים המגיעים בהודעות דוא"ל או בקבצים מצורפים לדוא"ל המבקשים לבצע פעילות כלשהי לאיפוס סיסמה, או הזדהות אחרת. גם אם בטעות לחצתם על קישורים כאלה, אין למסור מידע אישי כלשהו ו/או לאשר החלפת סיסמה. החלפת סיסמה אישית למערכות האוניברסיטה תיעשה כאמור בסעיף 5 להלן.
- 1.5. אין לאפשר לאף גורם מחוץ לאוניברסיטה להתחבר למחשב/ים של האוניברסיטה בתוכנת השתלטות.
- 1.6. יש להיזהר מהודעות או חלונות קופצים (Pop Ups), ולא ללחוץ על קישורים בהודעות מסוג זה.

### 2. שמירת סודיות

- 2.1. "מידע סודי" – מידע, שאינו פומבי, הנוגע לאוניברסיטה ו/או לאחרים הקשורים עמה - בהם תלמידים, עובדים, נותני שירותים, פונים ומקבלי שירותים ועוד - שחלקו כולל פרטים מקצועיים/ניהוליים/כלכליים/מסחריים ו/או פרטים אישיים, רגישים ו/או סודיים .
- 2.2. כל העובדים נדרשים לשמור בסודיות מידע סודי אליו הם נחשפים במהלך עבודתם, ולא לעשות בו שימוש אלא ככל שמתחייב לצורך ביצוע תפקידם ובמסגרת ההרשאות והנהלים שקבעה האוניברסיטה.
- 2.3. במעמד קליטתכם כעובדים, עליכם לקרוא ולחתום על טופס התחייבות לשמירת סודיות ולשימוש ראוי במידע.

### 3. הוצאת מידע מהארגון

- 3.1. ככלל, אין להוציא מסמכים משרדי האוניברסיטה.
- 3.2. כאשר יש צורך להוציא מסמכים לצרכי עבודה משרדי האוניברסיטה, לרבות עבודה מהבית, יש לפנות למנהל הישיר להסדרת אמצעי אבטחת המידע.
- 3.3. העברת מידע סודי באמצעות מדיה פיזית (כגון דיסק נייד או DISK ON KEY) תחייב הצפנת הקובץ עם סיסמה או כלל הרכיב.
- 3.4. אם אבד מידע (למשל-מסמכים), עליכם להודיע על כך מיידית למנהל הישיר ולמנהל אבטחת המידע של האוניברסיטה או ליועץ המחשוב, בהתאם לכללי הדיווח (ראו סעיף



#### **4. התקנה והסרת תוכנות**

- 4.1. אין לחבר באופן פיסית מחשב שאינו מחשב האוניברסיטה לרשת המחשבים של האוניברסיטה ואין לבצע כל שינוי בעמדת העבודה באורח עצמאי, כולל התקנת תוכנות.
- 4.2. בכל מקרה בו גיליתם תוכנה שמקורה אינו ברור, עליכם לפנות ליועץ המחשוב.
- 4.3. תוכנת אנטי וירוס
  - 4.3.1. בתחנת העבודה מותקנת תוכנת אנטי וירוס, חל איסור להסיר את התוכנה.
  - 4.3.2. היה והתוכנה מצאה קבצים נגועים בתחנה, או שהתקבלה הודעה על אי-פעילות של התוכנה מסיבה כלשהי, על עובד לפנות ליועץ המחשוב.

#### **5. שם משתמש וסיסמה**

- 5.1. כל עובד מקבל מאגף התקשוב שם משתמש ייחודי (Username) וסיסמה ראשונית למערכות השונות **לשימוש האישי והבלעדי** ולצורך מילוי תפקידו באוניברסיטה.
- 5.2. הסיסמה מהווה מפתח גישה למידע סודי ולמערכות הממוחשבות, ולכן הינה אישית וסודית.
- 5.3. עליכם להימנע משמירת הסיסמה במקום בו היא עלולה להיחשף (תיקיות ציבוריות, הדבקת פתק באזור העבודה וכו').
- 5.4. חל איסור למסור את פרטי הזיהוי האישיים והסיסמה לכל גורם אחר כגון- עובדי האוניברסיטה, מנהל, בעל תפקיד וגורם חיצוני.
- 5.5. חל איסור לעשות שימוש בפרטי הזיהוי האישיים של עובד אחר באוניברסיטה (בכל תפקיד), גם אם לצרכי עבודה. ככל שעובד סבור שנדרשת לו הרשאה אחרת למילוי תפקידו, עליו לפנות למנהלו הישיר.
- 5.6. בכל מקרה של חשיפת הסיסמה שלכם או של עובד אחר באוניברסיטה או אם עלה חשד לחשיפתה, יש להחליף אותה מיידית ולדווח למנהל אבטחת המידע על המקרה. החלפת הסיסמה תבוצע באמצעות פורטל החלפת הסיסמאות בכתובת: <https://sspr.biu.ac.il/sspr/public/forgottenpassword>
- 5.7. ניתן לצפות במדיניות הסיסמאות של האוניברסיטה בכתובת: <https://sspr.biu.ac.il/sspr/public/forgottenpassword>

#### **6. עזיבת עמדת העבודה**

- 6.1. בעת עזיבת עמדת העבודה יש לנעול באופן יזום את עמדת העבודה וכן לנעול את דלתות המשרד.
- 6.2. בנוסף, בתום יום העבודה יש לקיים מדיניות "שולחן נקי" באמצעות הקפדה על הפעולות הבאות:
  - 6.2.1. נעילת מסמכים סודיים ורגישים במקום מוגן.
  - 6.2.2. השמדת מסמכים סודיים ורגישים שאין בהם עוד צורך באמצעות גריסה.
  - 6.2.3. לוודא כי לא נשאר חומר סודי או רגיש במדפסות, פקס או מכונת הצילום.
- 6.3. שמירת קבצים באופן מקומי על עמדת העבודה עשויה לגרום לאובדן המידע שכן מידע זה אינו מגובה ויאבד עם כל תקלה במחשב. יש לבצע שמירה של המידע על כונני הרשת בלבד.



## **7. שימוש באינטרנט**

- 7.1. חל איסור מוחלט על גלישה לאתרים הבאים: אתרים פורנוגרפיים, אתרי הימורים, חדרי שיחה פרטיים (צ'טים), אתרי שיתוף קבצים, אתרים המאפשרים הורדת תוכנות בלתי חוקיות, אתרים הנוגעים במידע הקשור לפריצה למערכות מחשב, ובכלל אתרים בעלי תוכן בלתי נאות וזאת מחשש להידבקות בוירוסים, לחשיפת האוניברסיטה לתביעות משפטיות, לפגיעה בשמה הטוב של האוניברסיטה ועוד.
- 7.2. אין להעביר מידע סודי באמצעות תוכנות מסרים (כדוגמת ווטסאפ).
- 7.3. עובד המזהה אירוע חריג במחשבו כגון: השתלטות עוינת על המחשב, חדירת וירוס, חלונות קופצים של דפדפן, פתיחת אתרים אוטומטית וכו' ידווח מיידית ליועץ המחשוב או למנהל אבטחת מידע, כמפורט בסעיף 11 להלן.
- 7.4. חל איסור מוחלט להשתמש בשם האוניברסיטה, בעת רישום לאתרים או מוקדי מידע באינטרנט (כגון פייסבוק, קבוצות דיון, חדרי צ'טים, רשימות דיוור וכיו"ב) אלא אם הדבר מתבצע במסגרת התפקיד ולצרכי האוניברסיטה.
- 7.5. חל איסור להוציא קבצים המכילים מידע סודי מרשת האוניברסיטה, להעלותם לאתר כלשהו או להעבירם לגורם כלשהו באמצעות האינטרנט, אלא אם כן הדבר נעשה באתר שהוגדר לצרכי עבודה. כל צורך אחר בהעברת קבצים באמצעות האינטרנט יבחן על ידי מנהל אבטחת המידע באוניברסיטה, ויאושר או ידחה בהתאם להחלטתו.

## **8. שימוש בציוד של האוניברסיטה**

- 8.1. השימוש במחשבי האוניברסיטה ייעשה בכפוף לנהלי האוניברסיטה.
- 8.2. האוניברסיטה מנהלת מנגנון תיעוד אוטומטי שמאפשר ביקורת על הגישה למחשבים ולמערכות מאגרי המידע של האוניברסיטה לצורך ניהול מערך המחשוב, שמירת המידע ואבטחת המידע. המנגנון רושם בלוגים, בין היתר, את הפעולות הבאות: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה.
- 8.3. מידע פרטי שישמר במחשבי האוניברסיטה עשוי להיות מנוטר אף הוא. על כן, הנך מתבקש לשמור מידע פרטי בכוננים המיועדים לכך.
- 8.4. אם עולה בליבך חשד כי נעשה שימוש לא מורשה במחשבך האישי (עמדת עבודה), דווח מיידית ליועץ המחשוב.

## **9. גישה מרחוק ועבודה מהבית**

- 9.1. עובדים הנדרשים במסגרת תפקידם לעבודה מרחוק/מהבית, יקבלו אישור לכך מהממונה עליהם.
- 9.2. עובדים המורשים לכך, יוכלו להתחבר לרשת ומערכות האוניברסיטה באמצעות VPN מאובטח בלבד שהותקן ואושר על ידי אגף התקשוב.
- 9.3. עובדים המתחברים ממחשבם הביתי אל רשת האוניברסיטה יעמדו גם בכללים הבאים:
  - 9.3.1. עבודה עם מחשב בעל מערכת הפעלה עדכנית ונתמכת, המקבלת עדכוני אבטחה באופן שוטף.
  - 9.3.2. התקנת תכנת אנטי וירוס המתעדכנת באופן שוטף.

- 9.3.3 מומלץ להפעיל במחשב הפרטי את רכיב חומת האש (Fire-Wall).
- 9.3.4 עבור שלושת הסעיפים הקודמים, 9.3.1-2-3, ההמלצה היא לעבוד עם מערכת הפעלה Windows 10 ומעלה הכוללת בתוכה אנטיווירוס חינומי כולל רכיב חומת אש והגנות נוספות. הפעלת המחשב עם ברירות המחדל של המערכת עבור עדכונים שוטפים מבטיחה הגנה ורמת בטיחות סבירה.
- 9.3.5 מומלץ להגדיר נעילת מחשב באמצעות סיסמה PIN/ (נעילת דפוס, ביומטרי, כרטיס חכם וכד).
- 9.3.6 מומלץ להגדיר ביצוע עדכוני תוכנה אוטומטיים לכלל התוכנות במחשב, כולל דפדפנים.
- 9.3.7 מומלץ לבצע עדכון יזום למערכת ההפעלה מיד עם פרסומו.
- 9.3.8 מיד בסיום העבודה מרחוק, העובדים ינתקו את הקישור.
- 9.4 בעת שימוש במחשבים מחוץ למשרדים לצורך עבודה, יש להקפיד הקפדה יתרה על כל נושאי אבטחת המידע המפורטים בהנחיות אלה, ובהנחיות החוק והדין בהתאם לנהלי האוניברסיטה והדרכות המודעות..

## **10. שימוש בדואר אלקטרוני**

- 10.1 לכל עובד תוגדר כתובת דואר אלקטרונית בהתאם לצורך.
- 10.2 חל איסור לשלוח קבצים המכילים תוכנות פוגעניות, תוכנות נזקה ווירוסים.
- 10.3 בעת קבלת דבר דואר המכיל קובץ מצורף יש לוודא כי סוג הקובץ שנשלח מאושר לשימוש ע"י גורמי אבטחת המידע של האוניברסיטה. יש לשים דגש מיוחד על קבצים המסתיימים בסיומות הבאות: Exe, Com, Vbs, Bat.
- 10.4 העברה ו/או קבלת קבצים, או תוכנות כאמור לעיל, תיעשה רק לאחר בדיקת תוכנת הגנה (אנטי-וירוס).
- 10.5 אין להעביר תכתובות המכילות מידע רגיש לגורמים חיצוניים שאינם מאושרים לקבלת מידע מהאוניברסיטה ולגורמים פנימיים שאינם מורשים
- 10.6 אין לפתוח קישור או צרופה שהגיעו בדוא"ל ממקור בלתי מזוהה מחשש לחדירת וירוס או כופרה.
- 10.7 עובד שקיבל דוא"ל חשוד ממקור בלתי מזוהה ימחק אותו מיד. במקרה הצורך ידווח ליועץ המחשוב.

## **11. דיווח על אירועי אבטחת מידע**

- 11.1 עליכם לדווח למנהל אבטחת מידע או ליועץ המחשוב של האוניברסיטה על כל הפרה של כללי אבטחת המידע וסייבר המובאים בהנחיות אלה. לדוגמה: חדירה לרשת, נעילת קבצים, השחתת אתר, דלף מידע בדוא"ל, חשיפת סיסמאות גישה, גישת גורמים לא מורשים למשרדי האוניברסיטה ועוד.
- 11.2 מנהל אבטחת המידע של האוניברסיטה הוא מר רוני סולומון. פרטי התקשרות: טלפון-072-2644804; דוא"ל- Roni.Solomon@biu.ac.il