אבטחת מידע ונהלי עבודה למשתמשים

1. מבוא

1.1 כללי

אבטחת מידע הינה: כלל האמצעים הטכנולוגיים והארגונים הננקטים לשמירה על סודיות וזמינות שלמות המידע. נוהל זה מציג עקרונות ליישום אבטחת המידע במכללה.

1.2 יעדים.

יעדי הנוהל הינם:

- לספק מסגרת והכוונה ליצירתה של התנהגות ארגונית, סטנדרטים טכניים והטמעת כלים לטיפול בנושאי אבטחת מידע ברמת המשתמש.
- להעלות את מודעות המשתמשים לנושא אבטחת מידע.

2. יישום אבטחת המידע בארגון

2.1 .עקרון האחריות האישית

במכללה ישנן שלוש קבוצות עיקריות המקבלות שירות ממחלקת המחשוב:

- סגל מנהלי
- סגל אקדמי
- סטודנטים

כל אחד ממשתמשי המחשב במכללה יהיה אחראי באופן אישי לאבטחת המידע במגוון הנושאים אליהם הוא נחשף במהלך עבודתו. כל פגיעה במידע שתנבע מרשלנות של המשתמש או מאי עמידה בנהלים תהיה באחריות המשתמש.

במסגרת אחריות זו, על משתמש המחשב לנקוט בכל האמצעים העומדים לרשותו על מנת להגן על המידע. בין אמצעים אלה:

- שימוש אישי בזיהוי המשתמש.
- שמירה על חיסיון הסיסמא.
- דיווח על חריגות אבטחת מידע.
- אבטחת סביבת העבודה.

בעת קבלתם לעבודה יחתמו עובדי המכללה ,סגל מנהלי וסגל אקדמי, על הצהרת סודיות.

ניהול סיסמאות גישה :

1 כמשתמש קיבלת שם משתמש ייחודי Username אשר יאפשר לך גישה למערכת. סיסמא זו הינה אישית.

הסיסמה אותה קיבלת היא לשימושך האישי בלבד ולשם ביצוע עבודתך. עליך לשמור את הסיסמא במקום חסוי ובטוח, שאינו חשוף לעיניים זרות. אל תעביר/י סיסמא זו לגורם כלשהו, כולל עובד אחר ואל תרשם/י אותה במקום סמוך לתחנת הקצה ו/או בכל מקום אחר, אשר עלול לחשוף אותה לאחר, או על מדיה כלשהי .

2 את הסיסמא עליך להחליף בהתאם למדיניות אבטחת המידע בארגון. בעת החלפת הסיסמה יש לבחור סיסמא ארוכה ומורכבת מינימום 8 תווים הכוללים מספרים – אותיות גדולות וקטנות .

3) לאחר זמן מסוים , המוגדר ע"י המערכת, אשר בו לא תהיה פעילות בתחנת הקצה, תינעל התחנה על מנת לשחררה, עליך להקיש את סיסמת הכניסה ל . Windows כמו כן , עליך לנעול בעצמך את התחנה ע"י – התנתקות עם עזבך את מקומך או לבצע כיבוי מחשב.

4) במידה ושכחת את הסיסמא , או אם הנך סבור שהיא הגיעה לאחר , עליך לפנות באופן מיידי למחלקת המחשוב. על מנת לקבל סיסמה זמנית חדשה , אותה תחליפ/י עם הכניסה המחודשת למערכת .

אחסון מידע ותוכנות בתחנות הקצה :

5) השימוש במחשב ובמאגרי מידע של המכללה הנו לצורך עבודה בלבד .

6) אין לשמור מידע תפעולי כלשהו על תחנת הקצה , אלא בכונן הרשת . קובץ שלא ישמר בשרת, לא יבוצע לו גיבוי והוא עלול להימחק או להינזק ללא יכולת שיחזור ! .

7) במידה והינך נדרש/ת להוסיף תוכנות לתחנת הקצה שבה הינך עובד/ת ,פנה למוקד התמיכה במחלקת המחשוב.

8) במידה וגילית תוכנה שמקורה אינו ברור לך , פנה למוקד התמיכה.

9) בתחנות הקצה, בהן ישנם אמצעי מדיה נתיקה, ניתן להשתמש ב CD / USB לצורך העברת חומר עבודה בלבד! עליך לבדוק את תוכנם באמצעות תוכנת אנטי וירוס המותקנת במחשבך

10) אין לעבוד עם תוכנות שיתופיות והורדות קבצים, תוכנות כאלו יוצרות עומס רב על הרשת ובמקביל מהוות חורי אבטחה דרכם נכנסים וירוסים ותוכנות ריגול .

11) ברשת המחשוב של המכללה קיים מידע רב. כל עובד נדרש לשיקול דעת ואסור לו לנסות לגשת למידע אשר אינה לשם תפקידו .

12) לידיעתך, כל המידע ופעילות מערכות המחשוב של החברה מנוטרים ומבוקרים ע"י גורמי אבטחת המידע.

שימוש בדואר אלקטרוני :

1) כעובד/ת, תוגדר לך כתובת דואר אלקטרוני.

2) הקפד/י, כי השימוש בדוא"ל לא יכלול תכתובות כגון :מכתבי שרשרת, פרסומות ומודעות מכל סוג שהוא וכדומה, אשר מקורם מחוץ לארגון ואינו קשור לפעילות השוטפת.

3) כמו כן, אל תעביר/י קבצים כגון קבצי ריצה, מוצרי תוכנה וכן תמונות, קבצי וידיאו ואודיו שאינם קשורים לעבודה, קבצי - פונטים, פקדים שונים ועדכוני תוכנות, ובכללם קבצים שמקורם ברשת האינטרנט. כאשר קיים צורך בקבצים אלה, נא לפנות למוקד התמיכה.

4) בדוא"ל חיצוני, אין להעביר מידע ובו תכנים הכוללים מידע רגיש ,אלא לאחר התייעצות וקבלת אישור ממנהלך הישיר ו/או ממחלקת המחשוב.

5) אל תפתח דוא"ל או צרופה ממקור בלתי מזוהה ,מחשש לתוכן זדוני .

6) אסור למשוך מיילים מתיבות דוא"ל "פרטיות" (כולל ובמיוחד שרתי דוא"ל חינמיים כמו Hotmail,Gmail וכו') שאינן מנוהלות בשרת הדוא"ל של המכללה ומהוות פתח לאירועי אבטחת מידע במכללה .

7) יש להיות ערניים לגבי וירוסים שמגיעים דרך הדוא"ל , מספר כללי יסוד :

א. יש לפתוח מייל אך ורק אם אתם מצפים לדוא"ל הנ"ל וברור לכם מקורו ונושאו .

ב. לא לפתוח מיילים ללא שם השולח .

ג. לא לפתוח אם שם השולח אינו מוכר .

ד. לא לפתוח אם בשם השולח רשום השם שלכם .

ה. לא לפתוח אם נושא המייל לא מובן .

ו. לא לפתוח אם הנושא לא אופייני לשולח (למשל :מכתב שכותרתו : "אני אוהב אותך" והוא הגיע מספק הציוד המשרדי שלכם יש להניח שזה וירוס ....).

ז. לא לשלוח לעולם פרטי סיסמה בדוא"ל.

ח. לא למלא פרטים אישיים מכל סוג בדוא"ל שנשלח אליכם, או בקישור שנמצא בדוא"ל שנשלח אליכם. אם פעולה זו נדרשת, יש להיכנס דרך הדפדפן לאתר, ולא להשתמש בקישור שהתקבל בדוא"ל.

8) לא לפתוח דוא"ל שצורפה לו צרופה (קובץ) אלא אם יודעים בוודאות מה תוכנו, אתם מזהים את סוג ומהות הקובץ וציפיתם בדיוק לקובץ זה .

9) שליחת דוא"ל לרשימת תפוצה של כמה עשרות נמענים ויותר, עלולה לגרום ל"סימון" העסק כשולח דואר ספאם (זבל) וכתוצאה מכך לחסימת כל הארגון ומניעת האפשרות לשלוח מיילים ממנו, במידה ושליחה כזאת היא צורך ממשי יש לתאם זאת עם מוקד התמיכה.

10) בחברה מותקן שרת דוא"ל האוגר את כל תוכן ה Outlook שלכם, בשל מגבלות מקום ,יש להקפיד למחוק ב outlook שלכם כל מופע מיותר כמו : פגישות שכבר עבר זמנם, דוא"ל שקיבלתם וכבר קראתם, דוא"ל יוצא שהעתק ממנו נשמר בתיבת הדוא"ל הנכנס וכו'.

11) הודעות דוא"ל חשודות יש למחוק מיידית ולדווח למוקד התמיכה מחלקת המחשוב .

12) תיבת הדוא"ל מיועדת לשימוש של בעל התיבה בלבד, אין להעבירה לאדם אחר ללא אישור.

הסדרת הגלישה ברשת האינטרנט :

1) בכל מקרה ,דע כי חל איסור מוחלט על גלישה לאתרים הבאים :

א. אתרים בעלי תוכן פורנוגרפי

ב. אתרי הימורים

ג. חדרי שיחה פרטיים(צ'טים)

ד. אתרי שיתוף קבצים, וכן אתרים המאפשרים הורדת תוכנות בלתי חוקיות, וזאת גם מחשש לחשיפת החברה לתביעות משפטיות .

ה. אתרים הנוגעים במידע הקשור לפריצה למערכות מחשב, וזאת מחשש למלכוד הגישה לאתר .

ו. אתרים בעלי תוכן בלתי נאות , העשוי לפגוע בשמה הטוב של המכללה .

2) לידיעתך, קיים ניטור תמידי לגלישה באינטרנט .

3) אין לנסות להתחבר לרשתות אלחוטיות זרות.

4) אין להתחבר לרשת אחרת/אינטרנט מהיר במקביל לחיבור לרשת של החברה .

אירוע אבטחה:

על כל משתמש לדווח על אירועים/בעיות אבטחת מידע בהם הוא/היא נתקל/ת במהלך

עבודתו/ה.

<u>סוגי האירועים/בעיות עליהם יש לדווח:</u>

- חשד לפרצות אבטחת מידע במערכות השונות ובמחשב האישי.
- חשד כלשהו כי המידע האגור במערכות נפגע (נמחק, שונה או נחשף).
- Phishing - פישינג (דייוג) היא בעצם שיטת הונאה, הגורמת לקורבן לחשוב שהוא מספק פרטים לאתר ידוע ובטוח, ובעצם הוא מספק פרטים לאתר שמתחזה לאתר אחר(ויכול להיות גם באימייל).
- חשד של המשתמש כי נעשה שימוש לא מורשה בזיהוי המשתמש שלו/ה.

1) בזמן אירוע אבטחה במכללה חלה חובת הדיווח באופן ישיר ומהיר ביותר למחלקת המחשוב ולמנהל הרשת העומד בראשה
2) חובה לכבות את המחשב על מנת לבודד את התקלה ולמונע התפשטותו לשאר מרכיבי הרשת

אבטחת סביבת העבודה

כל עובד/ת אחראי/ת לאבטחת סביבת העבודה האישית שלו/ה. אבטחת סביבת העבודה.

1) מסמכים רגישים לא יותרו חשופים על השולחן כאשר העובד עוזב את סביבת העבודה בסוף או במהלך יום העבודה
2) בסוף כל יום עבודה , עליך לכבות את תחנת הקצה או לבצע ניתוק משתמש .
3) במידה והנך נדרש להריץ עבודה ארוכות , וודא/י את נעילת המסך לפני יציאתך מהמשרד.
4) אל תוסיף רכיבי תקשורת כגון מודם, כ.רשת אלחוטי וכו' לתחנת הקצה .
5) אל תשאיר מדיה נתיקה, כוננים שליפים, CD וכו' המכילים מידע רגיש בסוף יום העבודה כשהם אינם נעולים.
6) במידה והנך רוצה לבצע שינוי בתחנת הקצה שלך ,פנה למחלקת המחשוב
7) אל תתקין/תסיר או תבצע שינוי בחומרה או בתוכנה המותקנת בתחנות הקצה בעצמך ו/או על דעת עצמך .
8) במידה וברשותך מחשב נייד השייך למכללה אין להשאיר את המחשב הנייד ללא השגחה במקום ציבורי .

הריני מאשר/ת כי קראתי והבנתי את האמור לעיל והנני מסכים/ה לכל .

תאריך : _____ שם פרטי ומשפחה : _____

חתימה : _____