אבטחת תחנות קצה/מחשבים אישיים	
נוהל מספר: 05 -50	מהדורה: 1
בתוקף מתאריך:19 ינואר 2009	עמוד 1 מתוך 4
מאשר הנוהל: ישיבת הנהלה מס' 76 מיום 19/1/2009	

1. מטרה

להגדיר את תהליך אבטחת תחנות קצה /מחשבים אישיים כדי למנוע נזק הנגרם מחשיפת מידע רגיש לגורם כלשהו, בלתי מורשה מתחנת קצה של מחשבי המכללה.

2. מסמכים ישימים

2.1.נוהל מספר 10-50 גיבוי ושחזור.

3. הגדרות

3.1.**מידע** - כל רישום שנעשה בכתב יד, בהקלדה, בהקלטה, בצילום או ברישום שנעשה באמצעי טכני אחר, שממנו הופק אחד מאלה: מסמך על נייר, מסמך מחשב, קלטת של תמונה, קלטת של קול, תצלום, מפה, תרשים, תבליט, סרט צילום, סרט מגנטי, תקליטור, דיסק, פלט מחשב, קובצי מחשב או כל תוצר אחר של רישום שנעשה באמצעי טכני.

3.2.**נזק** - אחת מאלה:

3.2.1. נזק של זליגת מידע.

3.2.2. נזק לעבודה השוטפת של המכללה.

3.2.3. נזק של חדירה לפרטיות.

3.2.4. נזק של שינוי מידע חשוב.

3.3.**תחנת קצה** - מחשב קבוע, מחשב נייד או כל התקן אחר המעבד או המאחסן חומר מכללתי או מחובר לרשת מחשבים של המכללה.

3.4.**תחנת קצה בעלת רגישות גבוהה** - מחשב קבוע, מחשב נייד או כל התקן אחר המעבד או המאחסן חומר מכללתי בעל רגישות גבוהה שזליגת מידע או איבוד מידע יכולים להסב נזק ישיר או עקיף למכללה.

4. השיטה

4.1.כל גישה למחשב תחוייב בשימוש בסיסמא אישית ובאימות מרכזי. תקבע סיסמא באופן שלא תיהיה קלה לניחוש ולא מורכבת מפרטיו האישיים של בעל הסיסמא. איכות הסיסמא, הרכב התווים האקראי שלה ואי חשיפתה לעובדים אחרים יהוו את המחסום העיקרי בפני משתמשים לא מורשים.

אבטחת תחנות קצה/מחשבים אישיים	
נוהל מספר: 05 -50	מהדורה: 1
בתוקף מתאריך:19 ינואר 2009	עמוד 2 מתוך 4
מאשר הנוהל: ישיבת הנהלה מס' 76 מיום 19/1/2009	

4.2. על כל עובד יש לדווח לממונה הישיר וליחידת המחשוב על כל שימוש בסיסמא אישית ע"י גורם כלשהו שאינו בעל הסיסמא.במקרים חריגים יש צורך בקבלת אישור מיוחד ממנהל יחידת מחשוב.

4.3. על עובדי יחידת המחשוב יש לוודא הפעלת "שומר מסך" עם סיסמא לאחר 20 דקות של אי פעילות במחשב בכלל המחשבים ו- 10 דקות למחשבים בעלי רגישות גבוהה יותר (ראה סעיף 3.4). כדי לאכוף כלל זה נשתמש במערכת הפעלה בעלת יכולות אבטחה מובנות וטובות כדוגמת WIN XP PRO / VISTA או דומה.

4.4. חל איסור מוחלט על שימוש בתקליטונים,תקליטורים ובהתקנים המבוססים על טכנולוגיית USB (להלן "אמצעי אחסון ניידים") שאינם שייכים למכללה, שכן פעולה זו עלולה לגרום לתופעות הבאות:

4.4.1. החדרת וירוסים או תוכנות בעלות כוונות זדון.

4.4.2. שימוש בתוכנות לא חוקיות שיחשפו את המכללה לתביעות משפטיות.

4.5. אמצעי אחסון ניידים מכללתיים שאינם בשימוש, יועברו ליחידת מחשוב ותקשורת לצורך ביצוע תהליך של הריסת נתונים ללא יכולת שחזור.

4.6. אנשי המחשוב המוסמכים במכללה יוכלו להעזר בשירותי מיקור חוץ בנושאי אבטחת תחנות קצה, מחשבים אישיים ,שרתים או כל שירות מחשוב אחר ובכפוף לאישור מנהל המיחשוב והתקשורת.

4.7. מידע רגיש יוצפן במחשב האישי באמצעות שירותי האבטחה של מערכת המחשוב במכללה ע"פ החלטת מנהל מחשוב ותקשורת.

4.8. מחלקת המחשוב תוודא התקנת אנטי וירוס מעודכן המאפשר לערוך סריקה מקיפה נגד וירוסים וסוסים טוריאניים בדיסק הקשיח וברכיבי הזכרון, ולבודד קבצים נגועים כדי למנוע פגיעה בשאר המערכות ברשת.

4.9. במחשבים ניידים של המכללה יש להתקין מערכת FIREWALL אישית, המסננת מנות, חבילות (packets & frames) וכתובות בלתי רצויים ומונעת גישה של גורמים בלתי מורשים אל המחשב.

4.10. מחלקת המחשוב תוודא שהמחשבים האישיים/ תחנות הקצה מאובטחים

אבטחת תחנות קצה/מחשבים אישיים	
נוהל מספר: 05 -50	מהדורה: 1
בתוקף מתאריך:19 ינואר 2009	עמוד 3 מתוך 4
מאשר הנוהל: ישיבת הנהלה מס' 76 מיום 19/1/2009	

פיזית: על ידי אמצעי בקרת כניסה, בריח, ואזעקת מבנה. כמו כן, הם ישתמשו בפרופילי משתמשים המוגדרים במערכת ההפעלה. משתמש קצה לא ישתמש בסיסמת האדמיניסטרטור גם לא במחשב נייד.

4.11. אנשי מחשוב ותקשורת יוודאו ששירותי רשת בלתי הכרחיים לא יהפכו לזמינים לגורמים בלתי מורשים. לכן יש להסיר שירותי רשת שאינם בשימוש ואין לשתף קבצים או סיפריות, במחשבים אישיים/ תחנות הקצה.

4.12. על העובד לבצע יציאה מסודרת מן המחשב האישי/ תחנת הקצה (ניתוק) או כיבוי בסוף יום העבודה.

5. מחלקת המחשוב תבצע גיבוי יומי או שבועי לפחות, למחשב אישי/ תחנת קצה ותשמור את תוצרי הגיבוי בכספת מוגנת מפני אש ומאובטחת ע"פ הכללים שקבע מנהל יחידת מחשוב ותקשורת (כיוון שכל הנתונים נמצאים פיזית על השרתים ולא על התחנות, גיבוי הנתונים יתבצע על השרתים המתאימים כמפורט בנוהל גיבוי ושחזור מספר 50-10.) אחריות

5.1. **אחריות לקיום הנוהל היא של מנהל יחידת המחשוב**

5.2. אחריות לביצוע הנוהל היא על:

5.2.1. מנהלי המחלקות במכללה.

5.2.2. יחידת מחשוב ותקשורת.

5.2.3. כל עובדי המכללה שלהם נגישות לתחנות קצה או למחשבים אישיים של המכללה.

5.3. **אחריות בקרה**:

5.3.1. יחידת מחשוב ותקשורת.

5.4. **תדירות בקרה**:

5.4.1. אחת לשישה חודשים.

6. נספחים

6.1. אין

אבטחת תחנות קצה/מחשבים אישיים	
נוהל מספר: 05 -50	מהדורה: 1
בתוקף מתאריך:19 ינואר 2009	עמוד 4 מתוך 4
מאשר הנוהל: ישיבת הנהלה מס' 76 מיום 19/1/2009	

[טבלת שינויים שבוצעו בנוהל]

מהדורה	תאריך ביצוע העדכון	סעיף/ים מושפע/ים	תיאור העדכון

11 Jerusalem st. P.O.B 160 Zefat 13206 Israel
Tel. +972-4-6927800 Fax. +972-4-6927810
Operator: Tel +972-4-6927777
E-mail: nesi@zefat.ac.il

רח' ירושלים 11 ת.ד. 160 צפת 13206
טל: 04-6927800 פקס: 04-6927810
מרכזיה: 04-6927777
דואר אלקטרוני: