שם ההוראה	מספר ההוראה
קישור מודמים למחשבים באוניברסיטה והתקנת תוכנות השתלטות מרחוק	23-001
נספחים מצורפים	**בתוקף מתאריך פרסום**
	27.5.03

תוכן עניינים **עמוד**

1. מטרה 2
2. הגדרות 2
3. הגנה על הרשת 2
4. קישור מודמים 3
5. התקנת תוכנות השתלטות מרחוק 3
6. חיבורי אינטרנט (ADSL, כבלים, נל"נים ואחרים) 4
7. קישורים אלחוטיים 4
8. חריגים 5

1. מטרה

1.1 הוראה זו קובעת כי:

1.1.1 **חל איסור לחבר או לקשר באופן פרטי לרשת חיצונית לאוניברסיטה מחשבים/ציוד אחר,** אשר מחובר לרשת התקשורת של האוניברסיטה.

1.1.2 **חל איסור להתקין תוכנות להשתלטות מרחוק על ציוד המחובר לרשת התקשורת של האוניברסיטה.**

1.2 יחד עם האמור לעיל, ההוראה מפרטת מקרים יוצאים מן הכלל ביחס לאיסורים הנ"ל וקובעת את הגורמים המוסמכים לאישורם של מקרים אלה.

2. הגדרות

2.1 ציוד - כל רכיב המסוגל לעבד תקשורת מחשבים, לרבות מחשב, ציוד תקשורת, מודם וכדי.

2.2 מודם - רכיב המאפשר קישור בין מחשב ובין רשת בזק.

2.3 חיבור חיצוני - כל אמצעי המאפשר העברת מידע בין רשת האוניברסיטה, הנמצאת תחת אחריותה של הרשות למחשוב, תקשורת ומידע, לבין רשת שאינה באחריות הרשות.

2.4 השתלטות מרחוק - רכיב או תוכנה המותקן במחשב ומאפשר לגורם המחובר לרשת תקשורת כלשהי לפעול על המחשב כאילו היה מחובר אליו מקומית, לעתים תוך שימוש בדוי בזהות המשתמש החוקי (דוגמאות לתוכנות נפוצות כאלו הנן VNC, pcAnywhere ושירותי Terminal Services של Microsoft).

2.5 רשת המינהל - החלק של רשת התקשורת האוניברסיטאית, שממנו ניתנת גישה לשרתי המינהל של האוניברסיטה.

3. הגנה על הרשת

3.1 רשת התקשורת של האוניברסיטה מהווה יעד לניסיונות פריצה תדירים מצד גורמים שונים, **ולכן יש להגן עליה ועל המחשבים הקשורים אליה.**

3.2 חיבורים שאינם מוגנים מאפשרים החדרת תוכנות, היכולות לגרום לנזקים מסוגים שונים, כגון:

3.2.1 שליפת מידע ממחשב עליו מותקנת התוכנה ללא ידיעת בעל המחשב.

3.2.2 שליפת מידע לא מורשית ממחשבים אחרים אליהם ניגש בעל המחשב (לדוגמה: שליפת פרטי כרטיס האשראי כאשר המשתמש גולש לאתר חברת האשראי שלו).

3.2.3 שליפת ואף שינוי מידע במערכות המינהל של האוניברסיטה (כאשר קישור כזה נעשה למחשב המחובר לרשת המינהל).

3.2.4 אפשרות להפצת התוכנה העוינת ברשת וכתוצאה מכך הגדלת הנזק.

3.2.5 תקיפה של מחשבים אחרים באינטרנט כתוצאה מתוכנות עוינות, דבר שיגרום לחסימת הגישה של משתמשי האוניברסיטה למספר רב של אתרים באינטרנט.

3.2.6 תשלום חריג של האוניברסיטה על שימוש ברשת האינטרנט כתוצאה מתעבורה חריגה, שתיווצר בגין תוכנות אלו.

3.3 ההגנה על רשת התקשורת של האוניברסיטה נעשית בשתי רמות עיקריות: **הגנה על הרשת עצמה ושימוש באמצעי אבטחה והגנה על המחשבים המקושרים אליה**.

3.4 ההגנה על הרשת נעשית על-ידי הרשות למחשוב, תקשורת ומידע, אשר אחראית להגן על הרשת בחיבורים המקשרים אותה לעולם החיצון.

3.5 חל איסור לאפשר כניסה עוקפת ולא מאובטחת לציוד שמחובר לרשת האוניברסיטאית, כולל מחשבים אישיים; מסיבה זו, אין להתקין מודמים, תוכנות השתלטות מרחוק וחיבורי אינטרנט פרטיים אלא בכפוף לכללים ולהנחיות שלהלן.

4. <u>קישור מודמים</u>

4.1 לא יקושר מודם מכל סוג שהוא (לרבות מודם חיוג, ISDN, ADSL, מודם כבלים וכדי) לציוד המחובר לרשת האוניברסיטה, אלא אם הוא משמש כפקס בלבד. קישור מודם המשמש לגישת נתונים יותר **אך ורק** אם הוא חלק ממערך הגישה (המרכזי) מרחוק של הרשות למחשוב, תקשורת ומידע וכל גישה אליו מזוהה על-ידי מערכת הזיהוי המרכזית.

4.2 בשום מקרה לא יחובר מודם (כולל פקס) לציוד המחובר לרשת מינהל, אלא לאחר קבלת אישור בכתב ממנהל המחלקה למערכות מידע ממוחשבות.

5. <u>התקנת תוכנות השתלטות מרחוק</u>

5.1 תוכנות השתלטות מרחוק מאפשרות גישה מלאה למחשב מרוחק, לעיתים ללא הסכמה (או ידיעה) של בעל המחשב; במקרה של שימוש עוין בעל המחשב הוא האחראי לנעשה, ולכן עליו מוטלת החובה להימנע משימוש בתוכנות כאלו ככל האפשר. <u>במידה שנדרשת תוכנה כזו, היא תותקן בהתאם לתנאים שלהלן:</u>

5.1.1 הגישה תהיה מעל פרוטוקול TCP/IP ובשום מקרה לא בקישור מודם מקומי (אם נדרש קישור דרך מודם, הוא ייעשה על-ידי מודמים של הרשות למחשוב, תקשורת ומידע ומשם בפרוטוקול TCP/IP).

5.1.2 התוכנה לא תופעל כשגרה, אלא כאשר יש בה צורך ולאחר תיאום בין השולט לנשלט.

5.1.3 לכל חיבור תוקצה (על-ידי מחולל סיסמאות) סיסמה חד פעמית, שלא ניתן יהיה להשתמש בה בפעם הבאה.

5.1.4 התוכנה תיסגר מיד עם סיום השימוש על-ידי השולט או הנשלט. יאושר שימוש רק בתוכנות בהן ניתנת לשולט אפשרות לסגור את התוכנה הנשלטת מרחוק.

5.1.5 גישה לתוכנות השתלטות מרחוק לא תאושר מחוץ לאוניברסיטה, אלא במקרים חריגים אשר ייבדקו באופן פרטני; בכל מקרה, גישה כזו תהיה מוגבלת בזמן ותתבצע מעל תווך מוצפן (כגון SSL) כדי למנוע גילוי סיסמאות מקומיות.

5.1.6 ההתקנה אושרה על-ידי מנהל אבטחת המידע של הרשות למחשוב, תקשורת ומידע.

5.2 ברשת המינהל לא תותקן תוכנה המאפשרת השתלטות מרחוק, אלא אם אושרה בכתב על-ידי מנהל המחלקה למערכות מידע ממוחשבות וההתקנה נבדקה על-ידי מנהל אבטחת המידע של הרשות למחשוב, תקשורת ומידע.

5.3 לא ייחתם חוזה תמיכה המחייב שימוש בתוכנות השתלטות מרחוק, אלא אם אושר בכתב על-ידי מנהל הרשות למחשוב, תקשורת ומידע, ובמקרה של מערכות מידע מינהליות על-ידי מנהל המחלקה למערכות מידע ממוחשבות.

5.4 יש לדווח למנהל הרשות למחשוב, תקשורת ומידע על חוזים קיימים, שבהם קיים סעיף המחייב שימוש בתוכנות השתלטות מרחוק לשם אישור/בדיקה מחודשים.

6. <u>חיבורי אינטרנט (ADSL, כבלים, נל"נים ואחרים)</u>

כל קישור חיצוני אל ציוד המחובר לרשת האוניברסיטה **אסור בהחלט**, למעט הקישורים המרכזיים המנוהלים על-ידי הרשות למחשוב, תקשורת ומידע.

7. <u>קישורים אלחוטיים</u>

באחרונה מתרחב השימוש בציוד המאפשר קישור אלחוטי לרשת. מכיוון שאין אפשרות לשלוט על תחנות המנסות להתחבר לרשת אלחוטית, תוגן כל רשת כזו על-ידי שימוש באמצעי זיהוי חזק ובהצפנה (אשר יהיו מקובלים על מנהל אבטחת המידע של הרשות למחשוב, תקשורת ומידע). בנוסף לכך, ציוד שמתחבר או מתנתק מהרשת האלחוטית ישלח רשומות כניסה/יציאה בזמן אמת לשרת ה- Radius או ה- Tacacs+ של הרשות למחשוב, תקשורת ומידע.

בכל מקרה, ציוד לתקשורת אלחוטית לא יירכש ולא יותקן לפני קבלת אישור ממנהל אבטחת המידע של הרשות למחשוב, תקשורת ומידע.

8. חריגים

8.1 ניתן לקשר ציוד לרשת חיצונית, בתנאי שהציוד אינו מחובר לרשת האוניברסיטה.

8.2 אין לחבר את הציוד (שהיה מקושר לרשת חיצונית) חזרה לרשת האוניברסיטה, אלא לאחר ניתוקו מהרשת החיצונית ולאחר קבלת אישור לתקינות המערכת ממנהל אבטחת המידע של הרשות למחשוב, תקשורת ומידע. אישור זה יינתן רק לאחר שתבוצע סריקה מקיפה לאיתור וירוסים וסוסים טרויאניים במערכת. הסריקה תבוצע באחריות בעל הציוד ובסיועם של אנשי הרשות למחשוב, תקשורת ומידע או אנשי המחלקה למערכות מידע ממוחשבות.