תפעול מערך סיסמאות	
נוהל מספר: 02 -50	מהדורה: 1
בתוקף מתאריך:19 ינואר 2009	עמוד 1 מתוך 8
מאשר הנוהל: ישיבת הנהלה מס' 76 מיום 19/1/2009	

1. <u>מטרה</u>

1.1. ליצור שיטה אחידה לתפעול מערך סיסמאות המשמשות לזיהוי משתמשים במערכות הממוחשבות.

1.2. למנוע היחלשות מערך האבטחה כתוצאה מחוסר תיאום בין מנהלי מערכות שונים.

2. <u>מסמכים ישימים</u>

2.1. ת"י 1495

3. <u>הגדרות</u>

3.1. **משתמש** - כל אדם, הממלא תפקיד כלשהו במכללה. כולל עובדים, מנהלים, מרצים, עובדי קבלן וכד', אשר במסגרת תפקידו משתמש במערכות המידע הממוחשבות של המכללה.

3.2. **שם משתמש -** (USER ID) / זיהוי משתמש - שם ייחודי אשר נקבע לכל משתמש מחשב במכללה האקדמית צפת, לצורך זיהויו במערכת הממוחשבת.

3.3. **סיסמא** - שדה המכיל מספר תווים, אשר המשתמש חייב לזכור אותם ולהקישם בצמוד לזיהוי המשתמש בכדי לאמת את זהותו במערכת הממוחשבת.

3.4. **סיסמא ראשונית -** סיסמא הניתנת למשתמש חדש, או למשתמש ששכח סיסמתו. על המשתמש להחליף סיסמא זו מיד בכניסתו הראשונה למערכת באמצעותה. במערכת ההפעלה מוגדר שיש לכפות החלפת סיסמא ראשונית עם הכניסה הראשונה למערכת.

4. <u>השיטה</u>

4.1. <u>מבוא</u>

4.1.1. זיהוי המשתמש מול מערכות המחשב יעשה ע"פ שם משתמש שיורכב משם פרטי ולפחות אות משם המשפחה באנגלית.

4.1.2. אימות זיהוי המשתמש במערכות הממוחשבות יעשה ע"י הקשת סיסמא אישית או אימות אחר, כפי שיוגדר מעת לעת ע"י מנהל מחשוב ותקשורת (כרטיס זיהוי, ביומטרי, מחוללי סיסמאות וכו').

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 דואר אלקטרוני:

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

4.1.3. על המשתמש לבחור סיסמא לא טריוויאלית, בעלת מבנה קשה לניחוש. חוקי הסיסמא יוגדרו באופן מרכזי, בתלות ביכולות מערכת ההפעלה / מוצר אבטחה נלווה.

4.1.4. הסיסמא תוחלף באופן תקופתי, לאחר 240 ימים או כאשר קיים חשש שנחשפה. במרבית המערכות, החלפת הסיסמא תכפה באופן אוטומטי. במערכות שאינן מאפשרות כפיית החלפה, ההגדרה נוהלית.

4.1.5. הגדרת מערך הסיסמאות תתבצע על ידי מנהל מחשוב ותקשורת, או עובד מיחידת המחשוב בהנחיית מנהל מחשוב ותקשורת ראה סעיף 4.2 להלן.

4.1.6. טיפול שוטף בנושא סיסמאות (החלפת סיסמא שנשכחה, הדרכת משתמשים) יהיה גם הוא באחריות יחידת מחשוב ותקשורת.

4.2. <u>הנחיות שימוש בסיסמא – עבור משתמשים</u>

4.2.1. בעת הגדרת חשבון משתמש תוקצה סיסמא ראשונית. בכניסה הראשונה לחשבון יש להקיש סיסמא ראשונית זו ומיד לאחר מכן תדרוש המערכת להחליפה.

4.2.2. על המשתמש לבחור סיסמא לא טריוויאלית, בעלת מבנה קשה לניחוש. לדוגמא אין לבחור סיסמא זהה לשם המשתמש, או רצף תווים כגון 123456.

4.2.3. משתמש לא יחשוף את סיסמתו, ולא יאפשר לאף אדם אחר (כולל הממונים עליו) להשתמש בה. אין לרשום את הסיסמא בשום מקום גלוי.

4.2.4. משתמש לא יעשה שימוש בסיסמא של אדם אחר, גם במקרים בהם אדם אחר אישר לו לעשות שימוש בסיסמתו.

4.2.5. במקרה שמשתמש חושש שסיסמתו נחשפה, עליו להחליפה.

4.2.6. יש להחליף סיסמא גם בכל עת שהמערכת דורשת זאת – בד"כ מדי 8 חודשים (240 יום).

4.2.7. משתמש אשר שכח את סיסמתו, יפנה למנהל מחשוב ותקשורת, אשר יקצה עבורו סיסמא ראשונית או לממונה מטעמו.

תפעול מערך סיסמאות	
נוהל מספר: 02 -50	מהדורה: 1
בתוקף מתאריך:19 ינואר 2009	עמוד 3 מתוך 8
מאשר הנוהל: ישיבת הנהלה מס' 76 מיום 19/1/2009	

4.3. ניהול מערך הסיסמאות – ע"י אנשי SYSTEM

4.3.1. במכללה האקדמית צפת נקבעו כללים מנחים למבנה הסיסמאות. פירוט ראה להלן.

4.3.2. לכל משתמש במערכות המכללה תוגדר סיסמא, שתידרש בכל כניסה למערכת.

4.3.3. בעת הגדרת משתמש חדש, תוקצה לו סיסמא ראשונית. סיסמא זו תורכב ממספר ת.ז. של המשתמש, בתוספת מחרוזת כלשהי שתימסר לו בטלפון.

4.3.4. עם חיבור מערכת כלשהי לרשת המכללה, לאחר התקנת כל תוכנת מדף, ולאחר שדרוג של מערכת הפעלה, ישונו הסיסמאות של כל המשתמשים המסופקים עם המערכת כברירת מחדל. למשל GUEST, ADMIN, SYSTEM וכדי.

4.3.5. אפליקציה הדורשת סיסמא, לא תשמור קובץ סיסמאות בצורה גלויה, ולא תציג את הסיסמא על המסך בעת הקשתה.

4.4. מאפייני סיסמא כלליים

יש לוודא החלת כללים זהים למבנה הסיסמא בין פלטפורמות שונות, במידת האפשר, (תמיכת המערכות במאפיינים אלו).

הכללים להלן אינם פחותים מן הנדרש בתקן ישראלי 1495, עבור רמת אבטחה גבוהה.

4.4.1. אין לבחור סיסמא זהה לזיהוי המשתמש, לשמו, או לפרט מזהה אחר של המשתמש הידוע ברבים (כמו כינוי, שם משפחה, תפקיד, מס' טלפון). כמו כן, מומלץ שלא לבחור סיסמא שהיא מילה חוקית באנגלית, כיוון שקיימות תוכנות מיוחדות לפיצוח סיסמאות כאלו.

4.4.2. יש לכפות מבנה סיסמא שיורכב מ: אותיות גדולות, אותיות קטנות, ספרות וסימנים מיוחדים.

4.4.3. אורך מינימלי לסיסמא יהיה 6 תווים לכלל המשתמשים, ו- 8 תווים עבור משתמשים בתפקידים רגישים (לפי הנחיות מנהל מחשוב ותקשורת).

תפעול מערך סיסמאות	
נוהל מספר: 02 -50	מהדורה: 1
בתוקף מתאריך:19 ינואר 2009	עמוד 4 מתוך 8
מאשר הנוהל: ישיבת הנהלה מס' 76 מיום 19/1/2009	

4.4.4. המערכות יכפו החלפת סיסמא מדי 240 יום לכלל המשתמשים, ומדי 180 יום לחשבונות רגישים (כגון חשבונות SYSTEM). עם זאת, על המשתמש מוטלת החובה והאחריות להחליף סיסמא גם בתוך פרק זמן זה, במקרה שהוא חושד כי התגלתה לאדם אחר (כולל הממונים עליו).

4.4.5. המערכת תשמור רשימה של 24 סיסמאות היסטוריות, למניעת חזרה מהירה לסיסמא שהוחלפה. משתמש לא יוכל לשנות סיסמא לאחת מן הסיסמאות המופיעות ברשימה ההיסטורית.

4.4.6. גישת המשתמש תיחסם לאחר 5 ניסיונות גישה רצופים באמצעות סיסמא שגויה. לצורך שחרור החסימה – על המשתמש לפנות ליחידת מחשוב ותקשורת.

4.4.7. לכל משתמש חדש (או למשתמש ששכח את סיסמתו) תוגדר סיסמא ראשונית, כך שתוקפה יפוג מיד עם השימוש הראשון בה. על המשתמש להחליפה בעת הכניסה הראשונה למערכת.

4.4.8. מערך הסיסמאות, ינוהל עפ"י נוהל זה, עד ליישום מנגנון לסנכרון סיסמאות בפלטפורמות השונות במכללה ו/או עד לכינון מדיניות זיהוי אלטרנטיבית (כרטיס זיהוי, ביומטריה וכו'). בכל מקרה, נוהל זה יהווה את הבסיס למערך אימות זיהוי המשתמשים.

4.4.9. נושאים ספציפיים למערכת מבוססת NT – ראה בנספח.

4.5. <u>שחרור נעילת חשבון עקב ניסיונות גישה כושלים</u>

4.5.1. חשבונות משתמשים ננעלים לאחר 5 ניסיונות גישה באמצעות סיסמא מוטעית.

4.5.2. במקרה שמשתמש פונה ליחידת המחשוב לאחר שננעל, על עובד היחידה לזהות את הפונה זיהוי וודאי (בהתאם לפרטים המופיעים בהגדרת ה-USER במערכת ההפעלה), או במערכת נלווית.

4.5.3. על העובד לוודא שאכן הפונה הוא זה ששכח את הסיסמא (ולא שהחשבון ננעל לאחר שמישהו אחר ניסה לנחש את הסיסמא).

4.5.4. במקרה של ניסיונות גישה שלא נעשו ע"י המשתמש עצמו וגרמו לחסימת החשבון, על המשתמש לדווח למנהל מחשוב ותקשורת.

4.5.5. לאחר הזיהוי תינתן לפונה סיסמא ראשונית. סיסמא זו תימסר טלפונית, ותורכב ממספר ת.ז. של המשתמש + מחרוזת כלשהי.

4.5.6. על עובד היחידה להנחות את המשתמש להחליף את סיסמתו מיד בכניסה למערכת, וכן להמליץ לו להחליף סיסמא בכל המערכות אליהן הוא נוהג להתחבר, על מנת לשמור על סיסמא אחת אחידה (ולמנוע שכחה ובלבול בין סיסמאות במערכות השונות).

4.5.7. המשתמש יכול להחליף את סיסמתו באופן עצמאי ובהתאם להגדרות והרשאות שקיימות במערכת כמו כן יוכל לקבל סיוע ומדריך מטעם יחידת המחשוב לשינוי הסיסמא (נספח 6.2).

4.6. <u>חריגים</u>

בכל מערכת מוגדר שם משתמש מיוחד אשר משמש לתחזוקת המערכת בזמן שאנשי התחזוקה שלה אינם זמינים.

לגבי שם משתמש זה, חלים כללים חריגים. למשל: מותר לרשום את הסיסמא שלו (ולשמור זאת בכספת), אין לסיסמא תאריך פקיעה, אין למשתמש אפשרות להחליף את הסיסמא וכד'.

5. <u>אחריות</u>

5.1. **אחריות ביצוע - קיום הוראות הנוהל :**

5.1.1. מנהלי מחלקות .

5.1.2. מנהלי מערכות.

5.1.3. כלל המשתמשים.

5.1.4. עובדי יחידת המחשוב

6. <u>נספחים</u>

6.1. נ ס פ ח - מאפייני סיסמא במערכת מבוססת NT.

תפעול מערך סיסמאות	
נוהל מספר: 02 -50	מהדורה: 1
בתוקף מתאריך:19 ינואר 2009	עמוד 6 מתוך 8
מאשר הנוהל: ישיבת הנהלה מס' 76 מיום 19/1/2009	

נ ס פ ח 6.1 - מאפייני סיסמא במערכת מבוססת **NT** (2008 / 2003)

הנספח נכתב בהתאם לתקן ישראלי 1495, עבור רמת אבטחה גבוהה:

חלק א' - מדיניות סיסמא

פרמטר	הסבר	ערך מומלץ
Maximum Password Age	אורך חיי סיסמא מרבי בימים	240 יום או 180 יום
Minimum Password Age	אורך חיי סיסמא מינימלי. מונע מהמשתמש להחליף את הסיסמא יותר מפעם אחת ביום, באופן יזום, וזאת למניעת חזרה מהירה לסיסמא הקודמת (עקיפת מנגנון שמירת ההיסטוריה).	14 יום
Minimum Password Length	אורך סיסמא מינימלי.	6 תווים למשתמשים רגילים. 8 תווים למשתמשים פריווילגיים כגון Administrator, Server Operator, BackOperator ולבעלי תפקידים בכירים במכללה. (רצוי שהסיסמא תהיה מורכבת מ: אותיות גדולות, אותיות קטנות, ספרות וסימנים מיוחדים).
Enforce Password History	רשימה של סיסמאות היסטוריות של המשתמש. לא מאפשר לעדכן סיסמא שכבר הייתה בשימוש בעבר.	24 סיסמאות ישנות.

11 Jerusalem st. P.O.B 160 Zefat 13206 Israel
Tel. +972-4-6927800 Fax. +972-4-6927810
Operator: Tel +972-4-6927777

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

E-mail: nesi@zefat.ac.il דואר אלקטרוני:

תפעול מערך סיסמאות	
נוהל מספר: 02 -50	מהדורה: 1
בתוקף מתאריך:19 ינואר 2009	עמוד 7 מתוך 8
מאשר הנוהל: ישיבת הנהלה מס' 76 מיום 19/1/2009	

חלק ב' - מדיניות חשבון

פרמטר	הסבר	ערך מומלץ
Account Lockout Duration	משך הזמן שהחשבון יהיה נעול לאחר X ניסיונות כניסה כושלים	0 - החשבון יהיה נעול עד שה-Administrator יפתח אותו
Account Lockout Threshold	מספר הניסיונות הכושלים עד שהחשבון יכנס למצב Account Lockout	5 ניסיונות כושלים
Reset Account Lockout Counter After	משך הזמן שהמערכת תמתין עד לאיפוס הניסיונות הכושלים כל עוד שהחשבון עדיין לא ננעל (עד 4 ניסיונות, ב-5 החשבון ננעל)	60 דקות לאיפוס לפני מצב נעילה

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 דואר אלקטרוני:

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

תפעול מערך סיסמאות	
נוהל מספר: 02 -50	מהדורה: 1
בתוקף מתאריך:19 ינואר 2009	עמוד 8 מתוך 8
מאשר הנוהל: ישיבת הנהלה מס' 76 מיום 19/1/2009	

[טבלת שינויים שבוצעו בנוהל]

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

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