1. **<u>רקע</u>**
הטכניון, אשר ברשותו מערכות מחשוב, מחייב את המשתמשים להזדהות באמצעות סיסמאות לשם בקרת גישה אליהן.

2. **<u>מטרות</u>**
מטרת נוהל זה לקבוע סטנדרט אחיד לכלל המשתמשים, בנוגע למבנה הסיסמא ומורכבותה בכל מערכות המחשוב בטכניון.

3. **<u>הגדרות</u>**
3.1. <u>סיסמא</u> - אות מוסכם המשמש כאמצעי זיהוי לשם בקרת גישה . הסיסמה עשויה להיות מילה , ביטוי קצר (שבדרך כלל חסר משמעות), רצף ספרות ו/או תווים כלשהם, צליל ועוד.
3.2. <u>מתקפת כוח גס (Brute Force)</u>- מתקפה המשמשת בעיקר לפריצת סיסמאות, במטרה לגלות סיסמת גישה ע"י ניסוי ווריאציות שונות של צירופים.

4. **<u>סמכות ואחריות</u>**
4.1. באחריות מנהל מערכת להגדיר מדיניות הסיסמאות בהתאם לסטנדרט הנקבע ע"י נוהל זה.
4.2. בסמכות ואחריות ממונה אבטחת המידע לבקר את אכיפת הנוהל.

5. **<u>שיטה/מהות</u>**
5.1. <u>מבנה הסיסמא</u>
5.1.1. אורך הסיסמא יהיה 8 תווים לפחות, על מנת להקשות על מתקפות כגון כוח גס.
5.1.2. הסיסמא תכלול לפחות 3 מתוך 4 הקטגוריות הבאות :
5.1.2.1. אותיות קטנות (a,b,c,…..,x,y,z).
5.1.2.2. אותיות גדולות (A,B,C,….,X ,Y,Z).
5.1.2.3. הסיסמא תכיל תו מיוחד אחד לפחות.
5.1.2.4. הסיסמא תכיל ספרות (0,1,….,8,9).
5.1.3. הסיסמא לא תכיל מילים קלות לניחוש כמו password , secret , שם המשתמש וכדומה.

5.2. <u>תוקף סיסמא</u>
תוקף הסיסמא יהיה לכל היותר 365 יום. הסיסמא תידרש להחלפה באופן אוטומטי לאחר זמן זה.

5.3. <u>מנגנוני מניעת מתקפת כוח גס (Brute Force)</u>
5.3.1. כתובת התוקף תיחסם לאחר 10 ניסיונות כניסה כושלים לכל היותר, ובמידה ולא ניתן לחסום את התוקף החשבון ייחסם.
5.3.2. חסימת התוקף או החשבון תשתחרר אוטומטית לאחר 30 דקות.
5.3.3. שחרור מיידי של חסימת החשבון יוכל להתבצע באמצעות פנייה לאיש מחשוב יחידתי או למוקד התמיכה.

5.4. <u>החלפת סיסמא</u>
5.4.1. החלפת הסיסמא למשתמש במערכות המרכזיות תתבצע באתר http://cis-account.technion.ac.il בלבד, ואילו במערכות אחרות במקום הייעודי הרלוונטי בהתאם למערכת.
5.4.2. לא יתאפשר למשתמש לעשות שימוש חוזר בשלוש הסיסמאות האחרונות בהן עשה שימוש בעבר.

6. **<u>תחולה ותוקף</u>**

6.1. נוהל זה חל על כל מערכות המחשוב בטכניון ובמוסד הטכניון למחקר ופיתוח בע"מ למעט מערכות שלא ניתן ליישם בהן את הוראות הנוהל עקב מגבלות טכנולוגיות (ראה פרוט בנושא בנספח א' - החרגות).

6.2. כל חריגה מהנוהל, שאינה מפורטת בנספח א', מחייבת אישור בכתב של הממונה על אבטחת מידע.

6.3. נוהל זה תקף מיום פרסומו.

<u>נספחים</u>

א. נספח א' - החרגות.

פרופ' זלמן פלמור
משנה לנשיא ומנכ"ל

נספח א' – החרגות

בעיה	פתרון
המערכת לא מאפשרת מבנה סיסמא כמפורט בסעיף 5.1 בנוהל.	יש לבדוק: • באם מתבצעים עדכוני תוכנה בכלל ועדכוני אבטחה בפרט. • האם ניתן לשדרג את גרסת המערכת. • האם ניתן לעבור למערכת מתקדמת יותר. במידה והוכח כי אין למערכת תחליף, יבדוק נאמן אבטחת המידע את האפשרות לבודד את המערכת מהרשת והאחראי על המערכת יגדיר את הסיסמא המורכבת ביותר שהמערכת מאפשרת.
האחראי על המערכת אינו יודע איך משנים הגדרות סיסמא או שאין במערכת אפשרות לשנות סיסמא.	• יש לשקול הפסקת שימוש במערכת או הפרדתה מהרשת. • יש להגביל את הגישה למערכת לכתובות/סגמנט ספציפיים ולאסור אפשרות גישה מכל כתובת אחרת.
הסיסמא כתובה בשורות הקוד של המערכת.	יש להגדיר קובץ פרמטרים מוגן כך שהסיסמא תילקח מקובץ הפרמטרים אותו ניתן לשנות בלי הצורך לשנות את הקוד. במידה והדבר בלתי אפשרי, יש לשנות את הסיסמא לסיסמא מורכבת ולהקפיד לשנותה לפחות פעם בשנה.