

## Password Standards

### Purpose

This standard identifies the minimum password requirements needed to protect Michigan Tech's data and systems. Passwords are used on University devices and systems to facilitate authentication, i.e. helping ensure that the person is who they say they are.

The security of University data is highly dependent upon the secrecy and characteristics of the password. Compromised passwords can result in loss of data, denial of service for other users, or attacks directed at other Internet users from a compromised machine. Compromised passwords can also result in the inappropriate disclosure of private data such as private student data, research participant data, and private employee data.

### Scope

These standards apply to all electronic devices and systems connected to the University network including computers, network switches and routers, personal digital assistant devices, laptop computers, password authenticated software, etc.

### Standards

The following standards set the minimum requirements for passwords on any University IT system:

1. Passwords must have a minimum length of 8 characters. On systems with a maximum password length of less than 8 characters, use the maximum length that the system supports.
2. Passwords must meet at least 3 out of the 4 requirements for quality:
  - at least 1 lower case letter
  - at least 1 upper case letter
  - at least 1 number
  - At least 1 special character (?, \*, %, etc.)
3. Password should not contain the user's first name, middle name, last name, or username.
4. Users must choose passwords that are difficult to guess.  
Passwords must not:
  - Be based on a single dictionary word
  - Contain more than 2 repetitive characters (e.g., Mmmmmmm1, Ab7777777, etc.)
5. Passwords on sensitive IT systems must be changed, at a minimum, every 90 days.
6. Passwords used within the last year must not be repeated and accordingly a history of previously used passwords will be maintained.
7. Unique initial passwords must be provided through a secure and confidential manner and initial passwords must be changed upon first logon.

8. After 5 unsuccessful consecutive logon attempts (e.g., incorrect passwords) the user's account may become automatically locked. Users must contact the Help Desk for account unlocking.
9. Passwords should never be written down and left in plain sight, or stored in plain text online. If a password must be written down it should be stored in a secured location.
10. Users must prevent passwords from being known or used by others:
  - Users must log off of applications when done using them.
  - Users must secure workstations when they are away from them. Devices will be subject to lockouts for inactivity after 10 minutes.
  - Users must never use the "Remember Password" feature of any applications.
11. Users must only use their Michigan Tech ID and password for Michigan Tech systems and services. Users should create a different username and password for external services such as personal e-mail, banks, stores, personally owned computers or other systems.
12. Users must report suspected password compromises.
  - Users must contact the Help Desk if they believe someone has obtained their password.
  - Users must change their password if they suspect it has been compromised.

### **Remote Access Users**

Remote access to information technology resources (switches, routers, computers, etc.) and to sensitive or confidential information (social security numbers, credit card numbers, bank account numbers, etc.) are only permitted through secure, authenticated and centrally-managed access methods.

### **Related Information**

Adherence to password requirements is reviewed as part of the normal University audit procedures. Michigan Tech reserves the right to suspend account holders' access to preserve the confidentiality, integrity and availability of the University's network, systems or information if found in non-compliance.

---

END OF DOCUMENT