1 PASSWORD AND AUTHENTICATION STANDARD

Title	Password and Authentication Standard
Reference	ISS-02
Status	PUBLISHED
Version	1
Date	December 2024
Review	TBD
Classification	Public

The Chief Information Officer has issued this standard under the authority of UFV's Information Security Policy. Questions about this standard may be referred to cybersecurity@ufv.ca.

2 SUMMARY

This standard is part of the University's Information Security Policy and sets out the requirements for the effective management of account password and authentication mechanisms. This management is essential to ensure that access to the University's information and information systems is restricted to authorised users.

3 SCOPE

This Policy applies to Information Assets owned by and/or entrusted to the University (including whether held by the University or by others for the University) and to all computer systems, hardware and software, and networks which the company has designated as being subject to this policy.

Whenever circumstances or technologies make immediate compliance with this policy impractical, the exception process outlined in the Information Security Policy will be used.

4 STANDARDS:

4.1 PASSWORD MANAGEMENT

As part of the account provisioning process, the account may need to be created with a temporary password. This password must be communicated to the user in a secure way and must be changed by the user immediately. This change should be enforced automatically wherever possible.

1. Access to the network/servers and systems will be by individual username and password, or by smartcard and PIN number/biometric.

2. Usernames and passwords must not be shared by users.

3. All accounts will have an alphanumeric password of at least 8 characters.

4. The user account will be locked after 3 incorrect attempts.

4.2 MULTI-FACTOR AUTHENTICATION

Due to the increased likelihood of a user's password being compromised, users may be asked to use additional methods to authenticate themselves to university systems. This is referred to as Multi-Factor Authentication (MFA). The use of MFA greatly improves the security of user's accounts along with the data and systems they access.

Information given to the University for MFA will be stored securely and only used for authentication purposes. It will be stored by the University or a University trusted provider and will not be provided to any third party without your prior written consent unless we are required to do so by law.

Two-factor authentication (TFA) or multi-factor authentication (MFA) shall be used for any services remotely accessible by personnel and/or authorized third parties (e.g. Microsoft365, VPN, etc.), unless personnel and/or authorized third parties are connected to the protected corporate network.

4.3 PASSWORD REQUIREMENTS:

Passwords should be at least 8 characters long and contain a combination of upper and lowercase letters, numbers, and special characters. Passwords should not be reused or shared with anyone else. Passwords should be changed regularly, at least every 90 days.

4.4 PASSWORD STORAGE:

Passwords should be stored securely using a password manager or a similar application. Passwords should not be stored in plain text, written down, or emailed. If a password must be written down, it should be kept in a secure location and destroyed when no longer needed.

4.5 PASSWORD SHARING:

Passwords should never be shared with anyone else, including colleagues or IT staff. If someone requires access to a system, they should be given their own unique login credentials. University IT Support Staff will never ask for Users' passphrases/passwords.

Do not respond to emails or phone calls requesting passphrases/passwords and Multi-Factor Authentication (MFA) passcodes, even if they appear to be from a trusted source. These requests are often attempts to steal Users' credentials.

4.6 DEVICE SECURITY:

Devices used to access university networks and information should be secured with passwords or other forms of authentication. Mobile devices should be password-protected and have remote wiping enabled in case of loss or theft. Users are encouraged to keep their personal devices up-to-date with security patches and software updates.

4.7 AUDIT TRAILS:

Audit trails should be implemented to track user activity and detect any unauthorized access attempts. This can help to identify security breaches and provide valuable information for investigations.

5 ACCESS CONTROL STANDARDS

5.1 RE-AUTHENTICATE USERS OR EXPIRE SESSIONS AFTER A PERIOD OF INACTIVITY.

Systems and Applications must be protected against unauthorized access by invoking time-out facilities that automatically re-authenticate users or expire the session after a predetermined period of inactivity,

5.2 ENFORCE THE STANDARDS FOR AUTHENTICATION AND PASSWORDS.

Access control mechanisms based on passwords must align with the password policy based on the application's primary users.

5.3 ENFORCE STRONGER AUTHENTICATION REQUIREMENTS FOR PRIVILEGED ACCOUNTS.

Privileged user accounts must have a maximum 30-day expiry period or use multi-factor authentication.

5.4 STORE PASSWORDS AND OTHER IDENTIFIERS SECURELY.

Sign-on mechanisms must be configured to protect authentication details against unauthorized disclosure by using approved:

a) cryptographic hashing algorithms to conceal clear text passwords and resist brute force attacks,

b) salting methods to ensure each password hash is unique.

5.5 TRANSMIT PASSWORD SECURELY OVER THE NETWORK.

Approved cryptography must be used to render all authentication credentials unreadable during transmission on all system components.

5.6 PROVIDE APPROPRIATE AUTHENTICATION CONTROLS.

Access to applications and infrastructure must be restricted by:

a) using access control mechanisms, such as passwords, tokens or biometrics,

b) ensuring that administrator consoles always require authentication before use and be restricted to system administrators.