a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD M4
Securing User Accounts

1. Introduction

1.1 User Accounts control access to UBC Electronic Information and Systems and as such they must be effectively protected against unauthorized access. This standard is closely tied to the User Account Management standard.

1.2 This document defines standards that University IT Support Staff must comply with when securing these accounts.

1.3 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Account Protection Requirements

2.1 All User Accounts must be secured with:

2.1.1 passphrases or passwords that are in compliance with the Passphrase and Password Protection standard; or

2.1.2 private keys (e.g. X.509 certificates or SSH Keys) that are generated using, at a minimum, the Mozilla Key Management Acceptable algorithms, but wherever possible, should use the Recommended algorithms.

2.2 Where technically possible, UBC Systems must enforce password complexity rules in accordance with the Passphrase and Password Protection standard.

2.3 Where technically possible, Servers and Software Applications must be protected by Multi-Factor Authentication (MFA).

2.4 Users who receive new accounts or who require a replacement password must be forced to set or change the password upon first login. Account activation or password reset links, and temporary passwords must be transmitted to Users in a secure manner and expire as follows:

Credential Change	Initiated by	Link/Password Expiration	Examples
Account Activation	Administrator or automated process	7 days	New employees, sponsored guests and prospective student accounts
	User (self-serve sign-up)	3 days	New and prospective student accounts
Password Recovery	User (self-serve)	24 hours	Applies to all Users

2.5 Procedures must be established to verify the identity of a User prior to providing a new, replacement or temporary password for an account. Identification validation procedures must follow one of the following standard practices, listed in order of preference:

2.5.1 MFA application push to the User's Multi-Factor Authentication Device (MFA Device) that must be approved by the User;

2.5.2 Validation of the answers to three questions that were previously created by the User during account creation; or

2.5.3 In-person visit by the User to present valid photo identification, preferably University or government-issued.

2.6 Default vendor passwords must be changed following the installation of systems or software.

3. Authentication System Requirements

3.1 Where possible, all User Accounts should be centrally controlled in the UBC Enterprise Active Directory, Enterprise LDAP, or Campus-wide Login.

3.2 Authentication systems for User Accounts must be adequately protected from password cracking using at least one of the following methods:

3.2.1 the account is locked for a period of time if an incorrect number of passwords/passphrases is entered over a specified time period (for example, if an incorrect password/passphrase is entered 10 times within a 30 minute window, the account will be locked for 30 minutes); and/or

3.2.2 each time an incorrect password/passphrase is entered, the system introduces a delay before providing the failure response; this delay increases as the failed login attempts continue but will reset once the User successfully logs in (for example, the delay period could begin at 100 milliseconds, and double after each subsequent failed login).

3.3 Authentication systems must not store account passwords in clear text. Where possible, passwords should be stored using a strong cryptographic hash and salted; for further guidance see Salted Password Hashing – Doing it Right.

3.4 Where possible, authenticated application sessions must timeout as follows, after which Users must reauthenticate to continue an existing session or establish a new session:

3.4.1 after a maximum session length of 12 hours; and

3.4.2 where reasonable, after 30 minutes of User inactivity.

4. Related Documents and Resources

User Account Management standard

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

Passphrase and Password Protection standard

Mozilla Key Management document

Salted Password Hashing