a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD M2
User Account Management

1. Introduction

1.1 User Accounts control access to UBC Electronic Information and Systems. This document defines standards that Information Stewards/Owners must comply with when managing these accounts throughout their lifecycle to ensure individual accountability exists and access is restricted on a 'need to know' basis. In addition to this standard, Privileged Accounts must also comply with the Privileged Account Management standard.

1.2 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. Creating User Accounts

2.1 Applications for User Accounts must be reviewed and approved by Information Steward/Owners and a record must be kept of all Users being granted these accounts and who provided authorization. This record must be retained for at least one year.

Examples of User Accounts

- FASmail
- Student and Alumni Email
- Student Information System (SIS)
- Financial Management System (FMS)
- Workspace
- Home network drive
- Login account (Active Directory or equivalent)

2.2 Service Providers applying for User Accounts must comply with the Outsourcing and Service Provider Management standard.

2.3 All User Accounts must be uniquely identifiable to a specific User.

2.4 Users must be granted the minimum level of access for their defined job function (i.e. the Principle of Least Privilege).

2.5 User Accounts must not be shared. Accounts must be traceable back to the individuals using them. This requirement does not apply to test accounts, which may be shared during the pre-production phase.

2.6 Where possible, User Accounts should be linked to sources of record that can accurately capture User status (e.g. Workday, PersonHub, SIS or other ERPs).

3. Changing User Account Access Rights

3.1 When Users' roles and responsibilities change, their access rights should be updated in a timely manner to ensure they remain aligned with the Principle of Least Privilege.

3.2 Changes to User Accounts should be documented, approved and retained by Information Stewards/Owners in the same manner as User Account requests.

4. Disabling User Accounts

4.1 All User Accounts must be disabled (i.e. access is revoked) in a timely manner, especially when the User has been terminated or the User has a Privileged Account. Accounts may be disabled by either closing the account to all Users or changing the password to restrict access by specific Users.

4.2 On Merchant Systems, User Accounts must be automatically disabled if not used for 90 days.

4.3 The information stored in disabled accounts, as well as the username, logs and other metadata for these accounts, must be retained for one year, except for the following accounts:

Account	Retention
Student Email	TBD, currently indefinite
Student Email Alias	TBD, currently indefinite
Home Drive	90 days

4.4 In cases where accounts are migrated from one authentication system to another, the original account does not need to be retained, provided all of the information in the account has been migrated to the new system.

4.5 At any time before the expiration of the relevant retention period, the account can be reinstated to the account holder where appropriate.

4.6 After the expiration of the relevant retention period, the account and the information stored within it must be securely deleted.

5. Reviewing User Accounts

5.1 Users' access rights must be reviewed at regular intervals to ensure they remain aligned with current roles and responsibilities. The frequency of the review must be risk based (e.g. access rights to High or Very High Risk Information such as Personal Health Information should be reviewed more frequently than access rights to Medium Risk Information that may not do as much harm if exposed to unauthorized individuals).

6. Security of User Accounts and Authentication Systems

6.1 University IT Support Staff must protect User Accounts in compliance with Securing User Accounts standard.

7. Related Documents and Resources

Privileged Account Management standard

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

Outsourcing and Service Provider Management standard

Securing User Accounts standard