Standard for User Account Management

Parent Policy:	*Use of Information Technology Resources*		
Standard Sponsor:	College Information Officer		
Standard Contact:	Manager, IT Security		
Stakeholders:	Okanagan College Application Owners		
Approved by:	College Information Officer		
Effective Date:	29-April-2024		
Last reviewed:	29-April-2024	Scheduled review date:	29-April-2025

1. Purpose

User accounts control access to College 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.

2. Creating User Accounts

2.1 Applications for user accounts must be reviewed and approved by application 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.

2.2 All user accounts must be uniquely identifiable to a specific user.

2.3 Users must be granted the minimum level of access for their defined job function (i.e. the principle of least privilege).

2.4 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.

2.5 Where possible, user accounts should be linked to sources of record that can accurately capture user role (e.g. Banner, POST, Azure, or other enterprise systems).

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 application stewards/owners in the same manner as user account requests.

3.3 When users are on long-term leave or when there is no expectation of work responsibilities, access rights should be temporarily adjusted to reflect their inactive status, ensuring they only retain necessary access

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.

a) Accounts may also be disabled when there are no expectations of work duties. Examples include long-term leaves and pre-retirement. This ensures security and compliance during periods of inactivity.

4.2 On merchant systems, user accounts must be scheduled to be disabled at a certain date or after a defined period of inactivity.

4.3 The information stored in disabled accounts must comply with the Records Classification and Retention Schedule.

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 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).

History / Revisions

Date	Action
2024-04-29	*New Standard Approved by: College Information Officer*