INFORMATION SECURITY STANDARD #11
User Account Management

Introduction
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.

2. The Chief Information Officer has issued this document under the authority of Policy 104, **Acceptable Use and Security of UBC Electronic Information and Systems**. Questions about this standard may be referred to information.security@ubc.ca.

Creating User Accounts
3. Applications for User Accounts must be reviewed and approved 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.

4. **Service Providers** applying for User Accounts must comply with the **Outsourcing and Service Provider Access** standard.

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

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

7. 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.

8. Where possible, User Accounts should be linked to sources of record that can accurately capture User status (e.g. HRMS, SIS).

Changing User Account Access Rights
9. When Users’ roles and responsibilities change, their access rights should be updated in a timely manner to ensure they remain aligned with the “least privilege” principle.

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

Disabling User Accounts
11. 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.

12. On **Merchant Systems**, User accounts must be automatically disabled if not used for 90 days.

13. 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:

<table>
<thead>
<tr>
<th>Account</th>
<th>Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student Email</td>
<td>TBD, currently indefinite</td>
</tr>
<tr>
<td>Student Email Alias</td>
<td>TBD, currently indefinite</td>
</tr>
<tr>
<td>Home Drive</td>
<td>90 days</td>
</tr>
</tbody>
</table>
14. 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.

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

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

**Reviewing User Accounts**

17. 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 Confidential Information such as personal health information should be reviewed more frequently than access rights to Sensitive Information that may not do as much harm if exposed to unauthorized individuals).

**Security of User Accounts and Authentication Systems**


**Related Documents**

- [Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems](#)
- [Outsourcing and Service Provider Access standard](#)
- [Privileged Account Management standard](#)
- [Securing User Accounts standard](#)