INFORMATION SECURITY PROCEDURE

Authorization for Privileged Account Access

Introduction

1. Access to Privileged Accounts must always be approved by the relevant Information Steward/Owner, either manually or through automated rules approved by that Information Steward/Owner using the authorization process described below.
2. This procedure has been issued by the Chief Information Officer to supplement the Privileged Account Management standard. Compliance with this procedure is mandatory. Questions about this procedure may be referred to information.security@ubc.ca.

Considerations for Granting Privileged Access

3. A User must only be granted Privileged Access for one of the following reasons:
   a. the User is automatically entitled to such access by virtue of their job; or
   b. in other exceptional cases where the Information Steward/Owner decides that the User requires access to fulfil their duties.

Automatic Entitlement to Privileged Access

4. Users are automatically entitled to privileged access in one of the following situations:
   a. their role entitles them to have Privileged Personal Accounts, i.e. named admin accounts (e.g. jsmith.admin); or
   b. they have a role that allows them to temporarily elevate their privileges by using a tool such as sudo or runas.

Exceptional Granting of Privileged Access

5. In exceptional situations, the Information Steward/Owner may grant Users Privileged Access as long as the User requires such access to fulfil their duties.

Recordkeeping

6. In all cases, Information Stewards/Owners must maintain a log of all authorizations for auditing purposes.

Related Documents

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems
Privileged Account Management standard