a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD M3
Privileged Account Management

1. Introduction

1.1 Privileged Accounts provide a very high degree of access to UBC Electronic Information and Systems and therefore pose a significant risk if used in an unauthorized manner.

1.2 This standard establishes requirements for the management and use of Privileged Accounts. Unless otherwise stated, Privileged Accounts are subject to the same requirements as User Accounts, as set out in the User Account Management standard. The purpose of this standard is to highlight the different or enhanced security controls that must be in place to protect Privileged Accounts.

1.3 The Administrative Head of Unit, in consultation with the Technical Owner of the UBC System is responsible for compliance with this standard.

1.4 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. Types of Privileged Accounts

2.1 Privileged Accounts are usually categorized into the following types:

Privileged Account Type	Description
Named Privileged Accounts	
Privileged Personal Accounts	Privileged Accounts assigned to unique individual Users (usually University IT Support Staff). Examples include the following privileged groups which Users are added to in order to elevate their privileges to the associated group access levels: DBA user, Exchange Admins, Domain Admins.
Unnamed Privileged Accounts	
Generic/Shared Administrative Accounts	Privileged Accounts that exist in virtually every device or software application; these accounts hold “super user” privileges and are often shared among University IT Support Staff. These accounts may be used by multiple Users. Examples: Windows Administrator, UNIX root, Oracle SYS, SA.
Service Accounts	Privileged Accounts that provide a security context to a running service, daemon or process, such as a file server, web server, email server, etc., or are used by applications to access databases and other applications; these accounts typically have broad access to underlying business information in databases. Also called: app2app accounts, as they are used by one application to sign into another.
Emergency Accounts	Generic Privileged Accounts used by the enterprise when elevated privileges are required for business continuity, disaster recovery, or to fix urgent problems. These accounts may be used by multiple Users. Also called: break-glass accounts, fire-call IDs.

3. Creating Privileged Accounts

3.1 Unnamed Privileged Accounts may be shared between multiple Users. However, for all privileged account types, a single individual must be assigned with accountability for the security of the account.

3.2 Approval procedures for granting access to Privileged Accounts are set out in Authorization for Privileged Account Access procedure.

4. Protecting Privileged Account Passphrases, Passwords and SSH Keys

4.1 Passphrases and passwords for Privileged Personal Accounts and Generic/Shared Administrative Accounts must be changed regularly, in compliance with the Passphrase and Password Protection

standard, or at an interval stipulated by the Technical Owner (in consultation with the Administrative Head of Unit).

4.2 Service Accounts must not be shared between applications or services, i.e. a separate account must be created for each application/service.

4.3 When private keys are used with Privileged Accounts, they must be protected in compliance with the Passphrase and Password Protection standard, except when used with Service Accounts, it is reasonable to use passphrase-less keys.

4.3.1 Private user keys must never be copied to another system than your own Workstation/personal physical disks/tokens.

4.3.2 Private machine keys must be protected as follows, except when used with Service Accounts:

4.3.2.1 the recommended settings are identical to the user keys;

4.3.2.2 the keys must be accessible only by the admin user (root) and/or the system user requiring access;

4.3.2.3 usage of machine keys should be registered in an inventory (a wiki page, LDAP, an inventory database), to allow for rapid auditing of key usage across an infrastructure;

4.3.2.4 the machine keys should be unique per usage. Each new usage (different service, different script called, etc.) should use a new, different key;

4.3.2.5 only used when strictly necessary; and

4.3.2.6 restrict privileges of the account (i.e. no root or “sudoer” machine account).

4.3.3 For additional guidance, refer to the Mozilla OpenSSH configuration document.

4.4 Passwords for Unnamed Privileged Accounts should be machine generated and held securely in a Privileged Access Management (PAM) service in compliance with the policies of the PAM service, available to system administrators in the case of an emergency through a Break Glass Procedure created by the Technical Owner (in consultation with the Administrative Head of Unit). This requirement is mandatory for Unnamed Privileged Accounts used with ERPs.

4.5 A Break Glass Procedure (which draws its name from breaking the glass to pull a fire alarm) refers to a quick means for a person who does not have access to a Privileged Account to gain access in an emergency. When a Break Glass Procedure is used, access to the Privileged Account must be:

4.5.1 limited to the minimum amount of time necessary;

4.5.2 associated to a change, problem or incident number/ticket;

4.5.3 recorded by the specific database, system, or application; and

4.5.4 logged in an auditable record (which identifies the individual User who ‘broke the glass’) for later review.

4.6 After a Break Glass Procedure has been completed, the password for the Privileged Account must be changed.

5. Logging Privileged Accounts

5.1 There are special requirements for logging Privileged Account activity, which are set out in the Logging and Monitoring of UBC Systems standard.

6. Reviewing Privileged Accounts

6.1 Access to Privileged Accounts must be reviewed at an interval stipulated by the Technical Owner of the UBC System (in consultation with the Administrative Head of Unit), or at a minimum annually, to validate that they remain restricted to authorized personnel. Discrepancies must be reported in a in a timely manner to the Technical Owner for resolution.

7. Responsibilities of Users with Access to Privileged Accounts

7.1 As Privileged Accounts provide a significant level of control over UBC Electronic Information and Systems, individuals with access to these accounts are expected to exercise a higher degree of caution than for User Accounts.

7.2 All Users with access to Privileged Accounts must maintain the confidentiality of any information that they have access to both during, and after, their employment with UBC.

7.3 All Users with access to Privileged Accounts:

7.3.1 must not use Privileged Accounts for day-to-day activities, such as email and web browsing;

7.3.2 wherever possible, must not use Privileged Accounts (except Service Accounts) to run daemons, services or applications.

7.4 University IT Support Staff with access to Privileged Accounts, and all IT professionals must also comply with the System Administrators' Code of Ethics.

8. Related Documents and Resources

User Account Management standard

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

Authorization for Privileged Account Access procedure

Passphrase and Password Protection standard

Mozilla OpenSSH Guidance

Logging and Monitoring of UBC Systems standard

System Administrators' Code of Ethics