a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD M8
Logging and Monitoring of UBC Systems

1. Introduction

1.1 Effective logging and monitoring procedures (i.e. continual monitoring and/or periodic reviews) provide ongoing assurance that UBC Systems and the UBC Electronic Information that they hold are secure, and that confidentiality and integrity are effectively being ensured. In the event of a security breach, audit logs are relied upon to determine whether or not information has been accessed or modified without authority.

1.2 The nature and frequency of logging and monitoring procedures must be based upon the sensitivity of the information stored in the system and the potential impact of a security breach upon the University and affected individuals. It is only necessary to implement logging and monitoring at a level that will reasonably identify unauthorized access to UBC Systems and UBC Electronic Information in a timely manner. Logging and monitoring should be considered at the operating system, database and/or application level.

1.3 This standard defines requirements for effective logging and monitoring of UBC Systems and UBC Electronic Information for security purposes. Unless otherwise stated in this document, University IT Support Staff are responsible for ensuring compliance with these standards. In addition, Information Stewards/Owners are responsible for ensuring that logging and monitoring procedures are adequate for securing the information they are responsible for. ERPs, Merchant Systems and EMRs must be compliant with this standard; it is recommended that all other UBC Systems comply 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. Logging and Monitoring Requirements

2.1 The following key activities must be logged:

2.1.1 User login, logout and access to a resource;

2.1.2 action performed by the User and the time it was performed; and

2.1.3 where feasible, any access to, or modification of, records.

2.2 Logs should be configured to record system faults that are potential indicators for detecting attacks against UBC Systems or other unauthorized activity.

2.3 Logs provide valuable information that can be used to validate the integrity and confidentiality of UBC Electronic Information; to be effective, logs must be:

2.3.1 retained for at least 90 days (except for ERP logs, which must be retained for at least 365 days) and regularly backed up whenever possible, preferably to offsite secure storage;

2.3.2 retrievable in a timely manner if they are required for analysis; and

2.3.3 protected against unauthorized access and modification, preferably by locating them on a separate server outside the Demilitarized Zone (DMZ), such as a Database Server protected by a firewall, and restricting access as necessary; no-one should be able to change or delete log information.

2.4 Logs should be monitored to determine the use of system resources and to detect information security events (e.g. failed logons, simultaneous logins from different geographic locations, escalation of privilege, attacks against systems, etc.). Monitoring software should be configured to send an alert to responsible University IT Support Staff when appropriate.

2.5 Accurate logs are dependent on accurate time. Systems containing or processing High or Very High Risk Information must be set to synchronize their clocks with a reliable source. UBC's DNS servers act as the University's (Time synchronization) NTP servers. These are synchronized to an external time source, ntp.org; all Users and University IT Support Staff should use these or an equivalent service as a time synchronization source. More details on this service can be found on the myDNS Overview page.

3. Additional Requirements for Privileged Accounts

3.1 University IT Support Staff must ensure that logs are kept of the usage of all Privileged Accounts. Key activity to be logged must include the following:

3.1.1 login, logout and the identity of the User, if known;

3.1.2 action performed and the time it was performed;

3.1.3 where feasible, any access to, or modification of, UBC Electronic Information; and

3.1.4 any other information that the Information Stewards/Owners decide should be captured in order to protect high risk files.

3.2 Logs of Privileged Account activity must be reviewed on a regular basis to detect information security events and determine if further investigation is required; where feasible this should be automated. Investigations should be reported to the Information Steward/Owner as required.

3.3 Where appropriate, Privileged Account logging systems must automatically transmit alerts of significant activities to the technology owner (typically a manager of a University IT Support Staff team). The following activities must always trigger an alert:

3.3.1 escalation of privilege; and/or

3.3.2 usage of the Break Glass Procedure as described in the Privileged Account Management standard.

4. Additional Requirements for Merchant Systems

4.1 For all Merchant Systems processing PCI Information, there is a requirement that logs be maintained for the following events:

4.1.1 which particular record was accessed;

4.1.2 which User accessed the record; and

4.1.3 the time the User accessed the record.

4.2 Logs of access to PCI Information should be retained for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).

5. Use and Disclosure of Logs

5.1 Logs are generally intended to be used for maintenance and troubleshooting, as well as detecting and investigating information security events. Access for other purposes must be approved using one of the following methods:

5.1.1 internally, within UBC, in accordance with the Accessing Electronic Accounts and Records standard;

5.1.2 externally to law enforcement via Campus Security; or

5.1.3 externally to other entities via authorization from the Office of the University Counsel.

6. Related Documents and Resources

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

UBC IT myDNS

Privileged Account Management standard

Accessing Electronic Accounts and Records standard