Information Services Log Management Standard

Version:	0.4
Published:	Jan 17 2025
Published By:	Information Security Office - is.security@uregina.ca
Approved By:	AVP, Information Services
Approval Date:	Feb. 6, 2018

1. Introduction

The following standard is intended to direct information technology application and infrastructure owners at the University of Regina in order to ensure their systems are capturing and retaining critical events to support information security monitoring and forensics.

Effective logging standards assist in providing assurance that data is managed in order to preserve confidentiality, integrality and availability. Should an information security incident be suspected, logs must be analyzed and audited to determine if a risk was realized. Therefore, logs must be retained, accessible, and monitored to support such information assurance objectives.

This policy is issued under the authority of University of Regina Policy OPS-080-005 *Use of Computer and Network Systems.* Policy OPS-080-005 requires the University preserve the integrity of the systems and data against unauthorized or improper use through the process of examining logs.

2. Scope

This standard determines the requirements of effective logging for security purposes. While logging may support other information technology purposes, such as debugging or troubleshooting, this standard is focused on information security.

University of Regina Information Services staff are required to ensure compliance with this standard for systems under Information Services custodianship or ownership, excluding endpoint devices. This standard covers applications and infrastructure associated with the provisioning of services from the Information Services department.

Otherwise, application and infrastructure owners and/or operators outside of Information Services are responsible for ensuring their logging standards are adequate for providing assurance and security for the information they are responsible for. However, this standard forms the recommended enterprise logging guideline for University IT systems.

3. Log Configuration Standard

3.1. Events Required to be Logged

3.1.1. User authentication and/or user authorization, user logout or session termination

3.1.1.1. Both failed and successful authentications are to be logged.

3.1.2. Creation, updates, revocation or deletion of authorizations or permissions, including passwords, PINs, keys; or granting, altering, or removing a privilege, role, or right. For example: creation of new users, assigning new user rights, adding a user to a group, changing file permissions, changing application permissions, changing firewall rules, and user password changes.

3.1.3. Detection of suspicious/malicious activity such as from malware detection or intrusion prevention or detection system.
3.1.4. Initiate or accept a network connection. i.e. remote access session accepted, new web application session accepted.

3.2. Events Recommended to be Logged

Other types of events to be logged must be determined for each system taking into account an evaluation of risk, cost and performance of the system.

3.2.1. System, network, or services configuration changes, including installation of software patches, updates or other installed software changes.
3.2.2. Application processes start, shutdown, or restart, including failure, abort, or abnormal termination.
3.2.3. Use of elevated privileges.
3.2.4. Additional events as identified by vendor or system administrator which are related to security.

3.3. Required Elements of Event

Events within logs must contain sufficient information to determine what occurred, where they occurred (source and destination), and outcomes of events. For each event, the following should be recorded, as appropriate for the type of event:

3.3.1. Timestamp with sufficient granularity to support event sequencing and correlation.
3.3.2. Action type including ‘what’ occurred, such as authorize, create, read, update, delete. Required to include whether an action outcome (allowed/successful or denied/failed).
3.3.3. Subject Identifiers: including username, computer name, remote IP Address, and media access control address. As many identifiers as possible should be included for the subject requesting the action. Typically, this is an end user or remote system connecting to a service.
3.3.4. Object Identifiers: including records or resources accessed, query and parameters, service, system, subsystem, application, IP address, network port, protocol, hostname, and media access control. As many identifiers as required should be included in order to uniquely identify the resource and system where each event originates from or occurs on.

3.4. Prohibited Elements in Logs

3.4.1. Logs should not, by design, include:
3.4.1.1. Passwords, keys, or other private authentication mechanisms
3.4.1.2. Connection strings or community strings
3.4.1.3. Sensitive, personally identifiable information
3.4.2. If these elements predictably exist within logs, they should be masked, hashed, or anonymized.

3.5. Timestamp Requirements

3.5.1. Where supported, University of Regina provided Network Time Protocol (NTP) services should be utilized to ensure time stamp synchronization. Regular synchronization shall occur. The use of Linux ntpd daemon rather than scheduled synchronization is recommended.
3.5.2. Event timestamp format should be consistent across a log source and should include time zone if not in local time or Unix epoch time.

3.5.3. Timestamp should indicate time of event occurrence, not the time an event was written to a log file or is written to remote log server.

3.6. Centralization Requirements

3.6.1. Authentication management systems and services must send authentication logging to the centralized log management platform. This includes, but is not limited to, e-Directory/LDAP instances, CAS, Shibboleth/SAML, Radius, Active Directory, Banner, password management applications and identity management systems.

3.6.2. If local, on-device logging cannot service requirements in this standard such as retention, monitoring, analysis, and protection against unauthorized access and modification, centralization of the logging is recommended. However, security related events are to remain the focus of the centralized log platform. Thus, events considered for centralized logging must undergo an evaluation of risk, cost and performance to ensure they service information security.

3.6.3. If logging is utilized or monitoring is performed by resources who would not normally have access to the local logs, centralization is recommended as a mechanism to grant auditable access to logs. Centralization is preferred over granting privileges to local log files.

4. Log Monitoring and Analysis Standard

4.1. Logs are required to be regularly monitored for completeness and retention.

4.2. Where logs are centralized, they are required to be analyzed for identification of anomalies and security events.

4.3. Where evidence of an information security incident is discovered, such events must be reported to the Information Security Office.

4.4. Log monitoring and analysis tools or processes should not alter original log records, except in support of 3.4.2.

5. Log Retention and Use Standard

5.1. Retention, Storage and Retrieval

5.1.1. Logs should, wherever practical, be stored for a minimum of 120 days.

5.1.2. Logs should, wherever practical, be backed up as part of the systems backup and/or as part of centralized logging.

5.1.3. Logs should be retrievable for analysis in a timely manner with a target goal of one business day. Preferably, this is achieved by storing logs within the enterprise centralized logging platform.

5.1.4. Logs must be protected against unauthorized access and modification. Preferably, this is achieved, in part, by storing the logs separately from the source system. Sending logs to the consolidated log platform is the recommended method of compliance.

5.2. Use, Disclosure and Disposal of Logs

5.2.1. Logs should only be used for the purposes for which they are originally collected. For the purposes of this standard, use cases are limited to operations, maintenance and information security purposes.

5.2.2. Logs cannot be shared or disclosed except within Information Services or with the applicable Service Agreement’s authorized representative(s) without approval.

5.2.3. Unapproved or unintentional disclosure of confidential information recorded in logs should be reported to the AVP, Information Services.

5.2.4. Approval for sharing, disclosure, or alternative use cases which fall outside original purposes are to be approved by AVP, Information Services.

5.2.5. When appropriate, logs are to be securely disposed.

5.3. Other Governance Requirements

5.3.1. Other contractual, regulatory, legislative, or policy obligations may have more stringent requirements which can exceed the logging requirement of this standard. For example, Records and Information Management Retention schedules may require log records to be retained for a period greater than stipulated in this standard.

6. Exceptions

If an in-scope infrastructure component, application, or service is unable to comply with the requirements of this standard, other security measures must be implemented to ensure that the overall level of security is consistent with the intent of this standard. Exceptions to this standard must receive written approval from the AVP Information Services or designate. Non-compliance with this standard may result in revocation of system or network access, or the notification of applicable supervisors.

Related Information:

- Use of Computer and Network Systems Policy OPS-080-005: https://www.uregina.ca/policy/browse-policy/policy-OPS-080-005.html
- Time Services: https://www.uregina.ca/is/infrastructure/network/technotes/504.html
- Records and Information Management Records Schedule: https://www.uregina.ca/library/rim/schedules/index.html

Revision History:

Version	Version Date	Status	Summary of Change	Author
0.1	Nov. 5, 2017	Draft	Initial version	R. Jesse
0.2	Dec. 11, 2017	Draft	Revisions to reduce log monitoring requirements.	R. Jesse
0.3	Feb. 5, 2018	Draft	Inclusive of feedback from stakeholders.	R. Jesse
0.4	Feb. 6, 2018	Final Draft	Editorial updates from A. Exner	R. Jesse