Standard for Information Technology Logging

1. Purpose

Logging is an essential information security control that is used to identify, respond, and prevent operational problems, security incidents, policy violations, fraudulent activity; optimize system and application performance; assist in business recovery activities; and, in many cases, comply with federal, state, and local laws and regulations. The purpose of this standard is to define logging expectations and requirements for information technology (IT) systems. University organizational units (departments, institutes, centers, and others) bear the responsibility for documenting their adherence to and departure from this standard.

2. Scope

This standard applies to any university-owned IT resource or service that stores, processes, or transmits *high risk* or *moderate risk* university data regardless of where it is hosted. Additionally, this includes any IT resources or services identified by the IT Security Office as important to security operations.

The standard also applies to end-user devices that are critical to the operation and maintenance of high-risk IT systems. Examples of high risk *end-user devices* include desktops or laptops used to make configuration changes to production servers, databases, or applications and desktops or laptops used to assign or update IDs and passwords for other users. These end-user system logs should be treated the same as the logs of the servers with which they interface.

3. Standard

All systems that are in-scope shall record and retain audit-logging information sufficient to answer the following questions:

1. What activity was performed?
2. Who or what performed the activity, including from where or on what system the activity was performed (subject)?
3. On what the activity was performed (object)?
4. When was the activity performed?
5. With what tool(s) was the activity performed?
6. What was the status (such as success vs. failure), outcome, or result of the activity?

3.1. Activities to be Logged

Therefore, logs shall be created whenever any of the following activities are requested to be performed by the system:

1. Create, read, update, or delete high risk information, including authentication information such as passwords;
2. Create, update, or delete *moderate risk* information not covered in #1;
3. Initiate a network connection;
4. Accept a network connection;
5. User authentication and authorization for activities covered in #1 or #2 such as user login and logout;

6. Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes;
7. System, network, or services configuration changes, including installation of software; patches and updates, or other installed software changes;
8. Application process startup, shutdown, or restart;
9. Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault; and
10. Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

Logging additional items may be deemed necessary for higher risk or business critical systems at the discretion of the system administrator and IT Security Office.

3.2. Elements of the Log

Such logs shall identify or contain at least the following elements, directly or indirectly. In this context, the term “indirectly” means unambiguously inferred.

1. Type of action – examples include authorize, create, read, update, delete, and accept network connection.
2. Subsystem performing the action – examples include process or transaction name, process or transaction identifier.
3. Identifiers (as many as available) for the subject requesting the action – examples include user name, computer name, IP address, and MAC address. Note that such identifiers should be standardized to facilitate log correlation.
4. Identifiers (as many as available) for the object the action was performed on – examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
5. Before and after values when action involves updating a data element, if feasible.
6. Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time.
7. Whether the action was allowed or denied by access-control mechanisms.
8. Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

3.3. Formatting and Storage

The system shall support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. Mechanisms known to support these goals include, but are not limited to, the following:

1. Microsoft Windows Event Logs collected by a centralized log management system;
2. Logs in a well-documented format sent via syslog, syslog-ng, or syslog-reliable network protocols to a centralized log management system;
3. Logs stored in an ANSI-SQL database that itself generates audit logs in compliance with the requirements of this document; and

4. Other open logging mechanisms supporting the above requirements.

Whenever possible, departments should use the university's Central Log Service managed by the Division of IT. The departments and units within the Division of IT are required to use the Central Log Service but may use other tools in addition, but not instead of the Central Log Service.

3.4. Log Review

Log review is the responsibility of the service provider as applicable. Logs produced by university IT resources should be examined regularly to protect university IT resources and data. At a minimum, systems containing *high risk data* should have their logs reviewed weekly or more frequently if required by law, regulation, contract provisions, or industry standards. Logs must be reviewed within a 24-hour period in response to suspected or reported security problems on systems or as requested by the Information Technology Security Office. Additionally, departments must be able to generate a list of users with access to the logs.

Individuals shall not be allowed to be the sole reviewers of their own activity.

3.5. Log Retention

By default, logs will be retained no longer than six months. Exceptions to this will be allowed by recommendation from the IT Security Office or other Vice President for IT designee when different log retention requirements are mandated by university policy; federal, state, or local laws; or regulations.

4. Enforcement

It is the responsibility of service providers to ensure that the controls described in this document are implemented.

University departments undergo periodic audits. These audits sometimes include an analysis of the processes and controls used by departments to secure and manage end user devices, servers, and applications. The department is responsible for remediation of any findings of noncompliance with this standard within the time frame agreed to with the auditors.

Any exception to this standard must be approved by the Information Technology Security Office.

5. Definitions

End-user device: desktop, laptop, tablet, mobile or other networked device which a person directly interacts with.

High risk data: See Virginia Tech Risk Classification Standard

Moderate risk data: See Virginia Tech Risk Classification Standard

6. References

Policy 7100, Administrative Data Management and Access Policy
http://www.policies.vt.edu/7100.pdf
Standard for administrative data management
http://it.vt.edu/content/dam/it_vt_edu/policies/AdministrativeDataManagementStandard.pdf

Virginia Tech Risk Classification Standard
http://it.vt.edu/content/dam/it_vt_edu/policies/Virginia-Tech-Risk-Classifications.pdf

Minimum Security Standard
http://it.vt.edu/content/dam/it_vt_edu/policies/Minimum-Security-Standards.pdf

Policy 7010, Policy for Securing Technology Resources and Services
http://www.policies.vt.edu/7010.pdf

SANS Information System Audit Logging Requirements
https://www.sans.org/security-resources/policies/server-security/pdf/information-logging-standard

NIST SP 800-92, Guide to Computer Security Log Management
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

Policy 2000, Management of University Records
http://www.policies.vt.edu/2000.pdf

Policy 7105, Policy for Protecting University Information in Digital Form
http://www.policies.vt.edu/7105.pdf

The University IT Security Officer is responsible for this IT Standard. Questions may be directed to itso@vt.edu.

7. Revision History

11/1/2017 – standard creation by Philip Kobezak.

7/1/2020 –Sect. 3.5 revised to indicate the maximum retention period (6 month) unless otherwise mandated by University policy, federal/state laws or regulations.