PURDUE UNIVERSITY

BASIC LOGGING STANDARD

Developed to support the implementation of the IT Resource Logging Policy (VII.B.5).

Issued March 1, 2010 from Purdue University Security Officer's Group and IT Networks and Security. Questions about this standard can be addressed to itap-securityhelp@purdue.edu.

I. Introduction:

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.

This standard applies to all logging activities developed in support of the IT Resource Logging Policy (V.1.7).

II. Logging Standards:

Log Detail:

Centralized and departmental IT units and IT Resource owners or other designated individuals have some flexibility in determining the detail contained in logs of IT Resources within their areas of responsibility. The detail of information contained in an IT Resource log depends on the risks to the relevant IT Resource and underlying data and shall be commensurate with a particular system's profiled data classification category (e.g., it may be appropriate to have more log detail captured on a system that processes restricted data as opposed to a system that processes only public data).

Factors used to help determine the detail of information in an IT Resource log includes:

- Criticality of the IT Resource or underlying data
- Type of data and its classification stored on the IT Resource
- Past experience of IT Resource vulnerability, exploitation, and/or misuse
- Extent of system interconnectedness
- The primary purpose of logging on the IT Resource
- Effects on system performance
- Costs of logging and reviewing log data

When relevant, University IT Resource logs should include:

- User IDs or other identification mechanism
- Dates, times, and details of events key to the operation of the IT Resource
- Records of successful and rejected system access attempts
- Records of successful and rejected access to University data and other IT Resources
- Changes to IT Resource system configuration
- Use of privileged access or operations (to include the use of privileged accounts)

- Use of system utilities and applications
- Files accessed and the kinds of access
- Source and target network addresses and protocol details
- Alarms raised by University IT Resources (e.g., console alerts or messages; system log exceptions; network management alarms; alarms raised by access control systems)
- Activation and deactivation of protection systems such as anti-virus, intrusion detection , and file integrity systems

All University IT Resource logs must include:

- A timestamp. It is expected that the system's clock is synchronized using an application such as the Network Time Protocol (NTP) Service.

The following information must never be included in a University IT Resource log:

- Social Security Numbers
- Unencrypted personal information (e.g., personal account numbers, financial account numbers, credit card numbers, etc.)
- Cleartext authentication credentials (e.g., passwords)

Log Review:

Logs produced by University IT Resources must be examined on a regular basis in order to protect University IT Resources and data. Frequency and nature of log monitoring and review depends on the risks to the relevant IT Resource and underlying data and shall be commensurate with a particular system's profiled data classification category.

Factors used to help determine the time period for review of logging activities include:

- Criticality of the IT Resource or underlying data
- Type of data and its classification stored on the IT Resource
- Past experience of IT Resource vulnerability, exploitation, and/or misuse
- Extent of system interconnectedness
- The primary purpose of logging on the IT Resource

Log Integrity:

Logging facilities and log information should be protected against tampering, modification, destruction, and unauthorized access. Where possible, system administrators should not have permission to erase, deactivate, or modify logs of their own activities.

Log Classification and Handling:

University IT Resource logs may contain operational and/or confidential data, and must be classified and handled in a manner that is consistent with such data's classification according to the University's Data Classification system and Data Handling Requirements. The proper handling requirements for any IT Resource log must, at a minimum, match the highest classification of data which is contained in the log.

University IT Resource owners and/or other designated individuals responsible for implementing the IT Resource Logging Policy and related standards may elevate the data classification of logs within their areas of responsibility if there are special departmental circumstances that require an increased classification and handling requirement.

Log Retention:

Some logs may be required to be archived as part of the University's records retention policy or because of requirements to collect and retain evidence. University policy, departmental policy, and federal, state, or local laws may also specify minimum retention requirements for certain types of logs and log data. Where applicable, those retention requirements must be followed.

In all other instances where no retention requirement applies, University IT Resource owners and/or other designated individuals responsible for implementing the IT Resource Logging Policy and related standards may designate an appropriate retention period for logs produced by University IT Resources within their areas of responsibility.

III. Compliance

Centralized and departmental IT units and IT Resource owners or other designated individuals are responsible for ensuring appropriate compliance with this standard on University IT Resources within their areas of responsibility.

Additionally, centralized and departmental IT units and IT Resource owners or other designated individuals are responsible for documenting appropriate compliance with this standard on University IT Resources within their areas of responsibility. Documentation should include the type of logging taking place on IT Resources, data classification of the logs, retention periods for the relevant logs, frequency of log review, and brief justification of the detail of information contained in an IT Resource log and the reason that detail is being captured. Documented processes should be periodically reviewed to ensure continued compliance with the IT Resource Logging Policy and this standard.

IV. Related References

- University IT Policies are available at: http://www.purdue.edu/policies/information-technology.html
- Standards supporting the implementation of this and other University IT Policies are available at: http://www.purdue.edu/securepurdue/bestPractices/
- Purdue University Data Classification and Handling Requirements, available at: http://www.purdue.edu/securepurdue/bestPractices/dataClass.cfm

Revised November 21, 2011 to update URLs.