FLORIDA	**OFFICIAL**
POLYTECHNIC	**TECHNOLOGY SERVICES**
UNIVERSITY	**STANDARD**

Subject/Title: Technology Services Logging and Monitoring Standard
Date Last Revised: 2019.12.24
Responsible Division/Department: Technology Services
Initiating Authority: Ben Beachy, Chief Information Officer

A. STANDARD PURPOSE

This standard is to ensure that University systems are monitored and activity on them is logged to reduce risks to the confidentiality, integrity, and availability of University data. This standard describes expectations for IT staff, University employees, and contractors.

B. STANDARD SCOPE

This standard applies to all information systems used for official University business. An information technology system is a combination of software, hardware, storage, telecommunication, and/or automated processes that generate value for the University.

C. STANDARD CONTEXT

Florida State law and FPU-1.0123P – University Public Records require that most University records be made available to public inspection. This legal requirement effectively dispenses with concerns for the confidentiality of public University records. Integrity and availability remain pertinent concerns, however; as does the confidentiality of those few records exempted from public disclosure. The requirements of this standard reflect this regulatory context.

STANDARD REVIEW

This standard must be reviewed at least once annually by the standard owner. It may be modified at any time by the standard owner. Any changes to this standard will be promptly reviewed with affected employees.

D. STANDARD

Critical activity

Critical activity that must be logged on all systems includes but is not limited to:

- Authentication events, whether successful or not
- Changes to authentication or authorization configuration
- Privilege elevation and use of elevated privileges
- Access to restricted or highly restricted data

Additions to this list are noted below where appropriate.

Other activity may be logged to assist with troubleshooting, capacity planning, resource allocation, and other University functions.

Logged details

Where possible logs should include the following information about the logged event:

- Date-time of event
- Description of event
- Source and destination of event
- User or process triggering event
- Success or failure of event
- Data affected by event
- Access control rules evaluated before event

Log collection

Where technically practical all logs should be collected in a single system, separate from the system generating the log, to facilitate performance monitoring, threat detection, forensic exploration, and other activities.

For vendor-managed systems

Where practical, the University transfers responsibility for collecting logs to vendors managing Software as a Service (SAAS) offerings. These vendor's policies and practices are evaluated consistent with our current risk management practices. The details of vendors policies and practices are maintained by the vendors.

For workstations

Critical activity on University workstations must be logged; all activity may be logged.

For networking and telecommunications

Critical activity on to University networks and telecommunications systems must be logged; all activity should be logged.

For network and telecommunications systems, critical activity includes that defined above and:

- Changes to access rules
- Rebooting and restarting devices and services

For servers and applications

Critical activity on University servers and server applications must be logged; all activity should be logged.

For servers and high-risk server applications, critical activity includes that defined above and:

- Changes to scripted business processes, workflows, and/or integrations
- Rebooting and restarting servers and services

For computing classrooms and computer labs

Critical activity on systems used in University computing classrooms and computer labs must be logged; all activity may be logged.

Log review

Logs must be regularly reviewed by knowledgeable staff. This review should look for threats to the confidentiality, integrity, and availability of University data. Automated tools should be used to make log review, analysis, and monitoring more efficient.

Log review frequency aligns with the evaluated information security risk of the relevant system:

- For systems with high risk: critical activity logs must be reviewed daily; other logs should be reviewed monthly.
- For systems with moderate risk: critical activity logs must be reviewed monthly; other logs should be reviewed every six months.
- For systems with low risk: critical activity logs must be reviewed monthly; other logs may be reviewed as needed.

Log protection

Logs are highly restricted data and must be secured against unauthorized access or alteration.

Technology Systems is the data steward for all log data.

Log retention

Logs must be retained to a sufficient time to support mandatory review, incident reporting, threat detection, trend analysis, and other University functions.

E. RESPONSIBILITIES

Technology systems is responsible for configuring systems to log critical activity, except where such responsibility has been transferred to SAAS vendors (see above).

F. CHANGES

2019.12.24 Ben Beachy. First version.