PURPOSE

Establish procedures and policies for auditing and accountability of information systems.

PROCESS

Audit and Accountability Policy and Procedures (AU-01)

Temple College develops, disseminates, and periodically reviews/updates formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

The Chief Information Security Officer (CISO) in coordination with the Division Director of Information Technology and the information resource owners must develop document and disseminate controls addressing the Audit and Accountability of information resources.

The Chief Information Security Officer (CISO) and the Division Director of Information Technology must review and update these controls as necessary.

Audit Events (AU-02)

Information resources systems must provide the means whereby authorized personnel have the ability to audit and establish individual accountability for any action that can potentially cause access to, generation of, modification of, or affect the release of confidential information.

Appropriate audit trails must be maintained to provide accountability for updates to mission critical information, hardware and software and for all changes to automated security or access rules.

Student Information systems must log user access and activity including changes to data fields. College-owned computers must log user login and log off activity and retain data for a minimum 30 days. Wireless network must log user login activity and retain data for a minimum 30 days. A schedule of log retentions will be maintained by the Information Technology department and reviewed and amended in consultation with information resource owner, the Division Director of Information Technology and the Chief Information Security Officer (CISO).

Audit logs must be monitored and/or reviewed as risk management decisions warrant. Audit reports must be reviewed for indications of intrusive activity.

Content of Audit Records (AU-03)

Audit record content includes, for most audit records:

- date and time of the event;
- the component of the information system (e.g., software component, hardware component) where the event occurred;
- type of event;
- user/subject identity; and
- the outcome (success or failure) of the event. National Institute for Standards and Technology (NIST) Special Publication 800-92 provides guidance on computer security log management.

Audit Storage Capacity (AU-04)

Audit storage locations must be allocated in sufficient capacity and monitored to reduce the likelihood of such capacity being exceeded.

Response to Audit Processing (AU-05)

The information technology systems alert appropriate organizational officials in the event of an audit processing failure.

The Information Technology department must ensure that information resources are configured to automate alerts in the event of an audit failure, automate once maximum storage capacity for audit logs is reached, and configure audit logs to overwrite the oldest logs first in cases of reaching capacity.

Audit Review, Analysis and Reporting (AU-06)

The College regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Time Stamps (AU-08)

Whenever technically possible, information technology systems should provide time stamps for use in audit record generation.

Protection of Audit Information (AU-09)

The Information Technology department protects audit information and audit tools from unauthorized access, modification and deletion. Access must be restricted against unauthorized access and tampering. Access must be minimized to necessary Information Technology department resource custodians and Information Technology department security personnel.

Audit Record Retention (AU-11)

Audit records are retained to provide support for investigation of information security events and performance information.

Audit logs must be retained for a minimum of 30 days. Logs and records for known incidents and legal actions must be retained until the incident is closed.

Audit Generation (AU-12)

Audit records must be generated by information systems in support of AU-2 and AU-3.

*If the Chief Information Security Officer (CISO) and the Division Director of Information Technology are the same individual, the coordination as indicated in the policy requires coordination with immediate supervisor.

- Temple College is responsible for IT regulatory compliance as specified by the Department of Education, the Texas Higher Education Coordinating Board, and the State of Texas Administrative Code (TAC202) for Information Technology. The IT policies include the specific guidance, requirements, and procedures in line with the regulatory and audit requirements.