1. Purpose

The purpose of the Audit and Accountability Standard is to ensure that all the University's applicable systems, information, and data can support audit requirements, establish accountability for all users' actions, and provide the capability to identify and alert appropriate applicable parties of security, integrity, or availability issues. This includes ensuring that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. Additionally, this policy is meant to establish the processes to correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. The

4.1.2 Minimum Log Elements

All

4.3.3 Audit Log Retention

Audit logs must be retained in accordance with organizational data retention schedules to ensure the availability of audit logs for incident response and forensic investigation purposes.

Standard log archival periods (hot, warm and cold), retention periods and a verification process for all archival periods that require the logs to be re-ingested.

All logs shall be kept for a minimum of thirty (30) days, unless a longer time period is required per applicable laws or regulations. Logs related to credit card data per the Payment Card Industry Data Security Standard (PCI DSS) should be retained for at least one (1) year. Logs related to personal health information per the Health Information Portability and Accountability Act (HIPAA) should be stored for at least six (6) years.

After logs have met their retention requirement, they must be securely deleted.

4.4 Audit Log Protection and Review

4.4.1 Log Correlation and Analysis

All security event logs, as detailed in section 4.1 of this standard, must be sent to a secure, centralized repository for analysis, such as a Security Information and Event Management tool (SIEM). Rulesets must be established to continuously correlate log data and monitor events against organizationally defined threat scenarios and potential indicators of malicious activity.

When alerting is triggered, it is the responsibility of a Security Analyst to review logs for potential nefarious activity. All security events detected and alerted on should copy the ITS Security Services team.

Alerts in the SIEM tool should be configured based on risks identified during the annual IT Risk Assessment. Alerts should be based on indicators of compromise related to those top risks.

Business units who have experienced a security breach in the last year shall be monitored for a minimum of one year.

4.4.2 Audit Log Record Reduction

As a method of supporting the Audit log review requirements, Audit reduction and reporting generation capabilities must be established to summarize logging into meaningful metrics suitable for review and reporting.

4.5 Log System Maintenance

4.5.1 SIEM Maintenance

ITS Security must formalize the version requirements for t8(r)11(eTPh0009 2ETQ 0.000009 2 5eW*nBT/F3 10 Tcl( )-21(fo)9-2(to)9(r)8

6. Compliance

Compliance Measurement