Version:	Modified By:	Date:	Approved By:	Date:
1.0	Michael Hawkins	October 29, 2013	Dan Bowden	November 2013

Rule 4-004M Payment Card Industry (PCI) Monitoring, Logging and Audit (proposed)

01.1 Purpose

The purpose of the Monitoring, Logging and Audit Rule is to ensure that the University of Utah ("University") complies with all relevant PCI security requirements applicable to monitoring, logging and auditing activities, and ensures that appropriate monitoring, logging and auditing is in place to capture administrative activity for accountability and audit purposes.

01.2 Scope

The Monitoring, Logging and Audit Rule applies to all PCI information systems and resources connected to the University's network. This includes network devices, servers, operating systems, desktops, laptops, applications and programs.

01.3 Rule Statement

Campus University Information Technology ["UIT"], UUHC Information Technology Services ["ITS"], and Information Security shall ensure that relevant PCI actions are logged and reported in system and network log files are retained for a sufficient period (per PCI requirements) to audit historical events, meet legal requirements, and for forensic purposes.

01.4 Monitoring Activities for PCI Systems

01.4.01 Network and System Monitoring

PCI Information technology resources (as defined in Policy 4-004: University of Utah Information Security) shall be continuously monitored to ensure secure operation. Network and system activities that shall be monitored include: [Ref: CS223, PCI]

- Utilization of resources
- Remote access
- Security control mechanisms (e.g. firewalls, intrusion detection systems, level 2 routers, etc.)
- Capacity
- Overloads

- Outbound communications for unusual or unauthorized activities including the presence of malware (e.g. malicious code, spyware, adware)
- Periods of system unavailability

Faults reported by University employees or third parties regarding technical problems with information resources shall be logged and reported to the appropriate IT professional/administrator. IT professionals/administrators are responsible for addressing all technical problems that have been identified for the information technology resources under their control. [Ref: CS511]

Controls shall be enabled on all the University's PCI systems to allow logging of critical activities and software shall be configured to perform critical file comparisons at least weekly. [Ref: CS179, PCI]

[Rules] The following critical activities shall be logged:

- Application start/stop times
- System boot/restart times
- System configuration changes
- Abnormal system events
- Confirmation that files and output were handled correctly
- Critical file changes

01.4.02 Access Logging, Auditing, Monitoring

Audit trail logs shall be active at all times and protected from unauthorized access, modification and accidental or deliberate destruction on all University information system resources that contain Sensitive or Restricted information. Activities that shall be logged include: [Ref: CS224, PCI, HIPAA]

- All successful and unsuccessful login attempts
- All logoff's
- Login attempts using invalid passwords
- Additions, deletions and modifications to user accounts/privileges
- Users switching IDs during an online session
- Attempts to perform unauthorized functions
- Activity performed by privileged accounts
- Modifications to system settings (parameters)
- Access to Sensitive or Restricted data (e.g. Card Holder Data)

- Additions, deletions and modifications to security/audit log parameters

Audit logs shall be retained for at least six (6) months.

In addition to the general activities documented above, all eBanking/eCommerce applications shall also log the following information:

- The opening, modification or closing of a customer's account
- Any transaction with financial consequences
- Any authorization granted to a customer to exceed a limit
- Any granting, modification or revocation of the system's access rights or privileges

Event logs shall include: [Ref: CS225, PCI, HIPAA]

- Host name user account
- Date and time stamp
- Description of the activity performed
- Event ID or event type
- Reason for logging event (e.g. access failure)
- Source and destination network addresses (e.g. IP address)
- Referring page (in case of HTTP access)
- Type of browser used (in case of HTTP access)
- Other information or detail that may help to recreate a sequence of events to provide information for debugging or testing purposes

Systems shall generally be configured to log to centralized systems where technically feasible and supported by business purposes. Event correlation tools shall be used to analyze events from systems and identify potential risk areas or system problems. [Ref: CS226, PCI, HIPAA]

Centralized logging servers shall be considered critical assets and protected in accordance with the University's standards for Restricted information. Systems that cannot be configured to log to a centralized or consolidated log system shall have appropriate access controls for access to log data.

Only Information Security and individuals approved by Information Security have the authority to archive and delete PCI audit trail records. Audit trail records shall be backed up in accordance with the University's PCI Security Requirements/Rules, and protected based on a classification rating of Restricted. Auditing functions shall not record over previous audit records.

Auditing functions shall provide a warning when allocated audit record storage volume reaches a pre-defined threshold. Sufficient audit record storage capacity shall be provided. **01.4.03 Intrusion Detection Systems**

Information Security is responsible for approving all Intrusion Detection Systems (IDS) for use on the University's networks and systems. A listing of approved IDS products can be accessed by contacting the Chief Information Security Officer. [Ref: CS227, PCI]

Only IT professionals/administrators or third parties approved by Information Security may implement Intrusion Detection Systems on the University's networks and information systems and resources. [Ref: CS228, PCI]

The following intrusion detection mechanisms/concepts shall be implemented: [Ref: CS229, PCI, HIPAA]

- Intrusion detection agents shall be deployed on all the information resources (host-based) where sensitive data is stored and the potential for damage to organizational reputation is high.
- Real-time detection of known attack characteristics (e.g., denial of service attacks, viruses, etc.) shall be enabled
- Detected incidents shall be analyzed by system owners, or IT professionals/administrators on a periodic basis (per PCI requirements) to identify trends
- Logs shall be continuously monitored by authorized personnel
- The IDS shall be tuned on a regular basis to respond to specific threats, or based on intruder profiles and pattern. Consistent review of IDS logs will assist with knowing how often to tune
- System and virus signature updates shall be installed on a timely basis. This is called for in other security rules. It is specifically called here to point out that this functionality aids with successful IDS
- All events generated by agents of the IDS shall be stored in a centralized repository from which alerts and reports may be generated and standard alerting interfaces such as simple mail transport protocol (SMTP), simple network management protocol (SNMP), paging and flat files shall be supported
- Automated tools that integrate intrusion detection tools into access control and flow control mechanisms shall be employed for rapid response to attacks
- The design of the IDS shall be reviewed periodically to ensure that system or network changes have not reduced the effectiveness of the system

- The IDS sensors shall be protected against attack by preventing the transmission of any outbound network traffic or by using a network tap to hide the presence of the sensor.

The following shall be performed prior to implementing an IDS: [Ref: CS498, PCI]

- Identify the data flow of the information
- Identify the system processing data streams that will be monitored for anomalies and define which anomalies constitute an indicator of an intrusion
- Understand the scope and nature of the monitoring to be performed
- Understand the University's policies on the use and configuration of IDSs
- Review the listing of approved IDS products and select the most appropriate product
- Contact Information Security with questions regarding the use or configuration
- Assign a resource administrator to implement and maintain the system
- Identify any legal issues that need to be addressed. Legal requirements may include the notification of users regarding the monitoring and the extent to which monitoring will be performed.

01.4.05 Control of Monitoring Devices

The use of all monitoring and scanning devices or tools shall be authorized in advance by Information Security. The results of all monitoring and scanning activities shall be classified as Restricted. [Ref: CS232, PCI]

Incidents discovered by monitoring and scanning devices shall be communicated directly to the Information Owner, Resource Administrator, or Information Security and recorded. [Ref: CS347]

01.4.06 Review of Monitoring Activities

Information Security is responsible for performing periodic reviews to ensure the University's monitoring systems are successful in detecting unauthorized attempts to access information resources. [Ref: CS233, PCI]

01.5. Authentication for PCI Systems

01.5.01 Alarms

Alarms shall be implemented to detect and alert IT resource professionals/administrators of activities that might be attempts at unauthorized information resource access. The type of system events that trigger a duress alarm are determined by the risk profile of the information or applications protected by the operating system. [Ref: CS323]

System events that are used to detect the attack attempt shall be logged and stored in order to maintain evidence for incident follow-up. [Ref: CS324, PCI]

01.6 Privileged and Special Account Access

01.6.01 Special Privileges

Access privileges granted to privileged users shall be reviewed by the [Information Owner] at least every three (3) months to ensure the privileged access level is still valid. [Ref: CS283]

01.6.01 Logging Privileged Account Activity

UNIDs with privileged access rights shall be reviewed annually. [Ref: CS333]

Privileged access IDs shall be logged by system monitoring applications. [Ref: CS334]

User activity reports, such as failed access attempts and any changes to user rights shall be reviewed on a regular basis to deter misuse of privileged accounts. [Ref: CS335]

01.6.02 System Utilities/Commands

The authority and access to use advanced operating system utilities and commands that bypass system access controls shall be monitored, logged, reviewed and restricted to those individuals who require access to perform their job functions. [Ref: CS336]

01.7 Network Security Control Devices for PCI Systems

01.7.01 Logging and Auditing

The following logging and auditing standards for firewalls shall be implemented: [Ref: CS498, PCI]

- The firewall logs shall be filed, retained for six (6) months, and protected from manipulation
- They shall contain at least the following data:
    - Successful and rejected connections to the firewall
    - Successful and rejected connections to internal hosts
    - Connections to external hosts
    - Multiple, rejected connections to the same host
- The extraction of specific information shall be possible within 10 days
- The firewall logs are written to disk and access to this data shall be limited to the firewall administration and system management

- Alarm or monitoring tools shall be used to alert the appropriate resource administrator of security-related events originating from the firewall

Alarm or monitoring tools shall be used to alert the appropriate resource administrator of security-related events originating from the firewall. [Ref: CS380]

Firewall administrators shall review the system logs generated from firewalls they have been assigned, on a daily basis to detect any unauthorized entry attempts or unusual behavior. The following information shall be viewed and appropriate action shall be taken if any unusual activity is detected: [Ref: CS381]

- Successful and unsuccessful connections to firewall
- Successful and unsuccessful connections to internal hosts
- Connections to external hosts
- Multiple, rejected connections to same host
- Logs shall be mirrored on a separate system as "read only" data and filed and retained for six (6) months
- Logs shall be protected to prevent anyone from making changes to the stored data

01.8 Security of Facilities PCI Systems

01.9.01 Securing Computing Facilities

Physical access audit logs shall be maintained in either electronic or printed form for at least two (2) months, be designated Restricted, and be provided security protection commensurate to that classification. Appropriate managers shall review these logs on a daily basis. [Ref: CS081, HIPAA]

Fire detection and suppression systems for computing [critical computing, data centers] facilities shall be monitored. [Ref: CS132]

Critical computing facilities shall be monitored for water or moisture conditions, which could adversely affect the operation of information resources. These water and moisture monitoring devices shall be installed in all critical information processing environments. Shutoff valves shall be automatically closed in the event a significant water leak is detected. [Ref: CS146]

Computing facility environments, including temperature, humidity and power supply quality shall be monitored to identify conditions which might adversely affect the operations [Ref: CS158]

01.10 Operational Controls

01.10.01 Security Diagnostic Tools

Access to all tools (e.g., software, applications, documentation, work papers) required for system audits shall be restricted to authorized individuals. Possession, distribution or use of network diagnostic, monitoring and scanning tools shall be limited to designated and authorized personnel in accordance with their job responsibilities. Approval can only be granted by Information Security. This includes anything which can replicate the functions of such tools. Unauthorized possession, use or distribution of such tool of functions is prohibited and may be grounds for disciplinary action. [Ref: CS503]

01.10.02 Anti-Virus Software

Audit logs of scan results shall be kept for six (6) months. These logs shall note the date and times that scans occurred and any findings that were noted. [Ref: CS483]

01.7 Contacts

A. Policy Owner: Questions about this rule should be directed to the CISO, 801-213-3397 IT_policy@utah.edu

B. Policy Officer: Only the CIO, 801-581-3100, has the authority to grant exceptions to this rule.

01.8 References

A. Policy 4-002: Information Resources Policy
B. Policy 4-004: University of Utah Information Security Policy
C. Data Classification Model

01.9 Policy Meta-Data

A. Policy Owner
B. Audience
C. Status
D. Published Date
E. Effective Date
F. Next Review Date

01.10 Revision History