Configuration Management
HIPAA Policy: Security 14

Summary: Minimizing risk to PHI in HIPAA covered entities by managing the configuration of information assets

Affected Individuals: Employees in HIPAA covered entities; IT staff

Purpose of Policy

The purpose of this policy is to minimize risk to University of Mississippi (UM) and to ensure the operational effectiveness and continuity of the Information Technology (IT) environment by managing the configuration of information assets.

Configuration management controls and processes ensure that changes to UM's information assets are effective and efficient, reduce security risks, are fully documented, and that these changes occur with minimal disruption to operations.

Definitions

For a complete list of definitions, refer to the *Glossary*.

Scope

This policy applies only to covered entities as defined in the University of Mississippi (UM) HIPAA hybrid policy. This policy applies to all UM information assets, e.g., hardware, software, IT infrastructure (e.g., equipment, networks, and operating systems), services, and associated documentation regardless of origin, nature, or location (e.g., contractor, in-house, development, operations, all hosting data centers, internal and external systems) unless otherwise specified.

Policy

A. Configuration Management Plan

1. UM develops, implements, tests, and maintains a *Configuration Management Plan* that minimizes risk through planning, communication, and collaboration and that ensures changes to the IT Infrastructure and production environment are effective and efficient with minimal disruption to UM.
2. The *Configuration Management Plan* includes, at a minimum:

- Roles and responsibilities.
- Configuration management processes and procedures.
- A definition of the items in the IT Infrastructure that must be placed under configuration management.
- Processes for putting IT acquisition and development (pre-production) items under configuration management.
- Processes for managing, testing, documenting, deciding upon, and communicating status of the configuration of the items that are subject to configuration management.

B. Security of System Configuration Documentation

1. System configuration documentation is treated as confidential data with minimum necessary and need-to-know access, and is protected against unauthorized access in accordance with the *Access Control Policy*.
2. Access to system configuration documentation is authorized by the Chief Information Security Officer (CISO).

C. Baseline Configurations

1. UM develops, documents, controls, and maintains current baseline configurations for all managed information systems.
2. UM reviews and updates the baseline configurations of the managed information systems at least annually.
3. UM retains older versions of baseline configurations as deemed necessary to support continuity of operations (e.g., rollback of a system update).

D. Configuration Settings

1. UM establishes and documents mandatory configuration settings for IT infrastructure items using a security configuration checklist that reflects the most restrictive mode consistent with operational requirements.

2. Only authorized administrators are allowed to implement approved upgrades to software, applications and program libraries based on business requirements and the security implications of the release.
3. Applications and operating systems are successfully tested for usability, security and impact prior to production.
4. UM identifies and documents exceptions from the mandatory configuration settings for individual components within information systems based on explicit operational requirements. Exceptions are approved by the CISO.
5. UM uses its configuration control program to maintain control of all implemented software and system documentation and archives prior versions of implemented software and system documentation.
6. UM incorporates detection of unauthorized, security-relevant configuration changes into the *Incident Response Plan* to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes in accordance with the *Incident Management Policy*.

E. Configuration Change Control

1. The implementation of changes, including patches, service packs, and other updates and modifications, is controlled by the *Change Management Policy*.
2. UM audits activities associated with configuration-controlled changes to information systems.

F. Least Functionality

1. UM configures information systems to provide only essential capabilities and specifically prohibits or restricts the use of non-essential functions, ports, protocols, and/or services in order to reduce risk.

2. UM reviews information systems at least annually to identify and eliminate unnecessary functions, ports, protocols, and/or services.

G. IT Infrastructure Inventory

1. UM develops, documents, and maintains an inventory of IT Infrastructure items. Inventory detail must be maintained at a sufficient level for purposes of tracking and reporting.
2. UM continuously updates the IT Infrastructure inventory as an integral part of installations, removals, and information system updates.
3. UM verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.

Policy Compliance

Enforcement

The CISO, or designee, has general responsibility for the implementation and enforcement of this policy.

Future Revisions

UM reserves the right to add, delete, or revise any provision of this Policy (approved by committee) at any time, or any other Information Security Policy without prior notice to users.

Sanctions

Any user violating these policies or applicable local, state, or federal laws while using UM computing environment is subject to loss of network privileges and any other disciplinary actions deemed appropriate, up to and including termination and criminal and/or civil prosecution in accordance with policy.

Configuration Management
HIPAA Policy: Security 14

Exceptions

Exceptions to this policy must follow the approved exception process as outlined in the *Information Security Waiver Policy*. All approved policy exceptions will be reviewed periodically for appropriateness by the CISO and may be revoked at any time with or without notice.

Regulatory and Standards References

The following regulations and standards are applicable to this policy:

- **HITRUST References**: 09.r Security of System Documentation, 10.k Change Control Procedures
- **PCI References**: PCI DSS v3 6.4

Related Documents:

- Information Technology Access Control Policy
- Change Management Policy
- Configuration Management Plan
- Glossary
- Incident Management Policy
- Incident Response Plan
- Minimum Security Baseline Requirements
- Security Configuration Checklist

Approval

Chief Information Security Officer	<date>