Vulnerability Management
HIPAA Policy: Security 22

Summary: Outlines procedures for identifying and mitigating risks from vulnerabilities in HIPAA covered entities

Affected Individuals: Employees in HIPAA covered entities; IT staff

Purpose of Policy

The purpose of this policy is to state the actions University of Mississippi (UM) takes to manage risk related to technical vulnerabilities in an effective, systematic, and repeatable way, and to confirm the effectiveness of those actions.

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 information assets connected to UM's network including, but not limited to, computer workstations, laptops, tablets, smartphones, servers, network switches and routers, etc. The Chief Information Security Officer (CISO) has the authority to conduct vulnerability assessments on any information asset, product, or service within UM.

Policy

A. Control of Technical Vulnerabilities

1. UM takes deliberate actions to reduce and mitigate risks to UM's systems resulting from exploitation of technical vulnerabilities.
2. UM obtains timely information about technical vulnerabilities, evaluates the exposure to such vulnerabilities, and takes appropriate measures to address the associated risk.
3. In accordance with the *Information Asset Management Policy,* UM maintains an inventory of information assets with sufficient detail to identify systems at risk by a particular technical vulnerability.

4. UM develops, implements, tests, and maintains a *Vulnerability Management Plan* that facilitates the reduction of risk from published technical vulnerabilities. The *Vulnerability Management Plan* includes the following at a minimum:

    - Roles and responsibilities for technical vulnerability management
    - Processes and procedures for monitoring, assessing, ranking, and remediating vulnerabilities identified in systems.
    - Processes and procedures that provide a timely response to technical vulnerabilities that present a risk to any information asset, including a timeline based on the level of risk.

5. UM evaluates the *Vulnerability Management Plan* on an annual basis.

6. Risks identified in the *Vulnerability Management Plan* which are expected to persist for a period of greater than one (1) year are added to the Corrective Action Plan according to the *Risk Management Policy*.

7. Systems are appropriately hardened (e.g., configured with only necessary and secure services, ports and protocols enabled) according to the *Configuration Management Policy*. A hardened configuration standard exists for all system components and is documented.

8. Annual system scans are performed to detect vulnerabilities (e.g., unauthorized software).

9. Technical tests of the external and internal network are performed annually. Exploitable vulnerabilities found during technical testing are corrected and testing is repeated to verify the corrections.

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 (with committee approval) at any time without prior notice to users.

Sanctions

Any user violating these policies or applicable local, state, or federal laws while using UM's 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..

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 Reference**: 10.m Control of Technical Vulnerabilities
- **PCI Reference**: PCI DSS v3 2.2, PCI DSS v3 6.1, PCI DSS v3 6.2, PCI DSS v3 6.4.5, PCI DSS v3 6.4.5.1, PCI DSS v3 6.4.5.2, PCI DSS v3 6.4.5.3, PCI DSS v3 6.4.5.4, PCI DSS v3 11.2, PCI DSS v3 11.2.1, PCI DSS v3 11.2.2, PCI DSS v3 11.2.3, PCI DSS v3 11.3, PCI DSS v3 11.3.1, PCI DSS v3 11.3.2, PCI DSS v3 11.3.3., PCI DSS v3 11.3.4

Vulnerability Management
HIPAA Policy: Security 22

Related Documents:

- Change Management Policy
- Configuration Management Policy
- Glossary
- Information Asset Management Policy
- Nessus Network Vulnerability Scanner Procedures
- Risk Management Plan
- Risk Management Policy
- Vulnerability Management Plan

Approval

Chief Information Security Officer	<date>