Endpoint Protection
HIPAA Policy: Security 17

Summary: Methods for improving endpoint security in HIPAA covered entities

Affected Individuals: Employees in HIPAA covered entities; IT staff

Purpose of Policy

The purpose of this policy is to establish the methods for improving the security of endpoints through effective security configuration, malware detection, and malware prevention.

Policy Scope

This policy applies only to covered entities as defined in the University of Mississippi (UM) HIPAA hybrid policy. All workforce members and users, including third parties, who may have access or exposure to University of Mississippi (UM) data are required to comply with this policy.

All UM workforce members and users must take responsibility for minimizing the risk of their computing device infecting other systems or shared files on a server.

Definitions

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

Policy Statement

A. Controls Against Malicious Code

1. Detection, prevention, and recovery controls shall be implemented to protect against malicious code.
2. All computing devices, including personally owned devices, that connect to the UM network shall have appropriate anti-malware software installed and running at all times.
3. Where possible, anti-malware software shall ensure that updates are automatically applied within 24 hours of availability.
4. Where possible, anti-malware software shall automatically conduct scans of computing devices on boot and at least once every 24 hours.

5. Where automatic updates and scans are not possible, users shall be responsible for initiating the scan and updating the software to protect against the latest threats.
6. Anti-malware software shall be configured to scan downloads from external sources as they are downloaded and prevent infected files from opening or executing.
7. Anti-malware software shall maintain logs of all scans in accordance with to the *Audit, Logging, and Monitoring Policy*.
8. Anti-malware software shall automatically clean and remove or quarantine malicious code. Infected computing devices shall be removed from the UM network until they are verified as safe.

B. Third Parties

1. All third party laptops shall have up-to-date anti-malware software installed prior to connecting to the UM network.

C. Training and Awareness

1. User awareness and training on malicious code detection and prevention shall be provided in accordance with the *Privacy and Security Awareness and Training Policy*.

D. Acceptable Use

1. All users shall take reasonable measures to protect against the installation of unlicensed or unauthorized software in accordance with the *Information Technology Acceptable Use Policy*.
2. All users are strictly prohibited from conducting any activities with the intention of creating and/or distributing malicious programs using UM network (e.g., viruses,

worms, Trojan Horses, etc.) in accordance with the *Information Technology Acceptable Use Policy*.

E. Operating Systems

1. Operating systems shall be maintained by applying any service packs, patches, or security updates in accordance with the *Change Management Policy*.
2. Where possible, Operating System updates shall be provided automatically. Users must follow directions from User Support when Operating System updates are distributed.
3. The Chief Information Security Officer (CISO) must ensure, where feasible, that all users apply Operating System updates to their computing devices as soon as possible.
4. Unmanaged computing devices which become a security risk to the UM environment shall be disconnected from the UM network.
5. Operating Systems which no longer have security updates available to fix vulnerabilities shall be upgraded to a currently supported Operating System. If this is not possible or practical, the risk shall be documented and measures taken to reduce and mitigate that risk. The CISO shall determine the risk level and shall issue a waiver in cases where such a waiver is warranted in accordance with the Information Security Waiver Policy.

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 (approval 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'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 References

HIPAA Regulatory Reference: HIPAA § 164.308(a)(5)(ii)(B)
HITRUST Reference: 09.j Controls Against Malicious Code
PCI References: PCI DSS v3.1 5.1, PCI DSS v3 5.1.1, PCI DSS v3.1 5.2

Related Documents

Information Technology Acceptable Use Policy
Audit, Logging, and Monitoring Policy
Change Management Policy
Endpoint Protection Procedures
Glossary
Mobile Computing Device Security Policy
Privacy and Security Awareness and Training Policy

Endpoint Protection
HIPAA Policy: Security 17

Approval

Chief Information Security Officer	<date>