Firewall Review/Change log
HIPAA Policy: Security 27

Summary: Annually document the review of firewall rules.

Affected Individuals: Employees in HIPAA covered entities; IT staff

Purpose of Policy

The purpose of this policy is to document the ongoing firewall change log to ensure the protection of data in the HIPAA Covered Entities of the University of Mississippi (UM).

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 firewalls protecting HIPAA Covered Entities.

Policy

A. Firewall rule change log review and documentation

1. UM manages firewalls to protect information contained in HIPAA covered entity networks. These firewalls are configured to restrict IP traffic through both ingress and egress rules to only permit access to sites necessary to perform the necessary operational functions required and permit updating and patching of systems.
2. A firewall rule change log document is operationally maintained for each covered entity that records the date and time of rule adds, changes and deletions.
3. Annually, when the policy renewal processes, the change log document is reviewed for an overview of the previous year’s changes.

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, 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 and Standards References

The following regulations and standards are applicable to this policy:

- **HIPAA Regulatory References**: HIPAA §164.312(a)(2)(i), HIPAA §164.312(c)(1), HIPAA §164.312(c)(2), HIPAA §164.312(d), HIPAA §164.312(e)(1), HIPAA §164.312(e)(2)(i), HIPAA §164.312(e)(2)(ii)
- **HITRUST References**: 07.a Inventory of Assets, 09.m Network Controls
- **PCI References**: PCI DSS v3 1.1.1, PCI DSS v3 1.1.2, PCI DSS v3 1.1.3, PCI DSS v3 1.1.4, PCI DSS v3 1.1.5, PCI DSS v3 1.2, PCI DSS v3 1.2.1, PCI DSS v3 1.2.2, PCI DSS v3 1.2.3, PCI DSS v3 2.1.1, PCI DSS v3 4.1.1, PCI DSS v3 11.1

Related Documents:

- HIPAA CE Change Log

Approval

Chief Information Security Officer

<date>