[Insert Company Name Or Logo]	
Title: Network Security Continuous Monitoring	**P&P #:**
Approval Date: [Date]	**Review:**
Effective Date: [Date]	**Information Technology**

Purpose

The information network, systems and assets are continuously monitored to identify cybersecurity threats and/or events and to verify the effectiveness of protective measures.

Scope

This policy applies to all employees and other members of the workforce (whether paid, volunteer or contractor) working in all facilities under the organization's ownership and being granted access to any electronic information system.

Policy

Our Security Officers will implement policies and procedures to monitor information systems and assets to limit or contain the impact of a potential cybersecurity event.

Procedures

Network is monitored to detect potential cybersecurity events

I. The Security Officer will provide audit record generation capability for the event types the system is capable of auditing as defined below:
    a. Identify the types of events that the system is capable of capturing in support of the audit function: [organization-defined event types]

II. Security Officer will oversee the generation of audit records for the organization-defined event types listed above that include the audit record content defined below:
    a. What type of event occurred.
    b. When the event occurred.
    c. Source of the event.
    d. Outcome of the event; and
    e. Identity of any individuals, subjects, or objects/entities associated with the event

External service provider activity is monitored to detect potential cybersecurity events

I. Security Officer will establish the following system-level metrics to be monitored: [organization-defined system-level metrics]

II. Security Officer will establish ongoing frequencies for monitoring and assessment of control effectiveness.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

III. Security Officer will conduct ongoing control assessments in accordance with the continuous monitoring strategy.
IV. Security Officer will correlation and analyze information generated by control assessments and monitoring.
V. Security Officer will develop actions to address results of the analysis of control assessment and monitoring analysis and will report the security and privacy status of the system to [organization-defined personnel or roles].

Vulnerability scans are performed.

I. Security Officer will monitor and scan for vulnerabilities in the system and hosted applications [organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported.
II. Security Officer will employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    a. Enumerating platforms, software flaws, and improper configurations.
    b. Formatting checklists and test procedures.
    c. Measuring vulnerability impact
III. Security Officer will analyze vulnerability scan reports and results from vulnerability monitoring.
IV. Security Officer will remediate legitimate vulnerabilities in accordance with an organizational assessment of risk.
V. Security Officer will share information obtained from the vulnerability monitoring process and control assessments with [organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems.
VI. Security Officer will employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

Violations: Workforce members shall be responsible for reporting suspected or known information security concerns to the Security Officer as soon as discovered, with failure to do so resulting in appropriate sanctions**,** up to and including termination of employment.

Attachments: None

Related Policies: Risk Management

Reference: *NIST Special Publication 800-53 Revision 5*

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.