SOP: Network Security

Purpose:

The purpose of this document is to establish procedures for the protection of IT devices, network systems, and the data they contain.

Scope:

This policy impacts the entire organization, from the MSP to employees, contractors, vendors: everyone who accesses any part of the network.

Responsibilities:

- Senior Network Administrator: Responsible for implementing, following, reviewing, maintaining, and updating this policy. Responsible for responding to security incidents in accordance with the Cyber Incident Response Plan.
- System Administrators: Responsible for securing the network and corporate devices. Responsible for implementing security controls according to the principles of zero trust and least privilege. Responsible for monitoring network traffic as detailed in the SOP for network monitoring and notifying management of any suspicious activity.
- All Personnel, Contractors, Vendors: Responsible for implementing good cyber security practices as taught during cybersecurity training.

Prerequisites:

- Personnel with access to network systems
- Cybersecurity training program
- Familiarity with network security practices

Procedure:

Access Control

- Utilize strong authentication mechanisms such as capture portal and Active Directory for network access
- Regularly review and update user access privileges based on job roles and responsibilities to prevent privilege creep.

Authorization

- Utilize the principles of zero trust and least privilege to limit user access to only the apps, programs, files and other resources to only what is authorized by their associated Organizational Unit.

Firewalls and Intrusion Detection/Prevention Systems

- Firewalls will be utilized and configured to restrict unauthorized inbound and outbound traffic.
- Firewall rules and access control lists (ACLs) will be regularly reviewed and updated in Active Directory
- Utilize intrusion detection/prevention systems to monitor and block suspicious network traffic.

Encryption

- Utilize encryption protocols (e.g., SSL/TLS) for securing network communications.
- Encrypt sensitive data both at rest and in transit.
- Regularly update encryption algorithms and key lengths to industry best practices.

Patch Management

- Deploy security patches in a timely manner when received.
- Regularly update network devices, servers, and software with the latest patches.
- Test patches in a controlled environment before deploying them to the whole network.

Network Monitoring and Logging

- Follow the guidelines detailed in the SOP for network monitoring.
- Maintain comprehensive logs of network activities, including user logins, access attempts, and system events.
- Regularly review and analyze network logs to identify security incidents or policy violations.

Security Awareness Training

- Conduct security awareness training for all employees during onboarding and on an annual basis thereafter.
- Educate employees on common security threats, such as phishing and social engineering.
- Train employees on proper handling and protection of sensitive information.

Incident Response

- Follow the procedures outlined in the Cyber Incident Response Plan
- Document and report security incidents promptly to the appropriate stakeholders.
- Conduct post-incident analysis and implement corrective measures to prevent future incidents.

Compliance and Auditing

- Regularly conduct internal and external audits to assess network security compliance.
- Maintain documentation of security controls, policies, and procedures.
- Monitor compliance with applicable laws, regulations, and industry standards.

Documentation and Review

- Maintain up-to-date documentation of network security policies, procedures, and configurations.
- Conduct periodic reviews of network security controls and procedures.
- Update the SOPs, topologies and other documentation as necessary to reflect changes in technology, threats, or organizational requirements.

References:

- SOP for network monitoring.
- Cyber Incident Response Plan

Definitions:

- Access Control Lists (ACL) - Lists maintained in Active Directory and managed by group policies that control what systems, files and resources users have access to.
- IT - Information Technology: computers, servers, switches and other network devices.
- Encryption - Electronically coding data so that it can only be decoded by another program with the correct decryption key.

Revision History:

6/23/2023 -- SOP: Network Security created by Chris Bennett (with some assistance from ChatGPT)