SOP: Network Security.

Purpose:

The purpose of this SOP is to provide guidance on managing and maintaining network security.

Scope:

This SOP applies to all aspects of network security within the organization.

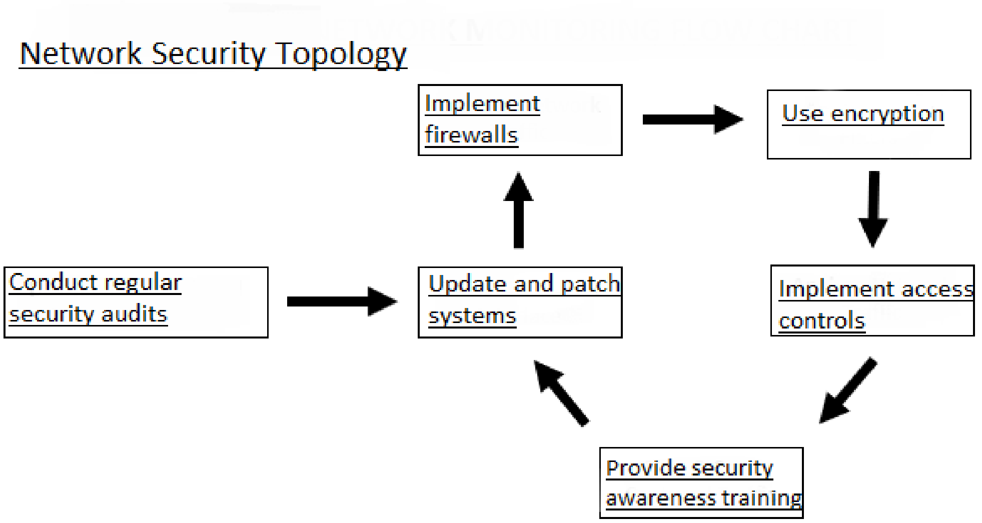
Responsibilities:

IT Specialist: Damian Nowak is responsible for implementing, following, reviewing, maintaining, and updating this policy.

Prerequisites:

IT Specialist Damian Nowak must ensure that all network devices, operating systems, applications, and data are up-to-date and patched with the latest security updates and configurations. All employees, contractors, vendors, and visitors must receive training on network security policies and procedures.

Procedure:


Network Security Topology
Implement firewalls
Use encryption
Conduct regular security audits
Update and patch systems
Implement access controls
Provide security awareness training

- Conduct regular security audits: The IT department should conduct regular security audits to assess the effectiveness of the organization's network security measures. This includes reviewing access logs, identifying vulnerabilities, and checking for unauthorized devices.
    - Define audit scope: Determine the scope of the security audit, including the systems, networks, and applications that will be audited.
    - Identify audit criteria: Identify the criteria that will be used to evaluate the effectiveness of the organization's security measures. This could include industry standards, best practices, and regulatory requirements.
    - Conduct the audit: Review access logs to identify any unauthorized access attempts or suspicious activity. Scan the network and systems for vulnerabilities using vulnerability scanning tools. Check for any unauthorized devices that may have been connected to the network.
    - Analyze audit findings: Analyze the findings from the audit to identify any weaknesses or gaps in the organization's security measures.
    - Develop an action plan: Develop an action plan to address the weaknesses or gaps identified in the audit findings. This may include implementing new security controls, updating policies and procedures, or providing additional training to employees.

- Update and patch systems: The IT department should regularly update and patch all systems and software to ensure that they are protected against known vulnerabilities. The IT department should also implement automated patch management tools to streamline the process.
    - Identify all the systems and software that need to be updated and patched. This includes servers, workstations, network devices, and any other devices connected to the organization's network.
    - Develop a patch management plan that outlines the process for testing, approving, and deploying patches. The plan should include a schedule for regular patching and a process for emergency patching in the event of critical vulnerabilities.
    - Implement an automated patch management tool that can identify and deploy patches across the network. The tool should be configured to prioritize critical patches and automate the deployment process to minimize downtime.
    - Test all patches before deploying them to ensure that they do not cause any compatibility issues or unintended consequences.
    - Monitor the network after patching to ensure that all systems have been updated and patched successfully. The IT department should also monitor for any new vulnerabilities that may require additional patches or updates.

- Implement firewalls: The IT department should install firewalls to protect the organization's network from unauthorized access. Firewalls should be configured to allow only necessary traffic and block all other traffic.
    - Determine the organization's network topology: Before implementing a firewall, the IT department should assess the organization's network topology to determine the most effective placement of the firewall.
    - Choose a firewall solution: The IT department should choose a firewall solution that is appropriate for the organization's needs. This could include hardware or software firewalls, or a combination of both.
    - Configure the firewall: The IT department should configure the firewall to block all traffic that is not necessary for the organization's operations. This includes configuring the firewall to block incoming traffic from unauthorized sources, and outgoing traffic that does not meet the organization's security policies.
    - Test the firewall: The IT department should test the firewall to ensure that it is effectively blocking unauthorized traffic and allowing necessary traffic. This includes testing the firewall's rules and policies, and ensuring that it is properly integrated into the organization's network.
    - Maintain the firewall: The IT department should regularly maintain the firewall to ensure that it is up-to-date and effective against new threats. This includes applying software updates and patches, monitoring the firewall's logs for suspicious activity, and reviewing and updating firewall policies as needed.

- Use encryption: The IT department should implement encryption to protect sensitive data that is transmitted over the network. This could include using VPNs or SSL/TLS encryption for web-based applications.
    - Identify the sensitive data: The IT department should identify the sensitive data that needs to be protected, such as financial information, personal data, and intellectual property.
    - Choose the appropriate encryption method: Based on the type of data being transmitted, the IT department should choose the appropriate encryption method. This could include using VPNs, SSL/TLS encryption, or other encryption technologies.
    - Install and configure encryption software: The IT department should install and configure encryption software on all relevant systems and devices. This includes configuring encryption protocols, generating encryption keys, and setting up secure connections.
    - Train employees on how to use encryption: The IT department should provide training to employees on how to use encryption technologies, including how to establish secure connections and how to properly store and transmit sensitive data.

    - Monitor and maintain encryption systems: The IT department should monitor and maintain the encryption systems to ensure that they are functioning properly and are up-to-date with the latest security patches and upgrades.
    -

- Implement access controls: The IT department should implement access controls to ensure that only authorized users have access to the network and the organization's sensitive information. This includes implementing password policies, multi-factor authentication, and user access management controls.
    - Implement password policies: The IT department should establish password policies that require strong passwords, regular password changes, and prohibit password sharing. Passwords should also be encrypted and stored securely.
    - Implement multi-factor authentication: The IT department should require multi-factor authentication for all user accounts to provide an extra layer of security. This could include using biometric authentication, smart cards, or one-time passwords.
    - Use user access management controls: The IT department should establish user access management controls to ensure that users only have access to the information they need to perform their job functions. This includes assigning roles and permissions, and regularly reviewing access privileges.
    - Use network segmentation: The IT department should segment the network to limit access to sensitive information. This involves dividing the network into smaller, isolated segments and controlling access between them.
    - Implement security policies and procedures: The IT department should establish security policies and procedures for user access and regularly train employees on how to follow them. This includes policies for password management, user access management, and network segmentation.

References:

- pfSense site to site VPN tunnel - The Complete Guide
- Configure RADIUS Clients

Definitions:

1. SSL/TLS: Secure Sockets Layer/Transport Layer Security.
2. VPN: Virtual Private Network.
3. RADIUS: Remote Authentication Dial-In User Service

Revision History:

03APR2023 – add SOP outline - Ethan Brock
04APR2023 – populated SOP information - Ethan Brock