Enhance the Network’s Usability and Security

1.0 Overview

The objective of the SOP is to set up a well-designed network to improve usability and security. Ensure that the network is designed to accommodate the company's current and future needs and is secure by design. Consider factors such as network topology, protocols, and security measures.

2.0 Scope

This SOP is applicable to implement access control measures to prevent unauthorized access to the network. This can be achieved through the use of firewalls, VPNs, access controls, and user authentication.

3.0 Procedures:

Patch Management: Ensure that the network's hardware and software are up to date with the latest patches and updates. This helps to prevent vulnerabilities and protect the network from security threats.

Network Monitoring: Regularly monitor the network for any unusual activity or anomalies. This can be achieved through the use of network monitoring tools, logs, and security information and event management (SIEM) systems.

Employee Training: Educate employees on network security best practices, including password management, data protection, and social engineering awareness. This can help to reduce the risk of human error and prevent security breaches.

Disaster Recovery Plan: Create a disaster recovery plan to ensure business continuity in the event of a network failure. This plan should include regular backups of critical data, alternative network access, and a process for restoring the network in the event of a failure.

Vulnerability Assessment: Perform regular vulnerability assessments to identify any security weaknesses in the network. This can be achieved through the use of vulnerability scanning tools and penetration testing.

Incident Response Plan: Create an incident response plan to address security incidents promptly. This plan should include procedures for reporting incidents, isolating affected systems, and restoring services.

Physical Security: Ensure that physical access to the network infrastructure is restricted to authorized personnel only. This can be achieved through the use of access controls, security cameras, and security personnel.

Regular Audits: Regularly audit the network to ensure compliance with industry standards and best practices. This can be achieved through the use of internal or external audits, risk assessments, and penetration testing.