Network Monitoring

Purpose:

Network monitoring provides visibility into each layer of OSI, helping network administrators easily identify and troubleshoot network issues.   Elven Enterprises will monitor traffic ensuring security of data exchange and guarding against suspicious activity. Employees of FrodoTech have already signed the Acceptable Use Agreement regarding what websites and services should and should not be accessed via company machines. The following is a high-level summary of Elven Enterprises Network Monitoring activities:

Common Network Devices to Monitor

- **Routers:** Routers help connect networks via the internet.
- **Switches:** Switches help connect devices such as servers, computers, printers, and more. Monitoring switches is critical to ensure network health and performance. It’s also essential to monitor traffic and hardware through the switch.
- **Firewalls:** The role of a firewall is to protect the network by controlling incoming and outgoing traffic.
- **Servers:** Server monitoring helps provide information about the network, data usage, and more.

Scope:

This SOP outlines the infrastructure to regulate, supervise and control the network. IT will monitor network traffic, server performance, and protect confidential data. Elven Enterprises will help optimize network performance, decrease downtime and improve data security through this type of data surveillance.

Responsibilities:

1. FordoTech Staff: Responsible for adhering to cybersecurity training, following access control policies, and reporting security incidents promptly.
2. Elven Enterprises: Responsible for implementing and maintaining cybersecurity measures, conducting regular audits, and managing incident responses.
3. Management: Responsible for approving and supporting cybersecurity initiatives, ensuring compliance with policies, and fostering a culture of security awareness.

Prerequisites:

1. Access to cybersecurity training materials.
2. Secure and updated computer systems.
3. Secure Wi-Fi network with WPA3 encryption.
4. Antivirus and anti-malware software installed on all devices.
5. Incident response plan documentation.

Procedure:

Elven Enterprises will be using Wireshark through Kali-Linux for network monitoring. The IT team will take care of this process in the background. Specific details of Elven Enterprises procedures can be described further but require higher authorization.

Definitions:

Network monitoring is the process of constantly monitoring a computer network for problems such as slow traffic, suspicious activity and/or component failure.

Revision History:

This SOP will be reviewed annually and updated as needed to reflect changes in technology, regulations, and the supermarket's operating environment

Date	Employee	Change
4/15/24	Julian Pena	“SOP: Network Monitoring”