SOP - Network Diagram

Purpose

To define a structured process for creating, updating, and managing **network diagrams** to accurately represent corporate infrastructure, enhance visibility, aid in incident response, and support audits and compliance.

Scope

Applies to all network environments including:

- Internal LAN/WAN
- Cloud and hybrid infrastructures
- VPNs, firewalls
- Third-party integrations
- Security appliances and monitoring systems

Objectives

- Maintain an accurate and up-to-date representation of the IT network
- Improve troubleshooting and change management
- Support risk assessments, audits, and compliance
- Facilitate onboarding and handovers within the IT/security teams

Roles and Responsibilities

Role	Responsibility
Security Team	Create and update diagrams
Security Team	Validate segmentation, firewall zones, and sensitive areas
CTO	Approve final versions and authorize access

Types of Network Diagrams

Type	Description
Physical Diagram	Shows hardware components, cabling, physical locations
Logical Diagram	Displays IP addressing, VLANs, routing, subnets, zones
Cloud/Hybrid Diagram	Maps cloud services (e.g., Microsoft 365, Azure AD) and their interaction with on-prem assets
Security Zone Diagram	Illustrates trust zones, firewalls, DMZ, segmentation

Access Flow Diagram	Describes user and data flow paths between systems

Diagram Components

Must include (as applicable):

- Core switches, routers, firewalls, load balancers
- Endpoints
- IP address ranges/subnets
- Cloud platforms and connectors
- VPN gateways
- Internet/inbound/outbound flows

Tools for Diagramming

Preferred tools (select based on availability):

Tool	Usage
Microsoft Visio	Enterprise standard for professional diagrams
Cisco Packet Tracer	Simulation tool for network devices
Draw.io (diagrams.net)	Free, simple, and integrates with Google Drive/OneDrive

Diagram Creation Process

Step 1: Asset Discovery

- Use Microsoft Defender, GDMS cloud or other sources to map network assets.
- Collect:
  - Device names
  - IP addresses
  - VLANs/subnets

Step 2: Group & Categorize

- Organize by layer: core, distribution, access

Step 3: Design the Diagram

- Choose appropriate template (physical/logical)
- Use standardized icons
- Label everything clearly:
  - Interfaces (for example: Gi0/1)
  - IPs
  - VLANs
  - Security zones

Step 4: Review & Validate

- Review with:
  - Security team
  - CTO
- Ensure sensitive systems are represented accurately

Step 5: Version Control & Documentation

- Save versions
- Store in:
  - SharePoint / OneDrive
  - Secure backup location

Maintenance and Update Frequency

Event	Action
Major network change	Update diagram within 2 business days
Quarterly review	Validate accuracy with network and security team