SOP Scenario & Problem Domain for Growing Technology Company

Client: Growing technology company with 20 employees in Sales & Marketing, R&D, and IT Management.

Needs:

- Network Upgrade: Support expanding workforce and enhance data security.
- Seamless Communication: Office to central server and vice versa.
- Data Security: Safeguard data, secure file shares, and implement backup solutions.
- Collaboration: Efficient file sharing across departments.
- Business Continuity: Robust backup solution for quick recovery in case of data loss.
- IT Onboarding: Streamlined procedures for new employees.

Proposed Solution:

Phase 1: Network Design and Infrastructure

- Network Topology:
    - Layer 2 Switch: Connects all physical devices in the office.
    - Virtual Machines (VMs):
        - Server VM (VLAN 10) hosts Windows Server and file shares.
        - Router VM (VLAN 10) manages VPN connection and internet access.
        - Computer VMs (VLANs 20, 30): One for each department with dedicated file shares.
        - Expansion VM (VLAN 40): Reserved for future growth.
- VPN Setup:
    - Site-to-site VPN tunnel between office router and central server using strong encryption and authentication protocols (e.g., IPsec, OpenVPN).
    - Cloud-based VPN management platform for simplified control and monitoring.
    - Demonstration of successful access to resources on the central server (file server, AD).

Phase 2: VLAN Implementation and Security

- VLANs: Separate network traffic for improved security and performance.
    - VLAN 10: Management (Server VM)
    - VLAN 20: Sales & Marketing (Computer 1)
    - VLAN 30: Research & Development (Computer 2)
    - VLAN 40: Future Expansion (Computer 3)
- Firewalls: Installed on router and server VMs to control inbound and outbound traffic.
- Antivirus Solutions: Deployed on all VMs to protect against malware and cyber threats.
- Security Policies: Define acceptable use of network resources and access controls for file shares.

Phase 3: Data Management and Collaboration

- Backup Solution:
    - On-site: Daily backups of server and workstation data to a local NAS device.
    - Off-site: Weekly backups to a cloud storage service for disaster recovery.
    - Automated Scheduling: Regular backups with minimal user intervention.
- File Shares: Separate file shares in the central server for each department with access controls.
- Mount Points: Map file shares to corresponding workstations for easy access.

Phase 4: IT Onboarding and Automation

- IT Onboarding Policy: Document procedures for new employees:
    - Account creation in AD and file shares.
    - Device setup with software installs and network access.
    - Security training on company policies and best practices.
- VM Deployment Scripts: Automate VM deployment for server, router, and workstations with pre-configured VLAN memberships.
- Windows Server Script: Automate server deployment with PowerShell, including:
    - Static IP address and DNS assignment.
    - Renaming VM.
    - Installing AD-Domain-Services.
    - Creating AD Forest, OUs, and users.
    - Configuring DNS and Domain Controller roles.
    - Network integration with existing infrastructure.

Phase 5: Documentation and Reporting

- Comprehensive documentation for all components:
    - Network diagrams and configurations.
    - VM deployment details and scripts.
    - Backup and file share setups.
    - IT onboarding policy.
- Regular reports for network health and resource utilization.

Benefits:

- Improved Network Performance: Secure and efficient network infrastructure supports efficient communication and collaboration.
- Enhanced Data Security: Strong security measures and backup solutions protect sensitive data.
- Streamlined Workflows: File shares and access controls simplify document sharing and collaboration.
- Reduced Downtime: Robust backup solution ensures quick recovery in case of data loss.
- Efficient Onboarding: Standardized procedures provide smooth integration for new employees.

This SOP provides a comprehensive framework for the network upgrade project. The specific technologies and solutions can be customized based on the client's budget, security requirements, and future growth plans.