**Developing Organizational Standards for Systems**

A network design plan is a comprehensive document that outlines the structure, components, and configuration of a computer network. It serves as a blueprint for building, expanding, or upgrading a network infrastructure. The plan includes various elements and considerations to ensure the network meets the organization's requirements and supports its operations effectively. Here are some key components typically included in a network design plan:

1. Network Goals and Objectives: Clearly define the purpose and goals of the network design, such as enhancing performance, improving security, supporting scalability, or accommodating future technology advancements.

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Requirements** | **Completed** |
| Performance |  |  |
| Security |  |  |
| Scalability |  |  |
| Reliability |  |  |
| Manageability |  |  |
| Cost |  |  |

1. Network Topology: Identify the network's physical and logical layout, including the placement of routers, switches, servers, and other network devices. This may involve selecting the appropriate network architecture, such as wired and wireless networks.

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Requirements** | **Completed** |
| Physical Layout |  |  |
| Logical Layout |  |  |
| Data Flows | Camera, Data Backup, Data Holding and Archiving, Database Management, Education Material Flow, Email Communication, Employee Access, Financial Flow - Invoicing and Payment, Financial Flow – Payroll, Grading, HVAC, School Meals, School Transportation, Student Access, Web Content |  |
| Communication Layout |  |  |
| Redundancy |  |  |
| High Availability |  |  |
| Scalability |  |  |
| Traffic Segmentation |  |  |

1. IP Addressing Scheme: Define the IP addressing scheme to be used within the network, including IP ranges, subnets, and allocation of addresses to network devices. This ensures efficient routing and management of network resources.

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Requirements** | **Completed** |
| IP Addresses |  |  |
| Private IPs |  |  |
| Static IPs |  |  |
| Dynamic IPs |  |  |

1. Network Segmentation: Determine how the network will be segmented into smaller subnets or virtual LANs (VLANs) to enhance security, optimize network performance, and isolate network traffic. Think about zones of security to separate less secure devices and users from more secure devices and users. Network access control lists to allow/restrict specific types of traffic (see #7) between different networks (external to internal, VLAN to VLAN).

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Requirements** | **Completed** |
| Critical Systems |  |  |
| VLANS |  |  |
| Access Control |  |  |
| NAT |  |  |
| Firewalls |  |  |
| Monitoring |  |  |
| Best Practices |  |  |

1. Hardware and Software Requirements: Specify the hardware devices and software applications needed to support the network design, including routers, switches, firewalls, servers, network monitoring tools, and any specialized network equipment. Restrict non-approved services (e.g., cloud, software-as-a-service, etc.) and only allow approved services (policy to prevent “shadow IT”). Only approved devices.

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Requirements** | **Completed** |
| Routers |  |  |
| Switches |  |  |
| Firewalls |  |  |
| Servers |  |  |
| Storage |  |  |
| Other Network Devices |  |  |
| Operating Systems |  |  |
| Software Apps |  |  |
| Restricted Services |  |  |
| Not Allowed Devices |  |  |

1. Security Measures: Outline the security measures to be implemented within the network, such as firewalls, intrusion detection systems (IDS), virtual private networks (VPNs), access controls, and encryption protocols (in-transit), network access control. Monitoring of ingress and egress traffic.

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Requirements** | **Completed** |
| Firewalls |  |  |
| Intrusion Detection Systems (IDS) |  |  |
| Virtual Private Networks (VPNs) |  |  |
| Access Controls |  |  |
| Encryption Protocols |  |  |
| Network Access Control |  |  |
| Monitoring |  |  |

1. Network Services: Identify the required network services, such as DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System), email, file sharing, remote access, and any other network services critical to the organization's operations. List and identify only the approved ports, protocols, and services.

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Requirements** | **Completed** |
| Required Network Services | Camera, Data Backup, Data Holding and Archiving, Database Management, Education Material Flow, Email Communication, Employee Access, Financial Flow - Invoicing and Payment, Financial Flow – Payroll, Grading, HVAC, School Meals, School Transportation, Student Access, Web Content |  |
| DHCP (Dynamic Host Configuration Protocol) | Student endpoint devices |  |
| DNS (Domain Name System) |  |  |
| Email |  |  |
| File Sharing |  |  |
| Remote Access |  |  |

1. Network Management and Monitoring: Define the processes and tools for network management and monitoring, including network performance monitoring, configuration management, device backups, and incident response procedures.

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Requirements** | **Completed** |
| Network Performance Monitoring |  |  |
| Configuration Management |  |  |
| Device Backups |  |  |
| Incident Response Procedures |  |  |

1. Scalability and Redundancy: Consider the potential growth and scalability of the network, as well as the need for redundancy and failover mechanisms to ensure network availability and minimize downtime. End-of-life/end-of-support must be considered due to risk for scalability and redundancy.

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Requirements** | **Completed** |
| Scalability |  |  |
| Redundancy |  |  |
| Failover mechanisms |  |  |
| End-of-life/End-of-Support |  |  |

1. Implementation Plan: Provide a detailed roadmap for deploying the network design, including timelines, tasks, resource allocation, and any dependencies or considerations for integration with existing infrastructure.

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Requirements** | **Completed** |
| Timeline |  |  |
| Resource Allocation |  |  |
| Dependencies |  |  |
| Integration |  |  |
| Testing |  |  |
| Training |  |  |
| Documentation |  |  |
| Monitoring |  |  |

1. Support Services: Consider internal IT/managed service providers/telecom providers, vendor risk management (e.g., are they meeting security requirements), and service level agreements.

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Requirements** | **Completed** |
| Support Services |  |  |
| Internal IT Support |  |  |
| External Vendors |  |  |
| Service Level Agreements (SLAs) |  |  |
| Monitoring |  |  |
| Maintenance |  |  |

A well-prepared network design plan serves as a guide for network administrators, engineers, and IT teams involved in building, operating, and maintaining the network infrastructure. It helps ensure a consistent and optimized network design that aligns with the organization's requirements, security policies, and future growth plans.