# ISO 27001 Network Diagram Template

## Introduction:

This document provides the structure and guidance for creating a network diagram aligned with ISO 27001 requirements. A network diagram is a visual representation of an organization's IT infrastructure, detailing how systems, devices, and networks interconnect. It ensures that network assets are documented, security risks are identified, and compliance with the Information Security Management System (ISMS) is maintained.

## 1. Purpose of the Network Diagram

The purpose of the network diagram is to:  
1. Provide a clear overview of the organization’s IT infrastructure, including critical systems and data flows.  
2. Facilitate risk assessments by identifying network vulnerabilities and dependencies.  
3. Support compliance with ISO 27001 controls related to network security (e.g., A.13.1, A.14.1).  
4. Assist in incident response and disaster recovery planning by detailing network dependencies.  
5. Enable secure planning for changes to the network architecture.

## 2. Elements of the Network Diagram

* Perimeter Devices: Firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS).
* Internal Network Devices: Routers, switches, and wireless access points.
* Servers: Application servers, database servers, file servers, and web servers.
* Endpoints: Laptops, desktops, mobile devices, and other connected devices.
* Data Flow: Visualize the flow of sensitive data between components (e.g., internal databases to external vendors).
* Cloud Services: Represent cloud-based resources and their integration with the internal network.
* Third-Party Connections: Connections to external partners, vendors, or remote users.
* DMZ (Demilitarized Zone): Outline any public-facing systems or servers.

## 3. Compliance Mapping to ISO 27001 Example

The network diagram aligns with the following ISO 27001 controls, ensuring secure configuration and compliance:

| ISO 27001 Control | Control Description | Network Diagram Impact |
| --- | --- | --- |
| A.13.1 | Network Security Management | Illustrates secure configuration of network components. |
| A.14.1 | Secure Development | Details secure architecture for application environments. |
| A.8.1 | Asset Management | Identifies and tracks critical network assets. |
| A.18.1 | Compliance with Legal and Contractual Requirements | Ensures compliance with regulatory requirements. |

## 4. Incident Response Mapping

The network diagram supports incident response planning by identifying critical systems and dependencies. Highlight high-risk systems, key access points, and data flows to streamline isolation and recovery during incidents.

## 5. Guidelines for Creating the Network Diagram

* Asset Identification: Ensure all network components are identified and documented in the Asset Register.
* Layered Security Visualization: Represent the network in layers (e.g., perimeter, internal network, cloud, and endpoints).
* Segmentation: Show network segmentation and isolation of sensitive systems.
* Access Points: Highlight areas where external access occurs (e.g., VPN connections, cloud endpoints).
* Security Control Tags: Label systems and connections with implemented security measures (e.g., encrypted, firewalled).

## 6. Tools and Recommendations

* Diagramming Tools: Use tools like Microsoft Visio, Lucidchart, or Draw.io to create the network diagram.
* Automation: Leverage network discovery tools (e.g., SolarWinds, NetBrain) to automate mapping and updates.
* Periodic Updates: Regularly review and update the diagram to reflect changes in the network infrastructure.

## 7. Metrics for Network Diagram Effectiveness

* Percentage of network components accurately documented in the diagram.
* Frequency of updates to the network diagram (e.g., monthly, quarterly).
* Time taken to isolate critical systems during an incident.
* Number of vulnerabilities identified and addressed through diagram review.

## 8. Roles and Responsibilities

Network Administrator:  
- Maintain and update the network diagram.  
- Ensure all components are properly documented.

Information Security Manager (ISM):  
- Validate the diagram’s alignment with ISMS requirements.  
- Conduct risk assessments based on the diagram.

IT Operations Team:  
- Implement and monitor network security controls.  
- Ensure compliance with security policies.

## 9. Revision and Maintenance

This document and the network diagram will be reviewed and updated [Insert frequency, e.g., annually or as needed] to reflect changes in the network infrastructure or compliance requirements.

## 10. Approval

| Name | Title | Date |
| --- | --- | --- |
|  |  |  |
|  |  |  |