

# Network Monitoring Policy Sample

## 1. Purpose

The purpose of this Network Monitoring Policy is to define requirements for monitoring all computer networks to ensure availability, integrity, and security of organizational data and resources.

## 2. Scope

This policy applies to all networks, systems, devices, and personnel that connect to or interact with the company's network infrastructure.

## 3. Policy

- All network activity must be monitored for the purpose of detecting and responding to security threats, performance issues, and unauthorized actions.
- Monitoring tools and systems must be configured and managed by authorized IT personnel.
- Alert thresholds must be established to identify unusual behavior, outages, or security events.
- Access to monitoring data must be restricted to authorized employees with a legitimate need to know.
- Logs and collected data shall be retained according to the organization's data retention policy.
- Regular reviews must be performed to assess monitoring effectiveness and address gaps.

## 4. Responsibilities

- **IT Department:** Manage network monitoring tools, analyze logs, and respond to incidents.
- **Employees:** Report any suspected network issues or security incidents.
- **Management:** Ensure adequate resources and support for network monitoring.

## 5. Enforcement

Violations of this policy may result in disciplinary action, up to and including termination of employment and legal action.

## 6. Review and Updates

This policy will be reviewed annually or as required to reflect changes to business and technical requirements.