2024

NETWORK MANGEMENT POLICY

NEW HAMPTON MUNICIPAL COMMUNICATIONS UTILITY

AUGUST 12, 2024

Contents

Network Management Policy

1. Introduction

This Network Management Policy outlines the practices and procedures employed by New Hampton Municipal Utilities (NHMU) to manage its network. This policy aims to ensure optimal performance, security, and reliability of the network for all users.

2. Objectives

- **Performance:** Ensure the network operates at peak efficiency.
- **Security:** Protect network integrity and user data.
- **Reliability:** Maintain high availability and minimize downtime.
- **Compliance:** Adhere to relevant regulations and industry standards.

3. Scope

This policy applies to all network devices, connections, and users within NHMU's infrastructure, including employees, contractors, and customers.

4. Network Management Practices – Additional information is available at www.nhmu.com in the links for NHMU's Interconnection Policy and Communications Service Policy.

4.1 Traffic Management

- **Bandwidth Allocation:** Allocate bandwidth to prevent network congestion and ensure fair usage.
- **Traffic Prioritization:** Prioritize critical services (e.g., emergency services) and latency-sensitive applications (e.g., VoIP).
- **Traffic Shaping:** Implement traffic shaping to manage data flow and reduce network congestion during peak times.

4.2 Monitoring and Performance Management

- **Continuous Monitoring:** Employ tools to continuously monitor network performance and health.
- **Performance Metrics:** Track key performance indicators (KPIs) such as latency, packet loss, jitter, and throughput.
- **Alerting and Reporting:** Set up alerts for anomalies and generate regular performance reports.

4.3 Security Management

- **Access Control:** Implement strict access control measures to restrict unauthorized access.

- **Encryption:** Use encryption protocols to protect data in transit.
- **Threat Detection:** Deploy intrusion detection and prevention systems (IDS/IPS) to identify and mitigate security threats.
- **Regular Audits:** Conduct regular security audits and vulnerability assessments.

4.4 Fault Management

- **Incident Response:** Establish an incident response plan to address network issues promptly.
- **Root Cause Analysis:** Perform root cause analysis for significant incidents to prevent recurrence.
- **Redundancy and Failover:** Implement redundancy and failover mechanisms to enhance network resilience.

4.5 Configuration Management

- **Standardization:** Use standardized configurations for network devices to ensure consistency.
- **Change Management:** Follow a formal change management process for network modifications.
- **Backup and Recovery:** Maintain regular backups of configuration files and critical data.

4.6 Customer Support

- **Help Desk:** Provide 24/7 customer support through a dedicated help desk.
- **Service Level Agreements (SLAs):** Define SLAs to set expectations for network performance and issue resolution times.
- **User Education:** Educate customers about best practices for network usage and security.

5. Compliance and Legal Requirements

- **Data Privacy:** Comply with data privacy laws and regulations, such as GDPR or CCPA.
- **Industry Standards:** Adhere to industry standards and best practices, such as ITIL or ISO/IEC 27001.
- **Regulatory Compliance:** Ensure compliance with relevant telecommunications and cybersecurity regulations.

6. Review and Revision

This policy will be reviewed annually or as required to accommodate changes in technology, regulatory requirements, or business needs. Revisions will be communicated to all relevant stakeholders.

7. Contact Information

For questions or concerns regarding this policy, please contact:

New Hampton Municipal Utilities
112 E Main Street
New Hampton, IA 50659
641-394-4550
info@nhmu.com