Oso Internet Solutions Network Management Policy

Version: 1.8
Effective Date: 10/01/2022
Review Cycle: Annual
Approved By: Margaret Merrill/ Owner

---

1. Purpose

The purpose of this Network Management Policy is to define the standards and procedures for the configuration, monitoring, and maintenance of Oso Internet Solutions' network infrastructure. This ensures availability, performance, scalability, and security for business-critical operations.

---

2. Scope

This policy applies to all employees, contractors, vendors, and third-party users who access, manage, or interact with the network resources of Oso Internet Solutions, including wired and wireless infrastructure, routers, switches, firewalls, VPNs, and cloud-based networks.

---

3. Responsibilities

3.1 Network Administrator(s)

- Ensure network availability and performance.
- Monitor network traffic and bandwidth utilization.
- Apply security patches and firmware updates.
- Maintain documentation of network diagrams and configurations.
- Respond to and investigate network incidents.

3.2 IT Security Officer

- Enforce network security protocols.
- Perform vulnerability assessments.
- Audit network access and activities.

- Approve network changes based on risk assessments.

3.3 End Users

- Use the network for authorized business purposes.
- Avoid activities that degrade network performance.
- Report suspicious activity or service degradation promptly.

---

4. Network Configuration Standards

- All network devices must be configured with strong authentication and encryption.
- Default passwords must be changed before deployment.
- Network equipment must be named consistently (e.g., based on location/function).
- VLANs must be used to segment traffic by department and sensitivity.
- Only approved ports and protocols shall be open on firewalls and routers.

---

5. Access Control

- Access to network infrastructure must be role-based and follow the principle of least privilege.
- Administrative access must require multi-factor authentication (MFA).
- VPN access must be logged, encrypted, and time-bound for remote users.
- Wi-Fi networks must be secured with WPA3 encryption (or WPA2 minimum) and segmented for guest access.

---

6. Monitoring and Logging

- All network traffic must be monitored using approved tools.
- Logs must include connection attempts, device changes, and traffic anomalies.
- Logs must be retained for at least 12 months and reviewed monthly.
- Intrusion detection and prevention systems (IDPS) must be active on all edge networks.

---

7. Maintenance and Updates

- Firmware updates must be applied quarterly or as required by security advisories.
- Network redundancy and failover must be tested annually.
- Backups of device configurations must be stored securely and tested monthly.
- Scheduled maintenance must be communicated at least 48 hours in advance.

---

8. Incident Response

- All network incidents must be reported to the IT department within 1 hour.
- Affected systems must be isolated until the issue is resolved.
- Root cause analysis must be conducted for major incidents.
- A report must be filed within 72 hours post-incident.

---

9. Compliance and Audits

- This policy complies with industry best practices and any applicable legal/regulatory requirements (e.g., GDPR, HIPAA if applicable).
- Internal audits must be conducted semi-annually.
- Non-compliance may result in disciplinary action or loss of access privileges.

---

10. Policy Review and Revisions

- This policy will be reviewed annually by the IT leadership team.
- Any revisions must be approved by executive management and communicated organization-wide.

Policy Owner: Ryan Merrill CTO/COO
Contact: ryan@osointernetsolutions.com