iWiSP llc
PO Box 207
Partlow VA 22534
www.iwisp.net

Network Management Policy for iWiSP LLC

1. Purpose
The purpose of this network policy is to ensure the secure, efficient, and reliable operation of iWiSP LLC's network infrastructure while promoting the responsible use of network resources.

2. Scope
This policy applies to all employees, contractors, and third-party users who access or utilize iWiSP LLC's network resources.

3. Network Security
iWiSP LLC will implement robust security measures to protect the network from unauthorized access, data breaches, malware, and other security threats. This includes the use of firewalls, intrusion detection systems, encryption, and regular security audits.

4. Access Control
Access to iWiSP LLC's network resources will be granted based on the principle of least privilege, ensuring that users have access only to the resources necessary for their roles. User authentication and authorization mechanisms will be employed to control access to sensitive data and critical network components.

5. Acceptable Use
All users are expected to adhere to iWiSP LLC's acceptable use policy, which outlines the permitted and prohibited uses of the company's network resources. This includes refraining from unauthorized access, distribution of malicious software, and engaging in activities that may compromise network security or performance.

6. Data Protection
iWiSP LLC will implement data protection measures to safeguard sensitive and confidential information transmitted over the network. This includes the use of encryption, data loss prevention mechanisms, and regular backups to prevent data loss or unauthorized disclosure.

7. Network Monitoring and Management
The network will be subject to continuous monitoring to identify and address performance issues, security incidents, and potential vulnerabilities. Routine maintenance and updates will be performed to ensure optimal network performance and reliability.

8. Compliance
iWiSP LLC's network management practices will comply with applicable laws, regulations, and industry standards related to data privacy, security, and network operations.

9. Reporting Security Incidents
All users are responsible for promptly reporting any suspected security incidents, unauthorized access attempts, or other network-related issues to the designated IT personnel or security team.

10. Policy Review
This network policy will be periodically reviewed and updated to reflect changes in technology, security threats, and regulatory requirements.

11. Enforcement
Non-compliance with this network policy may result in disciplinary action, including but not limited to suspension of network privileges, termination of employment, or legal action as appropriate.