IFIN Global Group

Network Management Policy

1. Purpose

The purpose of this policy is to establish guidelines for managing and securing the network infrastructure of IFIN Global Group. This policy aims to ensure network availability, integrity, and confidentiality while supporting the company's operational needs.

2. Scope

This policy applies to all employees, contractors, vendors, and any other parties who have access to IFIN Global Group's network infrastructure. It covers all network devices, systems, and connections within the company.

3. Network Management Objectives

- **Security**: Protect network resources from unauthorized access and threats.
- **Performance**: Ensure the network operates efficiently and effectively.
- **Reliability**: Maintain network availability and minimize downtime.
- **Compliance**: Adhere to relevant laws, regulations, and industry standards.

4. Roles and Responsibilities

- **Network Administrators**: Responsible for configuring, monitoring, and maintaining network devices and services.
- **IT Security Team**: Ensures network security measures are implemented and updated.
- **IT Support Staff**: Provides technical support and handles network-related issues reported by users.
- **Employees and Users**: Adhere to network usage policies and report any security incidents or network problems.

5. Network Design and Architecture

- **Segmentation**: Implement network segmentation to enhance security and performance.
- **Redundancy**: Design the network with redundancy to ensure high availability.
- **Scalability**: Ensure the network can scale to accommodate future growth and new technologies.

6. Access Control

- **User Authentication**: Implement strong authentication mechanisms for network access.
- **Authorization**: Define user roles and access levels based on job requirements.
- **Remote Access**: Use secure VPNs and multi-factor authentication for remote access.

7. Network Security

- **Firewalls**: Deploy firewalls to protect network boundaries.
- **Intrusion Detection and Prevention**: Implement IDS/IPS to detect and mitigate threats.
- **Anti-Malware**: Use anti-malware solutions to protect against viruses and other malicious software.
- **Encryption**: Encrypt sensitive data in transit and at rest.
- **Production Environment Security**: Implement strict access controls, regular security assessments, and real-time monitoring to ensure the security and integrity of the production environment. Only authorized personnel should have access to the production environment.

8. Network Monitoring and Maintenance

- **Monitoring**: Continuously monitor network performance and security.
- **Patch Management**: Regularly update network devices with the latest firmware and patches.
- **Backups**: Perform regular backups of network configurations and critical data.

9. Incident Response

- **Incident Reporting**: Establish a process for reporting network security incidents.
- **Response Plan**: Develop and maintain an incident response plan to address and mitigate network incidents.
- **Recovery**: Ensure rapid recovery of network services following an incident.

10. Compliance and Audit

- **Regulatory Compliance**: Ensure the network adheres to relevant regulations (e.g., GDPR, HIPAA).
- **Regular Audits**: Conduct regular network audits to identify and address vulnerabilities and ensure policy compliance.

11. User Education and Awareness

- **Training**: Provide regular training on network security best practices for employees.
- **Awareness Programs**: Conduct awareness programs to inform users about potential threats and safe network usage.

12. Policy Review and Updates

- **Periodic Review**: Review the network management policy annually or when significant changes occur in the network environment.
- **Updates**: Update the policy as necessary to reflect new technologies, threats, and business needs.

13. Enforcement

- **Compliance Monitoring**: Monitor compliance with this policy.
- **Disciplinary Actions**: Define consequences for policy violations, including disciplinary actions up to termination of employment.

14. Production Environment Security

Ensure the security and integrity of the production environment by implementing strict access controls, conducting regular security assessments, and performing real-time monitoring. Access to the production environment should be limited to authorized personnel, with all access being logged and reviewed periodically.

15. Force Reauthentication

Require users to reauthenticate at regular intervals to maintain security. This includes reauthentication after a set period of inactivity, during high-risk activities, and when accessing sensitive information or systems. This helps mitigate the risk of unauthorized access due to session hijacking or other security breaches.

16. Prohibit Remote Access Clients from Split Tunneling

To enhance security, remote access clients are prohibited from using split tunneling. This ensures that all remote traffic is routed through the company's secure VPN, preventing direct access to the internet that could expose the network to threats. This policy helps protect sensitive data and maintain the integrity of the corporate network.

Conclusion

The network management policy of IFIN Global Group is vital for maintaining a secure, reliable, and efficient network infrastructure. Adherence to this policy is mandatory for all users to protect the company's network resources and ensure operational continuity.