**Network Infrastructure Policy**

## 1. Purpose

This policy outlines the framework for securing, managing, and maintaining the network infrastructure at DevEngineer. It provides guidelines to ensure the integrity, confidentiality, and availability of the network and its components. The policy applies to all employees, contractors, and third-party service providers involved in network operations.

## 2. Scope

This policy covers all aspects of the network infrastructure, including but not limited to:

- Network Segmentation
- Access Control
- Monitoring and Logging
- Patch Management
- Incident Response
- Third-Party Compliance
- Disaster Recovery and Redundancy

## 3. Definitions

- **DMZ (Demilitarized Zone)**: A network area that separates internal systems from external networks to add an additional security layer.
- **VLAN (Virtual Local Area Network)**: A network configuration that segments networks at the data link layer for enhanced security and performance.
- **IDS (Intrusion Detection System)**: A system designed to monitor network traffic for suspicious activities.
- **IPS (Intrusion Prevention System)**: A system that actively prevents detected threats from affecting network operations.

## 4. Roles and Responsibilities

- **Network Administrator**: Responsible for managing network security tools, maintaining system updates, and ensuring compliance with this policy.
- **Security Team**: Responsible for monitoring network activity, responding to security incidents, and conducting regular security audits.
- **Employees and Third Parties**: Expected to follow access control policies and report any suspicious activity or network issues to the IT team.

## 5. Network Segmentation

- **Internal and External Networks**: Networks must be segmented using VLANs and DMZs to limit traffic between internal systems and external networks.
- **Micro-Segmentation**: For critical assets, micro-segmentation will be employed to further isolate sensitive data from unauthorized access.

### 6. Access Control

- **Role-Based Access Control (RBAC)**: Access to the network infrastructure will be granted based on job roles and responsibilities.
- **Multi-Factor Authentication (MFA)**: All remote and administrative access to network components will require MFA to enhance security.
- **Third-Party Access**: Access to the network by third-party vendors will be limited and monitored to ensure compliance with internal security protocols.

### 7. Monitoring and Logging

- **Real-Time Monitoring**: The network will be continuously monitored for security events using IDS and IPS systems.
- **Audit Logs**: Logs of all network activities will be maintained for a minimum of 12 months and regularly reviewed to detect potential threats.
- **Behavioral Analytics**: Anomalous behavior will be flagged using advanced detection techniques to identify possible security incidents.

### 8. Patch Management

- **Regular Updates**: All network components (e.g., firewalls, routers, switches) must be regularly updated with the latest security patches.
- **Testing Before Deployment**: Security patches and updates will be tested in a staging environment before being applied to the production network.

### 9. Incident Response

- **Incident Reporting**: Security incidents affecting the network infrastructure must be reported within one hour of detection.
- **Response Time**: Incidents must be investigated, and containment measures applied within 24 hours. A full report will be completed within five days.
- **Post-Incident Review**: After each incident, a review will be conducted to determine root causes and improve the network security posture.

### 10. Network Redundancy and Disaster Recovery

- **Redundancy Measures**: Critical network infrastructure components will have redundant systems to ensure high availability.
- **Disaster Recovery Plan**: A disaster recovery plan will be developed and regularly tested to ensure that network operations can be restored within a 48-hour window after a significant outage or failure.

### 11. Third-Party Compliance

- All third-party vendors providing network services must adhere to the same security standards outlined in this policy.

- Vendor access will be continuously monitored, and compliance audits will be conducted annually.

### 12. Training and Awareness

- Employees and network administrators will undergo annual training to stay updated on network security best practices and policy requirements.
- Ongoing security awareness campaigns will be conducted to educate users about emerging threats and proper use of the network infrastructure.

### 13. Compliance and Review

- This policy complies with all relevant laws, regulations, and industry standards, including ISO 27001, NIST, and GDPR.
- The policy will be reviewed annually or after any major security incident to ensure continued relevance and effectiveness.

### 14. Enforcement

Non-compliance with this policy will result in disciplinary action, including termination of employment or contract, and may also involve legal penalties where applicable.

---

### Revision History

| Version | Date | Changes | Approved By |
|---|---|---|---|
| 1.0 | 25 August | Initial policy creation | Chief Security Officer |