Network Security Policy

Approved by	Signature	Effective Date
Security Team	Official Security Team Approved	03/11/2025

1. Purpose

This policy establishes standards and controls for securing DanfeCorp's network infrastructure. It aims to protect against unauthorized access, data breaches, and cyber threats by defining guidelines for network security, monitoring, and incident response.

2. Scope

This policy applies to all employees, contractors, third-party vendors, and any other individuals who access DanfeCorp's network resources. This includes wired and wireless networks, cloud environments, and remote connections.

3. Roles and Responsibilities

The following roles have specific responsibilities for maintaining network security:

- **IT Security Team:** Oversees network security, monitors for threats, and enforces compliance.
- **Network Administrators:** Implement security controls, maintain network infrastructure, and manage access.
- **Employees and Contractors:** Adhere to security guidelines and report any suspicious network activity.
- **Third-Party Vendors:** Comply with DanfeCorp's network security requirements when accessing systems.

4. Network Security Controls

4.1 Access Control

- Network access is granted based on the principle of least privilege.
- Role-based access control (RBAC) is enforced for sensitive network segments.
- Multi-Factor Authentication (MFA) is required to access critical network resources.

4.2 Network Segmentation

- Separate networks are maintained for internal users, guest access, and third-party vendors.

- Critical systems and sensitive data are isolated from general access networks.

4.3 Firewall and Intrusion Prevention

- Firewalls are deployed at all network perimeters with strict access control rules.
- Intrusion Detection and Prevention Systems (IDPS) continuously monitor for suspicious activity.

4.4 Wireless Network Security

- Only company-approved wireless networks may be used for business operations.
- Wireless networks must be encrypted using WPA3 or an equivalent security protocol.
- Guest Wi-Fi is segregated from internal business networks.

4.5 Remote Access Security

- Remote access must be established through company-approved VPNs with strong encryption.
- Secure Shell (SSH) and Remote Desktop Protocol (RDP) access must be restricted and monitored.
- Remote access logs are reviewed regularly for anomalies.

5. Network Monitoring and Logging

Monitoring Requirement	Implementation Details
Traffic Monitoring	All network traffic is continuously monitored for threats, unusual activity, and policy violations.
Log Management	Logs from firewalls, IDPS, and other security systems are retained and periodically reviewed.
Alerting System	Automated alerts are configured to notify security personnel of potential security incidents.

6. Patch Management and System Updates

- All network devices, including routers, switches, and firewalls, must be patched regularly.
- Critical security patches must be applied within an appropriate timeframe based on risk assessments.
- Vulnerability scans are conducted periodically to identify outdated software and misconfigurations.

7. Incident Response and Reporting

- All network security incidents must be reported immediately to the IT Security Team.
- Established incident response procedures must be followed to contain, investigate, and remediate threats.

- Post-incident reviews are conducted to enhance network security controls and update response strategies.

8. Compliance and Auditing

- Regular network security audits are conducted to ensure compliance with internal policies and regulatory requirements.
- Security policies and controls are updated based on audit findings and evolving threat intelligence.

9. Policy Review and Updates

This policy will be reviewed and updated annually or upon significant changes to DanfeCorp's network infrastructure, regulatory requirements, or the cybersecurity landscape. The security team will approve all updates.

This policy document supersedes all previous network security guidelines and becomes effective as of the date specified above. All departments must align their operations with these requirements within 30 days of the effective date.

For questions or clarifications regarding this policy, contact the Security Team via secure channels only.