Logging and Monitoring Policy

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

1. Purpose

This policy defines the logging and monitoring requirements necessary to detect, investigate, and respond to security incidents and operational issues. It ensures that DanfeCorp maintains an effective security posture by capturing and analyzing relevant system and network activity across the enterprise infrastructure.

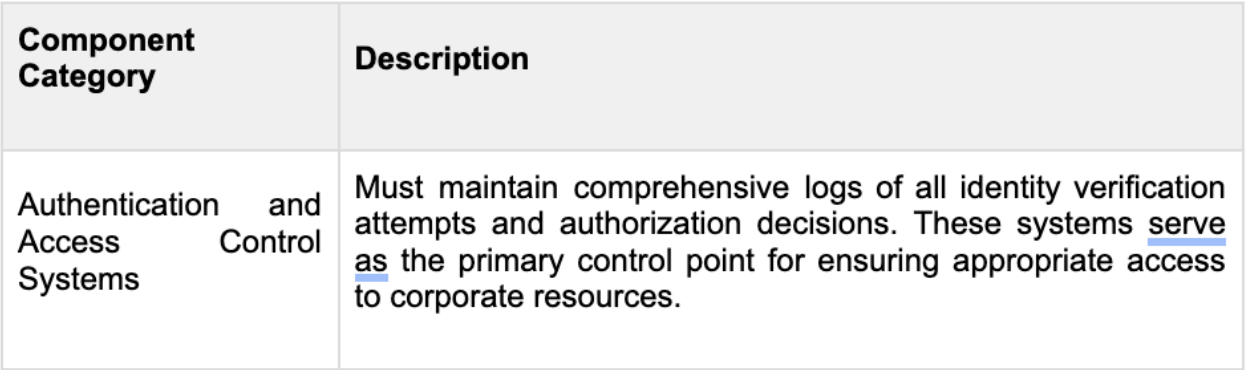
2. Scope

This policy applies to all employees, contractors, vendors, and any other individuals who access DanfeCorp's systems, applications, networks, or data. It covers all IT assets, including servers, workstations, applications, databases, and network devices, regardless of physical location or hosting environment.

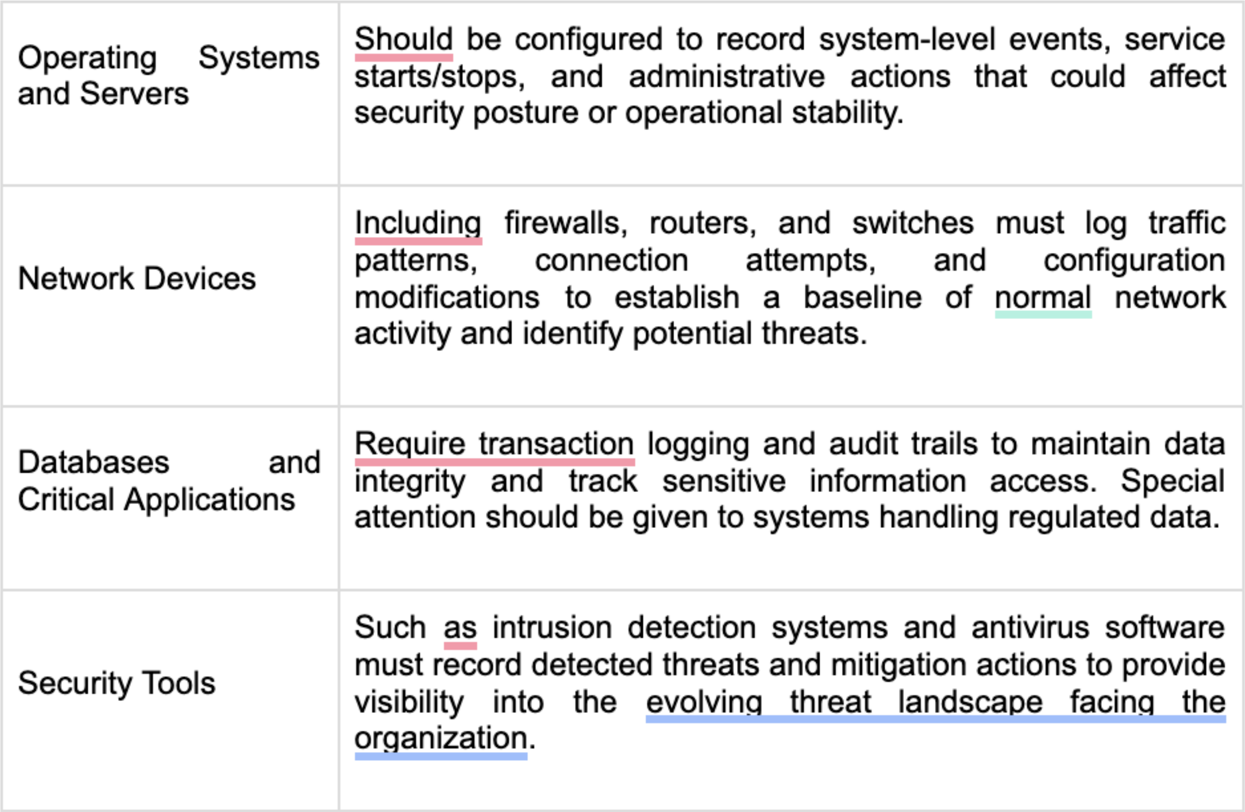
3. Logging Requirements

3.1 Log Sources

Logging must be enabled for the following critical components within the DanfeCorp technology ecosystem:



Component Category	Description
Authentication and Access Control Systems	Must maintain comprehensive logs of all identity verification attempts and authorization decisions. These systems serve as the primary control point for ensuring appropriate access to corporate resources.



Operating Systems and Servers	Should be configured to record system-level events, service starts/stops, and administrative actions that could affect security posture or operational stability.
Network Devices	Including firewalls, routers, and switches must log traffic patterns, connection attempts, and configuration modifications to establish a baseline of normal network activity and identify potential threats.
Databases and Critical Applications	Require transaction logging and audit trails to maintain data integrity and track sensitive information access. Special attention should be given to systems handling regulated data.
Security Tools	Such as intrusion detection systems and antivirus software must record detected threats and mitigation actions to provide visibility into the evolving threat landscape facing the organization.

3.2 Log Content

All logs must capture relevant security and operational details, including:

Required Element	Implementation Guidance
Timestamps	Synchronized with a reliable time source using enterprise NTP
User and System Activities	Contextual information including affected resources
Authentication Attempts	Record both successful and failed login events
Privileged Access	Detailed tracking of all administrative actions and changes
Configuration Changes	Modifications to system settings and security configurations with sufficient detail to understand both the previous and new state where technically feasible
Data Access and Modifications	Recorded with particular emphasis on interactions with sensitive or regulated information
Security Events	Detected threats and mitigation actions correlated with current threat intelligence

3.3 Log Retention and Protection

Log retention requirements are established to balance operational needs, security investigations, and compliance obligations:

Requirement	Specification	Implementation Details
Retention Period	Minimum of one year total retention	At least 90 days must be readily accessible
Storage	Secure, centralized log management system	Implement strict access controls
Integrity Protection	Prevention of unauthorized modifications	Use cryptographic verification when possible

4. Monitoring and Alerting

4.1 Continuous Monitoring

The security operations function must implement:

- **Real-Time Monitoring:** Security logs must be continuously monitored for anomalies and potential security threats using automated tools augmented by analyst review.
- **Automated Alerts:** Critical security incidents must trigger automated alerting mechanisms for immediate review by appropriate personnel according to severity-based escalation paths.

Monitoring effectiveness should be periodically assessed through targeted testing and validation exercises to ensure that detection capabilities remain aligned with the current threat landscape facing DanfeCorp.

4.2 Incident Detection and Response

When security events are detected, the following process flow applies:

Phase	Activities	Responsible Parties
Analysis	Assessment of security events and impact determination	Security analysts
Escalation	Immediate routing of high-risk incidents	Security Team leads
Forensic Review	Use of logs as evidence in investigations	Incident response personnel

5. Access Controls for Logs

Access to logging systems and log data represents a sensitive security control point that requires appropriate restrictions:

Restricted Access: Only authorized personnel may access system logs based on job responsibilities and security clearance. The principle of least privilege must be applied consistently across all logging systems.

Role-Based Access: Controls must limit log visibility based on job roles and business necessity. Differentiated access levels should be implemented to separate standard operational access from security investigation privileges.

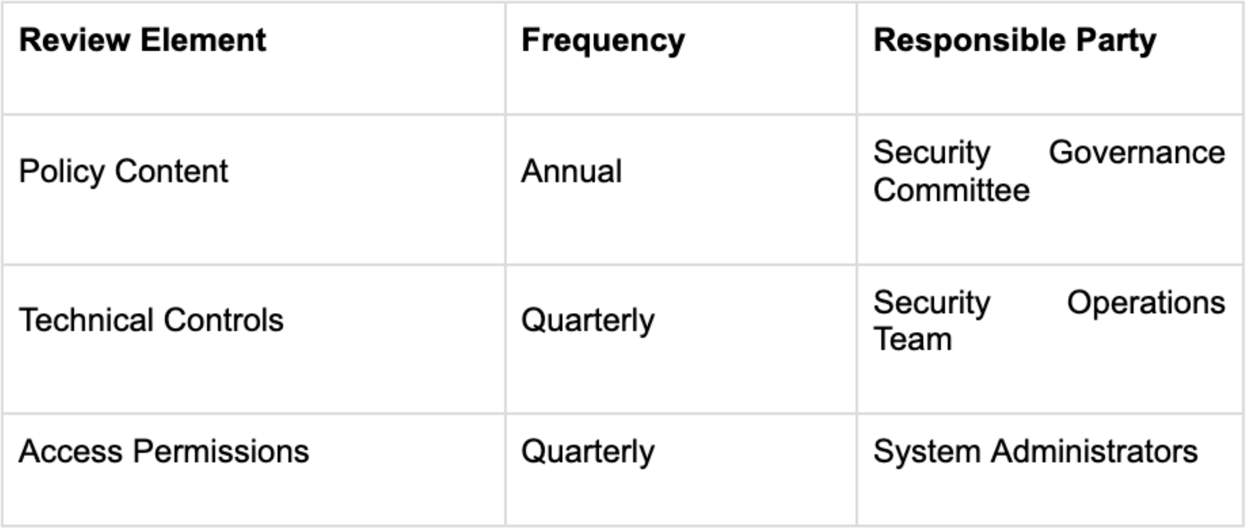
Regular Reviews: Access permissions must be conducted quarterly to prevent privilege creep and ensure that terminated employees no longer retain access to sensitive log data.

6. Policy Compliance and Enforcement

To ensure ongoing adherence to this policy:

Audits: Regular audits will be performed to verify compliance with this policy through both automated assessment tools and manual review processes. These audits will evaluate both technical implementation and operational practices.

Disciplinary Action: Non-compliance with logging and monitoring standards may result in disciplinary actions according to the corporate acceptable use policy and employee handbook. The severity of disciplinary action will be proportional of the compliance violation's potential impact.



Review Element	Frequency	Responsible Party
Policy Content	Annual	Security Governance Committee
Technical Controls	Quarterly	Security Operations Team
Access Permissions	Quarterly	System Administrators

This policy document supersedes all previous logging and monitoring 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.