DANFECORP

Encryption Management Policy

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

1. Purpose

This policy establishes the standards, processes, and practices for managing encryption across all systems, applications, and networks at DanfeCorp. It is designed to ensure the confidentiality, integrity, and security of sensitive and personal data by employing robust encryption mechanisms for data at rest, in transit, and in use.

2. Scope

This policy applies to all DanfeCorp systems, applications, networks, and data that contain or process sensitive information. It covers all IT assets, including databases, file systems, backup media, cloud storage, and any third-party services used for encryption or key management.

3. Definitions

- **Encryption:** The process of transforming data into a secure format to prevent unauthorized access.
- **Data at Rest:** Data stored on any physical or virtual medium that is not actively being accessed or transmitted.
- **Data in Transit:** Data that is actively being transmitted over a network.
- **Data in Use:** Data that is actively being processed or manipulated within a system.
- **Encryption Key:** A string of data used by an algorithm to perform encryption or decryption.
- **Key Management System (KMS):** A secure solution for generating, storing, and managing encryption keys.

4. Encryption Requirements

4.1 Data at Rest

- **Data Protection:** All sensitive or proprietary dataâ€”including personal, financial, and intellectual property dataâ€—must be encrypted when stored in databases, file systems, backup media, and cloud storage.
- **Algorithm Standards:** Encryption must be implemented using industry-standard algorithms (e.g., AES-256 or stronger).
- **Key Separation:** Encryption keys must be managed and stored separately from the encrypted data using a secure key management solution.

4.2 Data in Transit

Communication Type	Encryption Requirement	Implementation Standard
Network Transmissions	All sensitive or personal data transmitted over networks	Secure transmission protocols (e.g., TLS 1.2 or higher for HTTP, IPsec or VPN for private networks)
Email Communications	Email containing sensitive data	Secure email protocols or encryption methods
API Communications	Data transmitted via APIs	HTTPS to ensure data privacy during transmission

4.3 Data in Use

- **Processing Protection:** Where feasible, encryption should be applied to data during processingâ€”especially in shared or multi-tenant environments where the risk of unauthorized access is elevated.
- **Alternative Controls:** When full encryption of data in use is not feasible, additional security controls such as access controls, monitoring, and logging must be implemented.

5. Key Management

5.1 Key Generation

Encryption and decryption keys must be generated using secure cryptographic algorithms in a secure environment to prevent unauthorized access.

5.2 Key Storage

- All encryption keys must be stored in a secure Key Management System (KMS) with access restricted to authorized personnel.
- Key management must follow the principle of least privilege, ensuring that only necessary personnel have access.

5.3 Key Rotation and Expiry

- **Rotation Schedule:** Encryption keys must be rotated regularly, with a minimum rotation period of 12 months or immediately after any potential compromise.
- **Expiration Management:** All keys must have an expiration date; once expired, keys must be securely archived or destroyed.
- **Formal Policy:** A formal key rotation policy must be established, including procedures for key renewal and expiration.

5.4 Key Revocation

- In the event of a security breach or key compromise, affected encryption keys must be immediately revoked and replaced.
- A documented process for revoking and replacing keys must be enforced.

6. Access Control

Control Type	Implementation Requirement
Access Restrictions	Access to encryption keys and encrypted data must be restricted to authorized individuals based on role and necessity
Authentication	Strong authentication mechanisms, such as multi-factor authentication, must be used to access encryption keys or encrypted data
Monitoring	Encryption key access logs must be regularly monitored and audited

7. Data Integrity and Non-Repudiation

Data integrity must be maintained using secure hashing algorithms and digital signatures. Critical transactions and communications involving sensitive data must be digitally signed to ensure non-repudiation. Logs related to encryption key usage and access to encrypted data must be stored securely and be auditable.

8. Auditing and Monitoring

- **Regular Audits:** Regular audits of encryption practices and key management processes must be conducted to ensure compliance with this policy.
- **Log Review:** Logs of encryption activities, including key management and access to encrypted data, must be generated and reviewed to detect unauthorized access attempts.
- **Incident Investigation:** Any anomalies or potential security breaches must be promptly investigated and addressed.

9. Compliance and Legal Requirements

- **Regulatory Adherence:** Encryption practices must comply with all applicable legal, regulatory, and contractual obligations, including data protection laws.
- **Standards Monitoring:** DanfeCorp will continuously monitor relevant laws and industry standards, updating encryption practices as necessary to maintain compliance.
- **Security Review:** All encryption practices will be periodically reviewed to ensure they meet evolving security requirements.

10. Incident Response

In the event of an encryption-related security incident, DanfeCorp will activate its Incident Response Plan to mitigate risks, contain breaches, and ensure secure recovery. All encryption key usage during incidents must be fully documented and auditable to support post-incident analysis.

11. Training and Awareness

- All employees and contractors with access to encrypted data or encryption keys must undergo regular training on encryption standards, key management practices, and secure data handling.
- Ongoing security awareness programs will be conducted to reinforce the importance of data encryption and its role in protecting organizational data.

12. Third-Party Services

- Any third-party services used for encryption or key management must adhere to DanfeCorp's encryption policies and meet required security standards.
- Contracts with third-party service providers must include provisions for encryption and data protection in alignment with this policy.

13. Policy Review and Updates

DanfeCorp reserves the right to update this Encryption Management Policy at any time. Any changes will be communicated to all stakeholders and employees. The revised policy will be effective as of the posted date and will be reviewed regularly to ensure compliance with security best practices.

This policy document supersedes all previous encryption management 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.