DANFECORP

Information Security Policy

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

1. Purpose

This policy establishes the framework for safeguarding the confidentiality, integrity, and availability of DanfeCorp's information assets. It outlines the security controls and practices designed to protect sensitive data and ensure compliance with legal, regulatory, and contractual obligations.

2. Scope

This policy applies to all information assets at DanfeCorp, including physical and electronic data, systems, and networks. It is applicable to all employees, contractors, vendors, and third-party service providers who access, manage, or process DanfeCorp's data or systems.

3. Objectives

The comprehensive objectives of DanfeCorp's Information Security Policy are multifaceted and interconnected, forming the foundation of our security posture across the organization. First and foremost, we are committed to protecting all sensitive data and intellectual property from unauthorized access, disclosure, modification, or destruction through the implementation of appropriate technical and administrative safeguards. Simultaneously, we strive to guarantee that information systems and data remain available to authorized users when needed, ensuring business continuity and operational efficiency. This policy further aims to establish rigorous compliance with relevant laws, regulations, and industry standards regarding data protection and information security, including but not limited to privacy regulations and sector-specific requirements. Additionally, the policy establishes a systematic approach to identifying, assessing, and mitigating risks associated with information security through regular evaluations and implementation of controls commensurate with risk levels. Finally, this policy seeks to foster a culture of security awareness and responsibility across all levels of the organization, ensuring that security becomes an integral part of everyday operations rather than a separate consideration.

4. Information Security Governance

- **Information Security Management System (ISMS):** DanfeCorp will implement an ISMS based on industry best practices and standards (e.g., ISO 27001), incorporating the development and enforcement of security policies, procedures, and controls.
- **Information Security Committee:** A dedicated committee comprising key stakeholders from various departments will oversee the implementation and ongoing management of the information security program.

5. Information Classification and Handling

Classification Level	Description	Handling Requirements
Public	Information officially released to the public	No restrictions on distribution
Internal	Information intended for use within DanfeCorp	Should not be shared outside the organization without approval
Confidential	Sensitive business information requiring protection	Restricted access, encryption required for transmission and storage
Highly Confidential	Critical business information or regulated data	Strictly limited access, enhanced encryption, additional security controls

6. Access Control

- **User Access Management:** Access to DanfeCorp's systems and data will be granted based on the principles of least privilege and need-to-know, with regular reviews to ensure appropriate access rights.
- **Authentication and Authorization:** Robust authentication mechanisms (e.g., multi-factor authentication) will be implemented to access critical systems. Access is granted based on predefined roles and responsibilities.
- **User Accountability:** Users are accountable for their actions on information systems. Access logs will be maintained to track activities and detect potential security incidents.

7. Risk Management

- **Risk Assessment:** Regular risk assessments will be conducted to identify potential threats and vulnerabilities to information systems and data.
- **Risk Mitigation:** Appropriate controls and strategies will be implemented to reduce identified risks to acceptable levels, utilizing technical, administrative, and physical safeguards.

8. Data Protection and Privacy

DanfeCorp's approach to data protection and privacy encompasses multiple layers of safeguards designed to secure information throughout its lifecycle. All sensitive and confidential data will be protected using industry-standard encryption protocols both during transmission across networks and while stored on systems, servers, or backup media. The organization adheres strictly to data minimization principles, collecting and processing only the minimum amount of personal and sensitive data necessary for legitimate business purposes, thus reducing exposure and potential impact of security incidents. Data retention practices are carefully managed to ensure information is kept only as long as required by legal, regulatory, or operational needs, after which it will be securely deleted or anonymized through approved procedures. Access to sensitive data is strictly controlled through role-based access control mechanisms and the principle of least privilege, ensuring that only personnel with legitimate business requirements can access confidential information. This comprehensive approach to data protection not only safeguards DanfeCorp's proprietary information but also demonstrates our commitment to respecting privacy rights and maintaining compliance with global data protection regulations across all our operations and partnerships.

9. Incident Management

- **Incident Detection and Reporting:** All security incidents, including data breaches, vulnerabilities, and unauthorized access, must be immediately reported to the Information Security Team.
- **Incident Response Plan:** A comprehensive incident response plan will be maintained to ensure that incidents are detected, contained, eradicated, and recovered in a timely manner. This plan includes communication procedures with stakeholders and regulatory authorities.
- **Post-Incident Review:** Following an incident, a review will be conducted to evaluate the cause, impact, and response effectiveness. Lessons learned will be used to enhance future security measures.

10. Compliance and Legal Requirements

Requirement Area	**Implementation Approach**
Regulatory Compliance	DanfeCorp will comply with all applicable data protection and privacy laws (e.g., GDPR, CCPA) and industry standards through ongoing monitoring and policy updates.
Third-Party Security	Third-party vendors and service providers with access to sensitive data must adhere to DanfeCorp's security standards, enforced through contractual agreements and regular assessments.
Auditing and Monitoring	Regular audits and continuous monitoring of information systems will be conducted to ensure compliance with this policy and detect any security gaps.

11. Business Continuity and Disaster Recovery

- **Business Continuity Planning:** DanfeCorp will implement business continuity and disaster recovery plans to ensure the resilience of critical systems and data during emergencies or disasters.

- **Backup and Recovery:** Regular backups of critical data will be performed, and recovery procedures will be periodically tested to ensure rapid restoration of operations.
- **Testing and Drills:** Regular testing and simulation drills will be conducted to validate the effectiveness of business continuity and disaster recovery plans.

12. Training and Awareness

- **Employee Awareness:** All employees, contractors, and third-party vendors will receive regular information security training to understand their roles and responsibilities in protecting information.
- **Ongoing Training:** Periodic training sessions and awareness programs will be conducted to keep personnel updated on emerging threats, new security tools, and changes in policies or procedures.

13. Policy Review and Maintenance

- **Periodic Review:** This policy will be reviewed at least annually or after a major incident to ensure its continued effectiveness and alignment with changing business needs, regulatory requirements, and emerging security threats.
- **Continuous Improvement:** Feedback from audits, incident reviews, and training initiatives will be used to continuously enhance security policies, controls, and procedures.

This policy document supersedes all previous information 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.