Third-Party Vendor Management Policy

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

1. Purpose

This policy establishes a structured framework for managing third-party vendors, ensuring that they meet DanfeCorp's security, compliance, and operational requirements. It aims to mitigate risks associated with third-party relationships while safeguarding organizational assets and data.

2. Scope

This policy applies to all third-party vendors, suppliers, service providers, contractors, and partners accessing DanfeCorp's information, systems, networks, or facilities. It also applies to all employees and business units involved in vendor selection, onboarding, and management.

3. Roles and Responsibilities

Role	Responsibilities
Vendor Management Team	Oversees vendor risk assessments, onboarding, and ongoing performance monitoring.
Security Team	Conducts security assessments and ensures vendor compliance with DanfeCorp's security policies.
Procurement Team	Verifies that vendors meet business and contractual requirements.
Legal Team	Reviews contracts to ensure inclusion of security, confidentiality, and regulatory compliance clauses.
Business Unit Owners	Manage vendor relationships and ensure adherence to agreed-upon security and performance requirements.

4. Vendor Classification and Risk Assessment

All third-party vendors must undergo a classification and risk assessment process based on their level of access to DanfeCorp's data, systems, and operations:

Risk Level	Description
Critical Vendors	Vendors with direct access to sensitive or regulated data, critical systems, or key business operations.
High-Risk Vendors	Vendors handling confidential information or providing essential services.
Medium-Risk Vendors	Vendors with limited access to internal systems or data.
Low-Risk Vendors	Vendors with no access to internal systems or sensitive data.

Risk assessments include:

- Evaluation of the vendor's security controls and policies.
- Review of regulatory compliance status and industry certifications.
- Assessment of financial stability and operational resilience.
- Examination of past security incidents or breaches.

5. Vendor Onboarding and Due Diligence

Before engaging with a vendor, DanfeCorp requires:

- Completion of a security questionnaire and comprehensive risk assessment.
- Review of independent security audits (e.g., penetration tests, certifications).
- Background checks and financial stability analysis.
- Signing of contracts containing security, confidentiality, and compliance clauses.
- Approval from both the Vendor Management and Security Teams.

6. Contractual and Compliance Requirements

All vendor contracts must include the following elements:

Requirement	Description
Data Protection and Security Standards	Clear requirements for protecting DanfeCorp data.
Right to Audit	Provision for DanfeCorp to conduct audits of vendor security practices.
Incident Notification	Obligation for vendors to report security incidents within a defined timeframe.
Service Level Agreements (SLAs)	Defined performance, availability, and security expectations.
Regulatory Compliance	Assurance that vendors adhere to applicable laws and industry standards.
Data Retention and Deletion	Clauses governing the secure handling and disposal of DanfeCorp data.

DANFECORP

7. Ongoing Monitoring and Review

- Annual Security Reviews: High-risk and critical vendors must undergo annual security assessments.
- Periodic Risk Assessments: Vendors are periodically reassessed in light of emerging threats or business changes.
- Performance Monitoring: Regular reviews of SLAs and compliance metrics.
- Security Incident Reporting: Vendors must immediately report any security breaches and cooperate with investigations.

8. Vendor Offboarding and Termination

When terminating a vendor relationship, DanfeCorp requires:

- Confirmation of data return or secure deletion.
- Revocation of system and network access.
- A final security assessment to ensure no residual risks remain.
- Proper contract closure and documentation of offboarding activities.

9. Policy Review and Updates

This policy shall be reviewed and updated annually or upon significant changes to DanfeCorp's vendor management processes, regulatory requirements, or the security landscape. The Security Team must approve all updates.

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