Cloud Security Policy

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

1. Purpose

This policy establishes the framework for securely using cloud-based resources and services within DanfeCorp. It aims to ensure that cloud environments are properly secured, compliant with relevant regulations, and aligned with organizational security objectives, thereby safeguarding the confidentiality, integrity, and availability of data and systems.

2. Scope

This policy applies to all cloud environments and services used by DanfeCorp, including public, private, and hybrid clouds. It covers all employees, contractors, vendors, and third parties who use, manage, or have access to DanfeCorp's cloud infrastructure, applications, and services.

3. Cloud Security Objectives

DanfeCorp is committed to maintaining the highest level of security for all cloud services. Achieving this requires a comprehensive approach that addresses multiple aspects of cloud security. The following objectives form the foundation of our cloud security strategy and must be prioritized in all cloud deployments and operations.

- **Data Protection:** Secure data stored in or processed by cloud services against unauthorized access, modification, or loss.
- **Access Control:** Implement strict controls to ensure only authorized users can access sensitive cloud resources.
- **Compliance:** Ensure that all cloud services meet relevant regulatory, contractual, and industry standards.
- **Incident Response:** Establish procedures to respond promptly and effectively to security incidents involving cloud services.
- **Risk Management:** Regularly assess and manage risks associated with cloud environments to minimize vulnerabilities and threats.

4. Cloud Service Provider Security Management

4.1 Due Diligence in Vendor Selection

- **Third-Party Risk Assessment:** Conduct thorough due diligence before selecting any cloud service provider (CSP), including evaluating the CSP's security posture, compliance with industry standards, and ability to meet DanfeCorp's requirements.
- **Security Certifications:** Ensure CSPs demonstrate adherence to recognized security certifications and frameworks (e.g., ISO/IEC 27001, SOC 2) to confirm they meet DanfeCorp's security and compliance standards.
- **Data Processing Agreements (DPAs):** Establish formal agreements with CSPs outlining security responsibilities, data handling practices, and compliance with applicable laws and regulations.

4.2 Shared Responsibility Model

- **Security Ownership:** Recognize and manage the shared responsibility model, where DanfeCorp secures its own data and applications while the CSP secures the underlying infrastructure and services.
- **Clear Delineation:** Clearly define roles and responsibilities for security in the contractual agreements with CSPs, ensuring both parties understand their obligations.

5. Access Control and Identity Management

5.1 Authentication and Authorization

Control Type	Description	Implementation Requirements
Multi-Factor Authentication (MFA)	Additional authentication layer beyond password	Required for all users accessing cloud environments
Role-Based Access Control (RBAC)	Access based on user roles	Grant access based on the principle of least privilege, ensuring users have only the permissions necessary to perform their job functions
Identity Federation	Integration with corporate identity systems	Utilize identity federation protocols (e.g., SAML, OpenID Connect) to enable centralized authentication and authorization

5.2 Access Reviews and Audits

- **Periodic Access Reviews:** Regularly review access rights to ensure they remain appropriate and revoke any unnecessary or excessive privileges immediately.
- **Audit Logs:** Maintain detailed logs of all cloud access and activities, reviewing them periodically to detect unauthorized access, anomalies, and potential security incidents.

6. Data Security

6.1 Data Classification and Handling

- **Data Classification:** Classify all data stored or processed in cloud environments based on sensitivity and the potential impact of unauthorized disclosure, applying stricter controls to sensitive and confidential data.
- **Encryption:** Encrypt data at rest, in transit, and in use within the cloud using strong encryption algorithms. Manage encryption keys securely, under the control of DanfeCorp, to maintain data confidentiality and integrity.
- **Data Backup and Recovery:** Regularly back up cloud-based data and establish tested recovery procedures to ensure data restoration in the event of a disaster or data loss.

6.2 Data Residency and Compliance

- **Data Location:** Ensure that cloud providers comply with data residency requirements by storing and processing data within regions that meet regulatory and compliance obligations.
- **Compliance with Regulations:** Verify that cloud service providers adhere to applicable data protection regulations (e.g., GDPR, CCPA) and that all cloud-based activities align with these legal requirements.

7. Security Controls for Cloud Environments

7.1 Network Security

- **Virtual Private Network (VPN):** Establish secure connections to cloud environments via VPNs or other secure communication methods, ensuring that cloud-based data and services are accessed only through secure channels.
- **Firewalls and Security Groups:** Utilize firewalls, security groups, and network segmentation to isolate cloud environments and restrict access to only necessary services and resources.
- **Intrusion Detection and Prevention:** Implement intrusion detection and prevention systems (IDPS) to monitor cloud environments for malicious activity and respond promptly to detected threats.

7.2 Endpoint Security

- **Device Management:** Ensure all devices accessing cloud services (laptops, mobile devices, virtual machines) are secured using up-to-date antivirus software, security patches, and other endpoint protection measures.
- **Mobile Device Management (MDM):** Enforce security policies on mobile devices through MDM systems, including requirements for encryption and remote wipe capabilities.

8. Incident Response and Monitoring

8.1 Security Monitoring

Monitoring Activity	Description	Frequency
Cloud Security Monitoring	Deploy security monitoring tools (e.g., SIEM systems) to continuously track the activity and performance of cloud services	Continuous
Log Review	Review logs from cloud services to detect anomalous behavior	Daily
Vulnerability Scanning	Scan cloud-based systems to identify and remediate potential security weaknesses	Monthly
Penetration Testing	Test the resilience of cloud-based systems against external and internal threats	Quarterly

8.2 Incident Detection and Response

- **Incident Response Plan:** Develop and maintain an incident response plan specifically for cloud services, outlining procedures for handling incidents such as data breaches, unauthorized access, or service outages.
- **Notification and Reporting:** Require cloud providers to notify DanfeCorp within an agreed timeframe in the event of a security incident, after which internal processes will be followed to investigate, mitigate, and report the incident in compliance with regulatory and contractual obligations.

9. Training and Awareness

- **Security Awareness Training:** Provide regular training to employees on cloud security best practices, including the identification of phishing attempts, secure handling of cloud data, and responsible use of cloud services.

- **Specialized Training for IT and Security Staff:** Offer in-depth training for IT and security personnel focused on securing cloud environments, implementing effective security controls, and responding to cloud-specific threats and incidents.

10. Cloud Security Audits and Assessments

- **Regular Security Audits:** Conduct regular audits of cloud environments to ensure that security controls remain effective and that cloud services continue to meet DanfeCorp's security and compliance requirements.
- **Penetration Testing:** Perform periodic penetration testing to evaluate the resilience of cloud-based systems against external and internal threats.

11. Policy Review and Updates

This policy will be reviewed and updated annually or in response to significant changes in DanfeCorp's cloud strategy, technology, or regulatory environment. All updates will be documented, and relevant stakeholders will be informed of the changes.

This policy document supersedes all previous cloud 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.