DANFECORP

Data Center Security Policy

Approved by	Signature	Effective Date
Security Team	Official Security Team Approved	03/15/2025

1. Purpose

This policy establishes protocols and controls to ensure the security, integrity, and availability of DanfeCorp's data and IT infrastructure hosted at DanfeCorp's co-location data center. It outlines the physical and environmental security measures needed to protect these assets against unauthorized access, environmental hazards, and other potential threats.

2. Scope

This policy applies to all DanfeCorp assets housed at DanfeCorp's co-location data center, including servers, networking equipment, storage devices, and related hardware. It also covers all personnel who access these assets, including DanfeCorp employees, DanfeCorp staff, contractors, and authorized visitors.

3. Physical Security Controls

DanfeCorp implements robust physical security measures at its primary and alternate data center sites to prevent unauthorized access and mitigate environmental hazards. These measures encompass site selection and design, perimeter defenses, strict access controls, continuous surveillance, environmental controls, and equipment security.

3.1 Site Selection and Design

- **Primary Location:** DanfeCorp's primary data center is located in Dhulikhel, Nepal.
- **Alternate Site (Availability Zone):** An alternate data center site is established in Duhabi, Nepal, to ensure redundancy and support disaster recovery. This secondary location provides geographic diversity, reducing the risk of a single event disrupting both sites.

- **Redundancy:** Both data centers are built with redundant infrastructure (e.g., N+1 configurations) to ensure continuous operation even in the event of component failures.

3.2 Perimeter Security

- **Fencing and Barriers:** Each data center's perimeter is secured with strong fencing and barriers to prevent unauthorized entry.
- **Access Points:** Entry points are limited in number and each is equipped with security controls to monitor and restrict access.

3.3 Physical Access Controls

DanfeCorp enforces multi-layered physical access controls to ensure only authorized personnel can access sensitive areas:

- **Authentication Mechanisms:** Access to the data centers requires multi-factor authentication (e.g., biometric scans and access cards).
- **Access Authorization:** Only personnel with a legitimate business need and proper authorization are allowed to access the data centers. Access rights are reviewed regularly to ensure they remain appropriate.
- **Visitor Management:** All visitors must be pre-approved, registered upon arrival, and escorted at all times within the facility. Visitor logs must be maintained and reviewed regularly.

3.4 Surveillance and Monitoring

- **Video Surveillance:** Continuous video surveillance covers all critical areas (entrances, exits, server rooms). Recorded footage is retained for at least 90 days.
- **Intrusion Detection:** Physical intrusion detection systems are in place to alert security personnel immediately of any unauthorized access attempts.

3.5 Environmental Controls

Control Type	Implementation Requirements
Fire Detection and Suppression	Advanced fire detection systems (smoke and heat detectors) are installed, and fire suppression systems are designed to be safe for electronic equipment.
Climate Control	Data center environments are maintained at optimal temperature and humidity levels to ensure equipment reliability. Redundant HVAC systems are in place to prevent downtime due to environmental control failures.
Power Supply	Uninterruptible Power Supplies (UPS) and backup generators ensure continuous power in the event of an outage.

3.6 Equipment Security

- **Asset Management:** All equipment is inventoried and cataloged, and asset records are kept accurate and up-to-date.
- **Secure Disposal:** Decommissioned equipment is securely disposed of, with all data irretrievably erased.

4. Network Security Controls

Beyond physical safeguards, DanfeCorp employs stringent network security controls to protect data and systems within the data centers. These controls include network segmentation, deployment of firewalls and intrusion detection systems, and regular security audits.

- **Segmentation:** The network is segmented to limit access between systems based on role and function, thereby reducing the potential impact of any security breach.
- **Firewalls and Intrusion Detection Systems (IDS):** Firewalls and IDS are deployed to monitor and control network traffic in accordance with defined security rules.
- **Regular Audits:** Network security measures are audited regularly to ensure compliance with security policies and to identify potential vulnerabilities.

5. Compliance and Standards

DanfeCorp ensures that operations at both data centers comply with all relevant regulatory requirements and adhere to recognized industry security standards.

- **Regulatory Compliance:** Both data centers comply with all applicable local and international regulations and standards (including ISO 27001 for information security management).
- **Regular Assessments:** Security assessments and audits are conducted regularly to ensure ongoing compliance and to identify areas for improvement.

6. Incident Response

Despite strong preventive measures, security incidents may still occur. DanfeCorp maintains a comprehensive incident response program to handle any data center security breaches or emergencies swiftly and effectively.

Component	Description
Incident Management Plan	An incident management plan is in place to address security breaches or other emergencies. It details response procedures, communication protocols, and recovery steps.
Training	Staff receive regular training on incident response procedures to ensure preparedness for any security incident.

7. Review and Maintenance

DanfeCorp regularly reviews this policy and the associated security controls to ensure they remain effective and aligned with changes in the organization or external requirements.

- **Policy Review:** This policy is reviewed at least annually, or whenever significant changes occur to the company's systems, business requirements, or external regulations.
- **Continuous Improvement:** Feedback from security audits, assessments, and incident responses is used to continuously improve data center security measures.

This policy document supersedes all previous data center 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.