Access Control Policy

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

1. Purpose

This policy establishes protocols and controls to ensure that access to information, systems, and resources at DanfeCorp is granted strictly on the basis of business needs and the principle of least privilege. It is designed to protect sensitive data and company assets while maintaining a secure operational environment. This document outlines the procedures for granting, reviewing, and revoking access rights.

2. Scope

This policy applies to all employees, contractors, vendors, and third-party service providers who require access to DanfeCorp's information systems, networks, applications, or any resources that process or store sensitive data.

3. Access Control Principles

Principle	Description
Least Privilege	Users are provided only the minimum access necessary to perform their duties.
Need-to-Know	Access is granted solely based on business requirements and role-specific needs.
Separation of Duties	Critical functions are divided among multiple individuals to minimize conflicts of interest and reduce the risk of error or fraud.
Role-Based Access Control (RBAC)	Access rights are assigned according to predefined roles to ensure consistency and streamline management.
User Authentication and Authorization	Secure authentication is mandatory, and access is authorized based on the user's assigned role and responsibilities.

4. User Access Management

4.1 Account Creation and Provisioning

- **New Users:** When a new employee or contractor joins DanfeCorp, their role and responsibilities are assessed to determine appropriate access rights, in line with the principle of least privilege.
- **Role Assignment:** Each user is assigned a specific role, and access rights are granted in accordance with the established role-based access control matrix.
- **Temporary Access:** Contractors and third-party vendors receive temporary access only for the duration of their engagement; all access is revoked immediately upon project completion.
- **Access Documentation:** Every access request is documented, detailing the justification, assigned roles, and management approvals.

4.2 Remote Access Controls

- **Multi-Factor Authentication (MFA):** All remote access and privileged accounts require MFA.
- **Secure Remote Access:** Remote connections must be made through company-approved Virtual Private Network (VPN) services or equivalent secure methods.
- **Monitoring:** Remote access sessions are continuously monitored, with unauthorized attempts logged and investigated.
- **Endpoint Security:** Users accessing company resources remotely must comply with endpoint security policies, including updated antivirus software and encrypted connections.
- **Periodic Review:** Remote access permissions are regularly reviewed; temporary access requires management approval and is revoked when no longer necessary.

4.3 Access Reviews and Revocation

- **Periodic Reviews:** Access permissions are reviewed at least annually to ensure alignment with current job roles and business requirements; unnecessary privileges are promptly revoked.
- **Role Change Reviews:** A change in a user's job responsibilities triggers an immediate review and adjustment of access rights.
- **Exit Procedures:** Upon termination or departure, a formal offboarding process ensures that all access is immediately revoked.
- **Deactivation of Accounts:** User accounts are deactivated or removed promptly when no longer needed.
- **Third-Party Access:** Access granted to third-party vendors is reviewed regularly and revoked immediately upon contract completion or service termination.

5. Authentication and Authorization Mechanisms

5.1 Authentication Methods

Authentication Method	Requirements
Multi-Factor Authentication (MFA)	Users accessing sensitive systems must authenticate using at least two factors (e.g., a password plus a one-time passcode).
Strong Password Requirements	Passwords must comply with established complexity standards (minimum length, mix of uppercase/lowercase letters, numbers, and special characters).
Password Expiration and Rotation	Passwords must be changed every 90 days, with timely reminders for password updates.

5.2 Access Authorization

- **Access Control Lists (ACLs):** Systems maintain ACLs to define which users or groups may access specific resources; these lists are reviewed regularly.
- **Role-Based Access:** Users are assigned to roles with predefined access rights, ensuring that they only access resources pertinent to their responsibilities.

6. Monitoring and Logging

6.1 Audit Logging

- **Logging of Access Events:** All access events—including login attempts, role changes, and privilege escalations—are logged to maintain an audit trail.
- **Log Retention:** Audit logs are retained for a minimum of one year for monitoring and investigation purposes.

6.2 Access Monitoring

- **Real-Time Monitoring:** Systems are continuously monitored for signs of unauthorized access, privilege abuse, or other suspicious activities. Any anomalies are promptly investigated.
- **Incident Response:** Any access control-related incidents trigger a formal investigation and remediation process in line with the company's incident response policy.

7. Physical Access Control

- **Facility Access:** Physical entry to critical infrastructure (such as data centers) is restricted to authorized personnel. All entries are logged, and physical barriers (e.g., locked doors and biometric scanners) are enforced.

- **Workstation Security:** Devices used to access sensitive information must be secured. Employees are required to lock their workstations when unattended and adhere to company security policies.

8. Third-Party Access

8.1 Third-Party Vendor Access

- **Access Limitations:** Third-party vendors receive access only to the systems and data necessary for their work.
- **Periodic Reviews:** Access for third-party vendors is reviewed periodically to ensure compliance with DanfeCorp's security policies.

8.2 Contractual Agreements

- **Access Restrictions in Contracts:** All third-party agreements must explicitly outline access restrictions, data protection measures, and security expectations, ensuring that vendors comply with the same standards as internal employees.

9. Security Training and Awareness

9.1 User Awareness and Training

- **Access Control Training:** All employees receive regular training on access control principles, secure credential management, and the recognition of potential security threats.
- **Ongoing Awareness Programs:** Regular updates and training sessions reinforce best practices in access control.

10. Policy Compliance and Enforcement

- **Compliance Monitoring:** Regular audits are conducted to ensure adherence to this policy. Any deviations or violations are addressed according to DanfeCorp's disciplinary procedures.
- **Enforcement:** Non-compliance with this policy may result in disciplinary actions, including revocation of access, suspension, or termination, based on the severity of the violation.

11. Policy Review and Updates

This policy is reviewed and updated annually or whenever significant changes occur in the company's systems, business requirements, or external regulations. All updates will be communicated to affected personnel, and additional training will be provided as needed.

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