Password Management Policy

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

1. Purpose

This policy establishes standards for the creation, management, and protection of passwords to ensure the security of DanfeCorp's systems, applications, and data. Effective password management reduces the risk of unauthorized access and helps safeguard both corporate and customer information.

2. Scope

This policy applies to all employees, contractors, vendors, and any other individuals who access DanfeCorp's systems, applications, networks, or data.

Password security is a critical component of our overall cybersecurity strategy. Weak passwords are one of the most common points of entry for malicious actors. By following the requirements outlined in this policy, all users contribute to protecting DanfeCorp's sensitive information, intellectual property, and reputation. Remember that a security chain is only as strong as its weakest link.

3. Password Requirements

3.1 Password Complexity

Requirement	Description
Minimum Length	Passwords must be at least 12 characters long.
Character Requirements	Each password must contain at least one uppercase letter (A-Z), one lowercase letter (a-z), one number (0-9), and one special character (e.g., !, @, #, $, %).
Content Restrictions	Passwords must not include commonly used words, personal information, or company-specific terms.

Strong Password Examples:

- Tr0ub4dor&3 - Combines multiple character types

- D0g$-ruNN1ng-Fast - Uses a passphrase with special characters

Weak Password Examples (DO NOT USE):

- Password123! - Too predictable
- DanfeCorp2025 - Contains company name

3.2 Password Expiration and Rotation

- **User Passwords:** Must be changed every 90 days.
- **System and Privileged Account Passwords:** Must be changed every 60 days.
- **Password History:** Users may not reuse the last five passwords.
- **Default Passwords:** Must be changed before first use.

3.3 Multi-Factor Authentication (MFA)

- MFA is mandatory for accessing any corporate systems containing sensitive or confidential data.
- MFA is required for all remote access and for privileged accounts.

3.4 Password Storage and Transmission

Policy	Requirement	Reason
Storage	Passwords must be stored using industry-standard hashing algorithms (e.g., bcrypt, PBKDF2, or Argon2) and must never be written down or stored in plain text.	Plain text storage creates significant security vulnerabilities
Transmission	Passwords must never be transmitted unencrypted.	Unencrypted transmission can be intercepted
Sharing	Under no circumstances should passwords be shared.	Sharing eliminates accountability and increases risk

4. Privileged Account Management

Privileged accounts have elevated access rights and require additional security controls. These accounts are high-value targets for attackers and must be protected with the highest level of security measures available.

- **Unique Credentials:** Privileged accounts (e.g., admin, root, service accounts) must use unique, complex passwords that differ from those used for regular user accounts.
- **Dedicated Credentials:** Privileged accounts must have dedicated credentials and should not be shared.
- **Rotation and Storage:** Privileged passwords must be rotated at least every 60 days and stored in a secure password vault.

DANFECORP

5. Account Lockout Policy

Control	Implementation
Failed Login Attempts	Accounts will be locked after 5 consecutive failed login attempts.
Unlocking	Locked accounts will require administrative intervention or maybe unlocked automatically through self-service after 15 minutes.
Inactivity	Accounts inactive for 90 days will be disabled.

6. Password Sharing and Management Tools

- **No Sharing:** Users must not share passwords under any circumstances.
- **Approved Tools:** Only approved enterprise password managers should be used to store and manage corporate credentials.

7. Incident Response for Compromised Credentials

Even with strong controls in place, password compromises can still occur. When they do, swift action is essential to minimize potential damage. The following steps must be taken whenever a password compromise is suspected:

1. **Reporting:** Users must immediately report any suspected password compromise to the IT Security Team.
2. **Account Reset:** Affected accounts must be reset promptly and reviewed for any unauthorized access.
3. **Investigation:** The IT Security Team will conduct an investigation and implement corrective actions as needed.

8. Policy Compliance and Enforcement

- **Audits:** Regular password audits will be conducted to ensure compliance with this policy.
- **Disciplinary Actions:** Failure to comply with this policy may result in disciplinary action, up to and including termination.
- **Review Cycle:** The IT Security Team will review and update this policy at least annually.

This policy document supersedes all previous password management 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.