Acceptable Use Policy

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

1. Purpose

This policy ensures that the use of DanfeCorp's technology resources—including systems, networks, devices, and applications—is aligned with company values and objectives. It is designed to protect the organization from misuse and unauthorized access to sensitive information by outlining acceptable behaviors, responsibilities, and guidelines for all users.

2. Scope

This policy applies to all employees, contractors, consultants, temporary workers, third-party service providers, and any other users who have access to DanfeCorp's technology infrastructure. This includes computers, mobile devices, networks, cloud services, applications, and all related resources.

3. Acceptable Use Guidelines

3.1 Authorized Use

- **Business Use Only:** Technology resources provided by DanfeCorp should be primarily used for legitimate business purposes. Personal use must be limited and should not interfere with work responsibilities.
- **Access Control:** Users are permitted to access only those systems and data for which they are authorized. It is each user's responsibility to ensure they do not exceed their granted access rights.

3.2 Prohibited Use

DanfeCorp strictly prohibits a comprehensive range of activities that could compromise security, damage reputation, or expose the organization to legal liability. Any form of unauthorized access—whether actively attempting to gain entry to systems without proper permissions, assisting others in such attempts, or maintaining access beyond authorized scope—constitutes a serious violation of this policy and potentially applicable laws. Similarly, engaging in malicious activities using company resources is expressly forbidden, including but not limited to hacking attempts, deliberate introduction of malware, ransomware deployment, or any other actions intended to compromise the integrity, availability, or confidentiality of company or third-party systems and data. The

creation, transmission, storage, or display of inappropriate content, including materials that are offensive, discriminatory, obscene, harassing, or threatening in nature is prohibited regardless of intent or context. All company technology resources must never be used for unlawful activities such as fraud, identity theft, intellectual property violations, or distribution of pirated software or media, as such actions expose both the individual and the organization to significant legal consequences. Additionally, attempts to circumvent established security controls—including firewalls, authentication mechanisms, encryption protocols, or network monitoring tools—are strictly forbidden as these protective measures are essential components of our organizational security architecture designed to safeguard critical assets and information.

3.3 Email and Communication Systems

- **Professional Communication:** Company email and communication tools are to be used for professional, work-related activities. Personal use should remain minimal.
- **Sensitive Information:** Sensitive or confidential information must be protected during transmission and should only be sent using secure methods (e.g., encrypted email or secure file transfer).
- **Phishing and Social Engineering:** Engaging in or falling victim to phishing or social engineering tactics is strictly prohibited. All suspicious communications must be reported immediately to the IT or Security Team.

3.4 Internet and Web Usage

Usage Type	Guidelines	Requirements
Browsing	Internet access is intended primarily for business purposes	Avoid accessing inappropriate, illegal, or unrelated content; follow company filter policies
Social Media	The business use must follow DanfeCorp's social media policies	Personal social media should not disrupt work unless explicitly permitted
Remote Access	Access to company systems from outside networks	Must use approved secure channels (VPNs or other secure protocols)

3.5 Software and Applications

- **Approved Software Only:** Only software or applications authorized by the IT department may be installed on company systems. Unauthorized software that poses security risks will be removed.
- **License Compliance:** Users must ensure that all software used on company systems is properly licensed and compliant with applicable agreements.

3.6 Device Security and Usage

- **Device Security:** All devices (laptops, mobile phones, workstations, etc.) must be secured using passwords or other authentication methods as prescribed by the IT department.
- **Device Loss or Theft:** Any device containing DanfeCorp data or access to company systems that is lost or stolen must be reported immediately to the IT or Security Team.
- **No Unauthorized Devices:** Connecting unauthorized personal devices (e.g., USB drives, mobile phones) to company systems or networks is not permitted unless explicitly approved by the IT department.

3.7 Data Protection and Privacy

All users of DanfeCorp systems bear significant responsibility for safeguarding organizational information assets in accordance with established data protection frameworks. Confidentiality of information represents a fundamental obligation, requiring users to diligently protect any sensitive or confidential data they access, process, or store during the course of their work activities. This protection extends across all information classifications and must align with DanfeCorp's comprehensive data protection policies, which establish controls appropriate to various sensitivity levels. The sharing of company data or confidential information is permitted exclusively with properly authorized individuals who have legitimate business needs for such access. Moreover, any such sharing must employ secure transmission channels that ensure data integrity and confidentiality throughout the exchange process, implementing encryption technologies when transferring sensitive information across networks or to external parties. As part of their data stewardship responsibilities, users must strictly adhere to established guidelines regarding data backup and recovery procedures, following documented processes for both routine backups and restoration activities when necessary. These practices collectively ensure maintenance of data availability and integrity across the organization, protecting against accidental loss, corruption, or unauthorized modification of critical business information. Additionally, users must remain vigilant regarding potential data privacy implications of their activities, particularly when handling personally identifiable information or other regulated data categories that may be subject to specific compliance requirements under applicable privacy legislation.

4. Monitoring and Enforcement

4.1 Monitoring

- **System Monitoring:** DanfeCorp reserves the right to monitor all technology resources—including email, internet activity, and system access—to ensure compliance with this policy and protect against misuse.
- **Audit Logs:** Audit logs of system access, user activity, and communication traffic will be maintained and periodically reviewed to detect and investigate suspicious behavior.

4.2 Disciplinary Actions

Violations of this policy may result in disciplinary action, which can include revocation of access, suspension, termination of employment or contracts, and legal action, depending on the severity of the violation.

4.3 Reporting Violations

- **Incident Reporting:** Users must report any suspected violations, such as unauthorized access or security breaches, immediately to the IT or Security Team.
- **Anonymous Reporting:** Employees may also report violations anonymously through the company's ethics hotline or other reporting mechanisms, if available.

5. Security Awareness and Training

Component	Description	Frequency
Initial Training	All users receive comprehensive training on the Acceptable Use Policy and related security policies	Upon joining and after significant policy changes
Refresher Training	Focused sessions on specific aspects of security and acceptable use	Quarterly
Awareness Campaigns	Communications about emerging threats, best practices, and policy updates	Monthly
Simulated Phishing	Tests to evaluate user awareness and response to social engineering attempts	Ongoing, randomized

6. Policy Review and Updates

This policy will be reviewed and updated annually or whenever significant changes occur to DanfeCorp's systems, technology, or legal requirements. All updates will be documented and communicated to affected users, and additional training will be provided as necessary.

This policy document supersedes all previous acceptable use guidelines and becomes effective as of the date specified above.