DANFECORP

Remote Work and Remote Access Policy

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

1. Purpose

This policy establishes guidelines for secure remote work and remote access to DanfeCorp's systems, networks, and data. It ensures that employees, contractors, and third-party partners adhere to security best practices while working remotely.

2. Scope

This policy applies to all employees, contractors, and third-party vendors who access DanfeCorp's systems remotely. It covers remote access to company networks, cloud applications, internal systems, and sensitive data.

The modern workplace has evolved to embrace flexible work arrangements, including remote work. While this flexibility offers many benefits to both employees and the organization, it also introduces unique security challenges. This policy is designed to maintain the security of DanfeCorp's information assets while enabling productive remote work environments.

3. Roles and Responsibilities

Role	Responsibilities
IT Security Team	Manages remote access security, implements controls, and monitors compliance.
Employees and Contractors	Follow security guidelines, use approved tools, and report security incidents.
Management	Ensures that employees have proper access and adhere to remote work policies.
Third-Party Vendors	Must comply with DanfeCorp's remote access security requirements.

4. Remote Work Guidelines

- **Approved Devices:** Employees must use company-approved devices for remote work; personal devices are prohibited unless explicitly authorized.

- **Secure Environment:** Work must be conducted in an environment where unauthorized individuals cannot access company data.
- **Confidentiality:** Confidential discussions should not take place in public areas.
- **Compliance:** All company security policies, including data protection and incident reporting, must be followed at all times.

Remote Work Best Practices

- ✓ Use a dedicated workspace whenever possible
- ✓ Secure your home network with strong passwords and encryption
- ✓ Lock your computer when stepping away, even at home
- ✓ Be mindful of who might overhear sensitive conversations
- ✓ Regularly back up your work to approved company locations

5. Remote Access Security Controls

5.1 Authentication and Authorization

- **Multi-Factor Authentication (MFA):** MFA is required for all remote access.
- **Least Privilege:** Access is granted based on the principle of least privilege.
- **Periodic Reviews:** Access rights are reviewed periodically to ensure compliance.

5.2 Secure Connection Requirements

Requirement	Description	Implementation
VPN or Secure Gateway	Secure tunnel for remote access	Remote access must be established through a company-approved VPN or secure gateway.
Encryption	Data protection during transmission	All remote sessions must be encrypted using industry-standard encryption protocols.
Session Timeouts	Security for inactive sessions	Automatic session timeouts must be enforced to minimize security risks.

5.3 Device Security

- **Up-to-Date Software:** Devices must run current operating systems, antivirus software, and security patches.
- **Endpoint Protection:** Company-issued devices must have endpoint protection measures enabled, including firewalls and intrusion detection.
- **Incident Reporting:** Lost or stolen devices must be reported immediately to the IT Security Team.

DANFECORP

6. Data Protection and Privacy

Policy	Allowed	Prohibited
Data Storage	Company-approved cloud storage solutions and encrypted company devices	Storing sensitive company data on personal devices or unapproved cloud services
Data Transfer	Encrypted transfers through approved channels	Unencrypted transfers or use of personal email for company data
Collaboration Tools	Company-approved collaboration platforms	Unapproved messaging or file-sharing services

Remote workers must prioritize data security by ensuring proper handling of company information while working outside the office. This includes using only company-approved cloud storage solutions and encrypting data during transmission, especially when accessing or transferring sensitive information.

7. Monitoring and Compliance

- **Remote Access Logs:** DanfeCorp reserves the right to monitor remote access logs and audit activity for security purposes.
- **Policy Adherence:** Employees must comply with all applicable company policies, regulations, and security best practices.
- **Disciplinary Action:** Violations of this policy may result in disciplinary action, including termination of employment.

8. Incident Response and Reporting

- **Immediate Reporting:** Employees must immediately report any suspicious activity, security breaches, or potential threats to the IT Security Team.
- **Investigation and Mitigation:** The IT Security Team will investigate incidents and mitigate threats per the company's incident response plan.

9. Policy Review and Updates

This policy will be reviewed and updated annually or upon significant changes to remote work practices, the security landscape, or business operations. The Security Team must approve all updates.

This policy document supersedes all previous remote work and remote access 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.