DANFECORP

Incident Response Policy

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

1. Purpose

This policy defines the structured approach DanfeCorp will use to respond to security incidents. It aims to minimize the impact of incidents, preserve evidence for analysis and remediation, and ensure rapid recovery to maintain the confidentiality, integrity, and availability of our information systems.

2. Scope

This policy applies to all employees, contractors, third parties, and other stakeholders who access or manage DanfeCorp's information systems, networks, and data. It covers all types of security incidents, including but not limited to data breaches, malware attacks, phishing attempts, denial-of-service attacks, insider threats, and unauthorized access.

3. Objectives

The objectives of DanfeCorp's incident response strategy are multifaceted and designed to address all aspects of security incident management across the organization. Our primary aim is to rapidly identify, contain, and mitigate the effects of security incidents to minimize operational disruption and potential damage to systems and data. This requires swift action based on established protocols and well-defined escalation procedures that can be activated immediately upon incident detection. Equally important is our commitment to methodically collecting and preserving evidence throughout the incident lifecycle, which supports thorough post-incident analysis, guides effective remediation efforts, and provides necessary documentation for potential legal proceedings or regulatory inquiries. Compliance remains a cornerstone of our approach, ensuring we meet all relevant legal, regulatory, and contractual obligations related to data protection and breach notification, including timely reporting to affected individuals and authorities as required by applicable laws. Finally, we view each incident as an opportunity for organizational growth through continuous improvement, systematically analyzing incident data to enhance our security controls, detection capabilities, and

response strategies to strengthen our overall security posture and better prepare for future challenges.

4. Incident Response Lifecycle

4.1 Preparation

- **Incident Response Team (IRT):** DanfeCorp will maintain a dedicated team of security professionals and key stakeholders responsible for responding to incidents, including representatives from IT, legal, compliance, communications, and executive leadership.
- **Incident Response Plan (IRP):** A comprehensive IRP will be developed, maintained, and regularly updated, detailing procedures for identifying, classifying, containing, and mitigating security incidents.
- **Training and Awareness:** Regular training will be conducted for employees, contractors, and partners to recognize potential incidents and respond appropriately.
- **Incident Detection Tools:** Technical tools and monitoring systems (e.g., intrusion detection systems, firewalls, SIEM) will be deployed to detect potential security incidents in real-time.

4.2 Identification

- **Incident Detection:** Incidents may be identified through internal monitoring, external notifications, or employee reports. Common indicators include unusual network activity, unauthorized access attempts, or abnormal system behavior.
- **Incident Classification:** The IRT will classify incidents to determine severity, scope, and potential impact, guiding the appropriate response and escalation procedures.

4.3 Containment

Containment Stage	Actions	Objective
Immediate Actions	Disconnecting affected systems, disabling access, isolating network segments	Prevent further damage and limit incident spread
Short-Term Containment	Blocking malicious IP addresses, changing passwords, disabling compromised user accounts	Limit the incident's spread while maintaining essential services
Long-Term Containment	Applying temporary fixes and controls	Allow normal operations to continue while further investigation and remediation are underway

4.4 Eradication

The eradication phase represents a critical junction in the incident response process where DanfeCorp's security team transitions from containment to elimination of the security threat. This phase begins with a comprehensive root cause analysis conducted by the Incident Response Team, who will methodically examine affected systems and networks to identify the fundamental vulnerabilities or weaknesses that permitted the security breach. This analysis goes beyond merely identifying surface symptoms to uncover the underlying entry points, attack vectors, and exploitation techniques utilized by threats. Following this assessment, the team undertakes the systematic removal of all malicious software, files, compromised accounts, and unauthorized access points from the affected systems. This cleansing process must be thorough and precise to prevent incident recurrence or persistence. Once malicious elements have been removed, systems undergo rigorous hardening procedures, including the application of all relevant security patches, comprehensive update of system configurations to address identified vulnerabilities, implementation of enhanced access controls, and strengthening of network security parameters. Throughout this phase, all actions are meticulously documented to establish a clear record of remediation activities and to support subsequent verification of the eradication's effectiveness before proceeding to the recovery phase.

4.5 Recovery

- **Restoring Systems:** Affected systems will be restored to normal operations only once they are fully secure. This may include restoring from backups or reinstalling software.
- **Monitoring Post-Recovery:** Continuous monitoring will be conducted post-recovery to detect any signs of recurrence or abnormal behavior.

- **Communication with Stakeholders:** During the recovery phase, timely and accurate communication will be maintained with internal and external stakeholders.

4.6 Lessons Learned

- **Post-Incident Review:** A review will be conducted after resolution to assess response effectiveness, identify process gaps, and document lessons learned.
- **Updating Security Measures:** Findings from the review will be used to update security policies, incident response procedures, and controls to prevent future incidents.

5. Incident Response Team (IRT)

The Incident Response Team is responsible for leading the response to security incidents. The team will include:

Role	Responsibilities
Incident Response Manager	Oversees the overall response and ensures adherence to the IRP
IT Security Team	Handles technical investigation, containment, and eradication
Legal Team	Provides guidance on legal obligations and ensures regulatory compliance
Communication Team	Manages internal and external communications, including notifications to affected parties and regulators
Executive Team	Offers strategic direction and decision-making for significant incidents

6. Incident Reporting and Communication

- **Reporting Procedures:** Employees, contractors, and third parties must immediately report any suspected security incidents to the designated IRT or through established internal channels.
- **Incident Communication:** Once an incident is confirmed, the IRT will notify relevant stakeholders, including internal teams, external partners, and regulatory bodies providing details on the incident, actions taken, and further recommendations.
- **Breach Notification:** In cases involving data breaches, DanfeCorp will comply with legal requirements by notifying affected individuals and regulatory authorities within the prescribed timeframes.

7. Incident Severity Classification

Incidents will be classified to prioritize response efforts:

- **Low Severity:** Incidents with minimal impact and no risk to sensitive data or systems (e.g., non-critical malware or minor phishing attempts).
- **Medium Severity:** Incidents affecting non-critical systems or data that could escalate if not addressed promptly (e.g., internal phishing attempts leading to unauthorized access).
- **High Severity:** Major incidents with the potential to disrupt critical operations, compromise sensitive data, or affect a large segment of the organization (e.g., data breaches or ransomware attacks).

8. Compliance and Reporting

- **Regulatory Compliance:** DanfeCorp will adhere to applicable regulatory and industry-specific requirements for incident reporting, data breach notifications, and record-keeping (e.g., GDPR, HIPAA).
- **Reporting Obligations:** All incidents will be documented and reported in accordance with internal policies and external regulatory requirements.

9. Review and Testing

- **Incident Response Drills:** Regular drills will be conducted to test the effectiveness of the incident response process and ensure that all team members are prepared.
- **Policy Review:** This policy will be reviewed and updated at least annually or following a major incident to ensure it remains effective and relevant.

10. Documentation and Reporting

- **Incident Log:** A comprehensive log will be maintained for all incidents, documenting key actions, decisions, and communications.
- **Post-Incident Report:** A detailed report will be prepared for each incident, summarizing the event, response efforts, lessons learned, and recommendations for future improvements.

This policy document supersedes all previous incident response 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.