Vulnerability Management Policy

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

1. Purpose

This policy establishes a comprehensive vulnerability management framework to ensure the security and integrity of DanfeCorp's information systems, networks, and assets. It defines processes for identifying, assessing, and remediating vulnerabilities in a timely and systematic manner.

2. Scope

This policy applies to all DanfeCorp employees, contractors, third-party vendors, and any systems, networks, applications, or infrastructure owned, operated, or managed by DanfeCorp.

3. Roles and Responsibilities

Role	Responsibilities
Security Team	Responsible for vulnerability identification, risk assessment, mitigation planning, and reporting.
IT Operations Team	Implements patches, mitigations, and configuration changes based on vulnerability assessments.
System Owners	Ensure that remediation actions are taken within defined timelines.
Third-Party Vendors	Must comply with DanfeCorp's vulnerability management requirements and report identified vulnerabilities.

4. Vulnerability Identification

DanfeCorp utilizes a variety of tools and methodologies to identify vulnerabilities, including:

- Automated vulnerability scanning tools.
- Manual security assessments and penetration testing.
- Threat intelligence feeds and security advisories.
- Security incident reports and internal monitoring.
- Vendor security notifications and patch releases.

5. Risk Assessment and Prioritization

Once identified, vulnerabilities are assessed based on the following risk factors:

- Severity Level: Using industry standards such as CVSS (Common Vulnerability Scoring System).
- Impact on Business Operations: Evaluation of potential data loss, downtime, or financial impact.
- Exploitability: Likelihood of exploitation based on available threat intelligence.
- Asset Criticality: Importance of the affected system to business functions.

Priority Level	**Description**	**Remediation Timeline**
Critical (P1)	Vulnerabilities with high severity and exploitability	Must be addressed within 7 days
High (P2)	Vulnerabilities with significant impact	Must be addressed within 14 days
Medium (P3)	Vulnerabilities with moderate risk	Must be addressed within 30 days
Low (P4)	Vulnerabilities with minimal impact	Must be addressed within 90 days

6. Remediation and Mitigation

- Patch Management: IT Operations applies patches based on the severity and impact of vulnerabilities.
- Configuration Changes: Implement hardening and configuration modifications as necessary.
- Compensating Controls: If patching is not immediately possible, temporary controls (e.g., network segmentation, increased monitoring) must be implemented.
- Exception Management: If a vulnerability cannot be remediated within the prescribed timeframe, an exception request with a risk mitigation plan must be submitted for approval by the Security Team.

7. Continuous Monitoring and Reassessment

To ensure ongoing security, DanfeCorp implements the following monitoring practices:

- Regular Scanning: Conduct vulnerability scans at least monthly.
- Penetration Testing: Perform periodic penetration testing (at least annually).
- Continuous Monitoring: Monitor for new threats and vulnerabilities continuously.
- Reassessment: Regularly reassess open vulnerabilities to ensure timely remediation.

8. Reporting and Metrics

Report Type	Frequency	Audience	Content
Weekly Reports	Weekly	IT and Security Teams	Updates on vulnerability remediation progress
Monthly Reviews	Monthly	Leadership	Executive summaries on trends, remediation efforts, and compliance status
Incident Reporting	As needed	Senior Management	Immediate escalation of critical vulnerabilities

9. Third-Party and Supply Chain Security

- Vendor Compliance: All vendors and third-party service providers must adhere to DanfeCorp's vulnerability management standards.
- Pre-Onboarding Assessments: Conduct security assessments before onboarding any vendor with access to critical systems.
- Vendor Reporting: Vendor-reported vulnerabilities must be assessed and remediated according to internal SLAs.

10. Policy Review and Updates

This policy shall be reviewed and updated annually or upon significant changes to DanfeCorp's technology infrastructure or regulatory requirements. The security team must approve all updates.

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