Dallas County Information Technology Threat and Vulnerability Policy

1. Scope

The Dallas County Threat and Vulnerability Policy applies to all Users (County employees, elected officials, contractors, subcontractors, part-time and temporary workers, individuals telecommuting, and those who have been granted access to County's electronic and computing devices).

Computing resources include all Dallas County-owned, licensed, or managed hardware and software, data, information, information assets, Dallas County-assigned user accounts, and use of the Dallas County network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

Because Dallas County owns the network, this Policy applies to technology administered in all departments and divisions, all computers and devices connected (wired and wireless) to the Dallas County network, and to off-site computers that connect remotely to the Dallas County network services.
This policy supersedes all other policies on this topic either written or verbal.

2. Purpose

This document defines the policy necessary to identify who has the responsibility to identify, contain and eradicate threats and vulnerabilities within the County's data networks to reduce risk and unintended data loss.

3. Policy

General Requirements

- Vulnerability Assessments, Penetration Tests, or both will be conducted on Dallas County information systems and data networks twice per calendar year as determined by the Chief Information Security Officer (CISO).
- Vulnerability Assessments, Penetration Tests, or both will be conducted on Dallas County information systems when significant changes to environments occur as determined by the CISO.
- Vulnerability Assessments, Penetration Tests, or both will be conducted before applications are released to production environments as directed by the CISO.
- Vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process will be implemented.
- Vulnerability Scanning will be conducted regularly on the information system (infrastructure/ Cloud environment) and hosted applications to identify potential weaknesses that require secure configuration and patching.
- Vulnerability management will include Identification, reporting, and remediation of information system flaws in software and infrastructure environment, testing fixes for effectiveness and potential side effects before Production implementation.
- Application of vendor-supplied and industry recognized (e.g., NIST NVD, CISA, etc.) security updates and patches will be timely and consistent based on system criticality and vulnerability risk.

Vulnerability Identification

- Dallas County will monitor vulnerability alerting services to identify vulnerabilities that, if exploited, could adversely impact the confidentiality, integrity, or availability (CIA) of Dallas County systems which will Include monitoring, review and deployment of secure configuration and patches.
- Applicability of identified vulnerabilities will be determined by the IT Security Team.
- Response and mitigation will be based on potential impact to the system if exploited and the likelihood of attack from a threat.
- Relevant vulnerability information will be distributed to the appropriate business owners, application administrators, and IT Security.

Vulnerability Standards

- Vulnerability assessments and Penetration Tests will be conducted by authorized staff, contracted third parties, or authorized Dallas County personnel, as defined in the Authorized Staff Section of this document. The Security Team staff will discuss the scope of the assessments with business owners.
- The Security Team will ensure that vulnerability assessments are conducted by personnel with appropriate skills and appropriate methods are followed in the planning, conducting, and reporting of the results of the assessment.
- A combination of automated vulnerability scanning tools and manual testing processes will be employed to provide vulnerability findings of relevant systems.
- Vulnerability assessments will follow a standardized methodology as defined by NIST 800-53.
- Vulnerability assessment findings will be prioritized based on potential impacts to the system if exploited, the likelihood of attack from a threat, and will be documented.
- Frequency of vulnerability assessments will be based on criticality and assessment types as defined in the Frequency of Assessment Section of this document.
- Security Team staff supervising or executing Threat and Vulnerability scans will ensure that scans are appropriately configured.
- Vulnerability scans will include all Dallas County Systems, including internet-facing and internal assets. Scans will be conducted in groups, based on business units or risk classification as deemed feasible by the Security Team.
- Scans of systems will be performed by IT Operations to determine if inherit risks exist in a version of software or model of hardware.
    - Software version risks will be reviewed to determine if a sufficient level of remediation can be accomplished through the application of a patch.
    - Hardware model risks will be reviewed to determine if a compensating control can be applied to ease the risk, or if replacement is required.
- Scans shall be performed during hours appropriate to the business needs of Dallas County's business units in order to minimize disruption to normal business functions.
- Scans will be executed from locations whitelisted by firewalls, anti-virus products, IDS, IPS, and other monitoring services that will not block scan activity.
- Appropriate IT stakeholders will be notified of scan activity ahead of schedule.
- Data and analysis generated from vulnerability scans is to be classified and marked as confidential pursuant to Texas Government Code § 552.139. Any tickets generated due to remediation activities should not contain any confidential data.

Frequency of Vulnerability Assessments

- At a minimum, authenticated vulnerability assessments and Penetration Tests of Dallas County Systems will be executed on a semiannual basis.
- Interim scans will be executed at least monthly, or ad hoc as determined feasible by the Security Team and IT Leadership.
- New information systems purchased from third parties, vendors, contractors or developed within Dallas County will be subject to assessments and multiple vulnerability scans through development lifecycle process before being deploying to Dallas County's production environments.

Approved Scanning Tools

- The Security Team is responsible for approving all tools used to identify vulnerabilities. Unapproved tools will not be utilized to scan Dallas County Systems.
- An enterprise-class vulnerability scanning and assessment tool will be used to conduct scans. This tool will be capable of scanning information systems from a central location and be able to provide remediation suggestions. In the event that scans are being executed on segmented portions of the network and it is not possible to scan from a central location, a local scanning tool may be utilized, once approved by the Security Team. This applies to scans conducted by the Security Team and third parties, vendors, and contractors.
- The vulnerability scanning tool will have the ability to associate a severity value to vulnerabilities, based on the relative impact of the vulnerability on the organization.

Authorized Staff

Threat and Vulnerability scans will only be executed by the Security Team or by qualified third parties, vendors, contractors authorized by the Security Team.

Scans related to the County's technology environments, being executed by a vendor or a third party will be done so under the supervision of the Security Team.

Penetration Testing

Penetration testing is performed regularly by either a certified penetration tester in the security team or an independent third party. Findings from a vulnerability scan or penetration test are analyzed by the Security Officer, together with IT and Engineering as needed, and reported through the process defined in the next section.

Security Findings Reporting and Tracking

Upon completion of vulnerability scans, IT Operations will be responsible for the creation of a Vulnerability report which will summarize the following:

- Name and IP address of the asset that was scanned.
- A list of vulnerabilities identified.
- Severity associated with each vulnerability.
- Detailed information related to the steps or tasks required to remediate or eliminate the vulnerability.

Dallas County follows a simple vulnerability tracking process using the **Trouble Ticketing System**. The records of findings are retained for **2 years**.

Reporting a Finding

- Upon identification of a vulnerability (including a vulnerability in software, system, or process), a ticket is created.
- The description of the Finding should include further details, without any confidential information, and a link to the source.
- The Finding will be given priority level in ticketing system.

Priority/Severity Ratings and Service Level Agreements

To quickly remediate security vulnerabilities, the following timelines have been put in place to address vulnerabilities:

Priority Level		Definition	Examples
Critical		Vulnerabilities that cause a privilege escalation on the platform from unprivileged to admin, allows remote code execution, financial theft, unauthorized access to or extraction of sensitive data, etc.	Vulnerabilities that result in Remote Code Execution such as Vertical Authentication bypass, SSRF, XXE, SQL Injection, User authentication bypass
High		Vulnerabilities that affect the security of the platform including the processes it supports.	Lateral authentication bypass, Stored XSS, some CSRF depending on impact
Medium		Vulnerabilities that affect multiple users, and require little or no user interaction to trigger	Reflective XSS, Direct object reference, URL Redirect, some CSRF depending on the impact
Low		Issues that affect singular users and require interaction or significant prerequisites (MitM) to trigger.	Common flaws, Debug information, Mixed Content

* Highly critical vulnerability with known exploits in the wild and potential for significant impact to Dallas County information system and services, will be subject to remediation timeline override in accordance with Incident Response policy.

In the case a severity rating or priority level is updated after a vulnerability finding was originally created, the Priority is updated as follows:

- Priority upgrade: reset Priority from time of escalation
- Priority downgrade: Priority time remains the same from the time of creation or identification of finding

Resolving a Finding

- The finding should be assigned to the owner responsible for the system or software package.

- All findings should be addressed according to the established SLA.
- No software should be deployed to production with unresolved CRITICAL or HIGH findings unless an Exception is in place (see below).
- A finding may be resolved by:
    1. providing a valid fix or mitigation, which will included deploying patches in a timely manner or product/hardware replacement
    2. determining as a false positive
    3. documenting an approved exception

Closing a Finding

- The assignee should provide a valid resolution (see above) and add a comment to the finding.
- The finding should be re-assigned to the reporter or a member of the security team for validation.
- Upon validation, the finding can be marked as Done (closed) by the reporter.
- Before the finding can be marked as closed by the reporter, the fix must be deployed to a development environment and have a targeted release date for deploying to production noted on the ticket.

Priority of Remediation

- "High" or "Critical" vulnerabilities will be fully addressed within 30 calendar days of discovery.
- "Medium" level vulnerabilities will be addressed within 60 calendar days of discovery.
- "Low' level vulnerabilities will be addressed within 90 calendar days of discovery.
- “Informational” vulnerabilities will be reviewed to ensure they do not pose a significant threat to Dallas County Systems.
- An exception must be filled out and approved if vulnerabilities are not capable of being remediated. This exception must be submitted to the Compliance Committee for approval as defined in the Exception Section of this document.
- The report will be submitted to the Dallas County CIO and the Compliance Committee.
- The Security Team will ensure that vulnerability scan results, data or reports are not be altered or tampered with to ensure an objective assessment of risk to Dallas County.

4. Roles and Responsibilities

Chief Information Security Officer (CISO)

- Sponsor Threat and Vulnerability policy enforcement across Dallas County.
- Review and approve frequency of vulnerability scanning activities based on the risk classification of Dallas County Systems.
- Conduct periodic compliance reviews of Dallas County Systems.
- Procure resources to conduct vulnerability assessments.
- Ensure that there is no conflict of interest between staff who conduct vulnerability assessments and ownership of Dallas County Systems.
- Review vulnerability assessment reports to determine and present the risk posture of Dallas County’s assets to the Compliance Committee.

- Sponsor policies, procedures, and practices to comply with assessment results or remediate vulnerabilities.

Security Team

- Enforce Threat and Vulnerability policy across Dallas County.
- Identify and provide an enterprise-class vulnerability scanning product.
- Notify Asset owners and relevant stakeholders of scanning activities ahead of schedule.
- Determine groups of Dallas County's assets based on risk classification, business unit, or other criteria as directed by the Security Team.
- Execute non-intrusive vulnerability assessment scans in accordance with the schedule approved by the Change Control Committee.
- Ensure that scans are configured NOT to attempt Denial of Service attacks or other exploits.
- Supervise scanning activity, if conducted by a third-party vendor.
- Report vulnerabilities identified in Dallas County Systems to the IT Services Department.
- Identify remediation tasks aimed at eliminating vulnerabilities identified in Dallas County Systems.
- Sponsor policies, procedures, and practices to comply with assessment results or remediate vulnerabilities.

Chief Information Officer (CIO)

- Review enterprise risk reports and support enforcement and compliance with this policy across Dallas County.
- Escalate matters as needed to appropriate leadership.

IT Staff

- Support and comply with the Threat and Vulnerability policy.
- Engage with the Security Team to understand the nature of vulnerabilities and draft a vulnerability remediation strategy.
- Identify potentially negative impact to Dallas County Systems, as a result of installation of a specific patch or remediation activity.
- Perform vulnerability remediation activities as directed by the Change Management Committee.
- Report identified computer security incidents to the Security Team.
- Identify, record, and share any clues, behavior, or anomalies that may assist with determining the cause of a potential incident.

5. Periodic Reviews and Audits

- Ensure two vulnerability tests are performed in each calendar year.
- This policy will be reviewed and updated on an annual basis.

6. Enforcement and Exception Handling

Failure to comply with this Policy can result in a loss of access and disciplinary actions, up to and including termination of employment, contracts or other relationships. Additional legal actions may also be taken in response to violations of applicable regulations and laws.

Requests for exceptions to Dallas County security policies should be submitted to the ServiceDesk and routed to the Security Team. Exceptions will be permitted only upon receipt of written approval from the Dallas County CIO, with deference to the security processes as determined by the Compliance Committee.

7. Appendix

- The Priority remediation goal is to meet or beat the Average time in the below table by asset importance and vulnerability importance.

  The below table shows a notional example of actionable performance metrics. Each cell provides mitigation metrics based on the relative importance of the assets (low, moderate, or high) and the vulnerabilities (low, medium, high, or critical), with the categories defined by the organization. The metrics in each cell also reflect the percentage of assets that were patched by the corresponding maintenance plans' deadlines, as well as the average (mean) time and median time for patching.

Vulnerability Importance	Asset Importance		
	Low	Moderate	High
Low	By deadline: 64.7 % Average time: 80.4 days Median time: 75.2 days	By deadline: 72.4 % Average time: 34.7 days Median time: 33.7 days	By deadline: 85.0 % Average time: 14.6 days Median time: 8.1 days
Medium	By deadline: 66.5 % Average time: 75.1 days Median time: 70.7 days	By deadline: 68.7 % Average time: 33.2 days Median time: 31.6 days	By deadline: 71.4 % Average time: 12.9 days Median time: 10.5 days
High	By deadline: 68.6 % Average time: 62.1 days Median time: 58.0 days	By deadline: 78.8 % Average time: 26.8 days Median time: 22.1 days	By deadline: 85.5 % Average time: 8.8 days Median time: 8.1 days
Critical	By deadline: 81.4 % Average time: 44.4 days Median time: 41.3 days	By deadline: 92.3 % Average time: 21.2 days Median time: 23.9 days	By deadline: 95.2 % Average time: 5.2 days Median time: 5.1 days

National Institute of Standards and Technology (NIST) 800 - 40 r4 - Vulnerability Mitigation Time Summary Matrix

8. References

NIST SP 800-53 - Moderate Baseline Control Objectives
NIST SP 800-40 - Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology
FBI Criminal Justice Information Services (CJIS) Version

Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, as amended
Payment Card Industry-Data Security Standard Version

9. Revision History

Date:	***version #:***	***Description:***	***Updated by:***
06/07/21	1.0	Initial Draft	Security Team
04/22/2022	1.1	2022 Plan	Security Team
10/10/2022	1.2	Patch Mgmt. updates	Security Team
8/28/23	1.3	Review and Revisions	Chief Privacy Officer