Vulnerability Management Policy

Policy #: TC-ITS-255 **Approved By**: Paul Hopingardner, County Executive, Technology & Operations
Version #: 1.0 **Effective Date**: March 1, 2019

Accountability & Responsibility

This policy is governed by the accountability and responsibility section found here.

Purpose

The purpose of this policy is to define the roles and responsibilities for Information Technology Services (ITS) employees and the requirements for notification, testing, and installation of security-related patches on devices connected to Travis County Information Technology (IT) infrastructure. This includes Internet of Things (IoT) devices, which are devices such as fitness tracking watches, drones, or smart thermostats, that can send and receive information by being connected to the Internet.

Policy

All IT infrastructure risks must be actively managed by undergoing regular scans to ensure vulnerabilities are addressed and remediation efforts prioritized on a risk basis.

Roles and Responsibilities

The Information Security Team maintains the vulnerability management solution, generates reports, and monitors the vulnerability posture of the County. They ensure that systems are scanned for vulnerabilities on a regularly scheduled basis and prioritizes remediation needs discovered from vulnerability scans based on risks.

Operations maintains the patching capability, determines the schedule for routine patching, and works with the Information Security Team to remediate newly discovered vulnerabilities.

The Chief Information Security Officer (CISO) approves the acceptance of risks, compensating controls, and vulnerability recasts identified through the vulnerability management process.

The County Executive, Technology & Operation (CETO) is apprised of the County's vulnerability to risk and is briefed on the mitigation or acceptance of risks on a monthly basis.

Notification

Stakeholders will be advised when vulnerability scanning is taking place through the scanning schedule on the Security Operations SharePoint calendar.

Vulnerability Scanning

Vulnerability scanning is a security technique used to identify security weaknesses in a computer system and includes both external and internal systems. Using authenticated scanning will result in more accurate and complete vulnerability scanning reports, but unauthenticated scanning should be used periodically to gain an attacker's perspective. The single internal baseline vulnerability policy scan will be conducted at least once a month on the entire network. Exceptions may exist, but must fit into one of the exceptions described in this policy.

Once scanning is complete, the results are analyzed by the Information Security Team for an initial vulnerability prioritization. This includes negating false positives, (i.e., Windows vulnerability on a UNIX system) or taking additional steps via penetration testing to validate the exposure.

Results of the scan and prioritization are then reviewed by Operations or the appropriate Department IT. The manager works with their staff to schedule the work to resolve the vulnerability and provides a response plan of action.

Once a change is implemented, Information Security rescans for the vulnerability to verify the resolution. If the vulnerability is still present another solution may be attempted or alternative compensating controls will be put in place. In the event there is no practical solution, the risk must to be accepted by the business unit and tracked in the risk register.

Risk Prioritization
Travis County uses the Common Vulnerability Scoring System (CVSS) for all Common Vulnerabilities and Exposures (CVE) provided by the National Vulnerability Database. A “critical” rating is given to a vulnerability if it is activity being exploited. However, the calculation does involve other variables. Priority will be placed on patching or mitigating the vulnerability based on a combination of CVSS scores, criticality, number of the systems affected, and the impact to business processes.

Vulnerabilities discovered during scans are evaluated and prioritized by the Information Security Team. Recommendations are derived from the evaluation of both risk and work-effort are then passed to Operations or the appropriate Departmental IT for testing and deployment.

The following is recommended to help prioritize vulnerabilities to be remediated or mitigated:

- Identify High value information assets and internet-accessible systems.
- Fix oldest vulnerabilities first.
- Fix vulnerabilities from publicly available exploits and/or those that are included in automated tools.
- Fix the vulnerabilities that are present on the highest number of assets.

The Information Security Team will meet periodically with Operations to review and evaluate both patched and unpatched vulnerabilities to review the priorities of vulnerabilities not otherwise being addressed by regular patching. Vulnerability information is also communicated with Department Information Technology personnel responsible for the impacted systems outside the management responsibility of Operations.

Remediation
Remediation is prioritized based primarily on risk. For example, an Internet web server susceptible to a vulnerability granting administrative level access should be remediated before an internal system requiring a “low” severity security patch. Consideration for work-effort is part of the remediation process. For example, the inability to patch a legacy system may result in the acceptance of the risk.

Travis County personnel are expected to cooperate with a vulnerability assessment being conducted on systems for which they are responsible and cooperate in formulating a remediation plan.

Patches are tested in a non-production environment to determine if there are system compatibility issues. If a patch is not available, a compensating control is developed to mitigate the risk of not having a patch.

A compensating control might include:

- Creating log analysis rules to look for any indications that the risk is being exploited
- Using a white or blacklisting application to monitor for any changes to the device
- Implementing additional firewall rules to restrict access to suspect IP addresses used by exploits

Remediation Targets
Since prioritization includes additional criteria other than the CVSS score, an interruption of critical service, the sensitivity of the data, or complexity of remediation could delay action. Delayed action in the mitigation of real vulnerabilities that cannot be mitigated in the time frame specified in the remediation target because of complications like business impact (downtime to apply remediation) or testing that is required to ensure operations are not affected by the recommended remediation, are documented with justification and an expiration date.

Remediation targets are identified in the following chart:

Remediation Targets		
Severity	**Description**	**Service Level**
Critical	Critical vulnerabilities have a CVSS score of 8.0 or higher. They can be readily compromised with publicly available malware or exploits.	7 Days

High	High-severity vulnerabilities have a CVSS score of 8.0 or higher, or are given a High severity rating by PCI DSS v3. There is no known public malware or exploit available.	30 Days
Medium	Medium-severity vulnerabilities have a CVSS score of 6.0 to 8.0 and can be mitigated within an extended time frame.	90 Days
Low	Low-severity vulnerabilities are defined with a CVSS score of 4.0 to 6.0. Not all low vulnerabilities can be mitigated easily due to applications and normal operating system operations. These should be documented and properly excluded if they can't be remediated.	180 Days

Scanning Process Exemptions
Vulnerability management scanning is an essential practice and the goal is to have 100% participation. If participation creates issues for a system, the system owner or administrator shall work directly with Information Security to review possible options. Those options might include disabling a specific vulnerability check that may be causing an issue. An approach that solves the specific problem is preferred over a general exemption as more general exemptions may cause critical vulnerabilities to be missed.

Risk Acceptance or Risk Recasting
While every effort must be made to correct issues, some vulnerabilities cannot be remediated. Vendors may have appliances that cannot be patched, services may be exposed for proper application operations, and systems may still be commissioned that are considered end-of-life by the developer or manufacturer. In these cases, accepting the risk or recasting the vulnerability score may be appropriate.

In some cases, there may be no option except to accept an unmitigated risk. Accepted risk vulnerabilities are those where the vulnerability is real, but compensating controls are in place to mitigate the risk or the service has been deemed too critical for intervention. Recasting the vulnerability involves rescoring a vulnerability based on specific information that either decreases or increases the impact vulnerability could have on your specific environment. The NIST Common Vulnerability Scoring Calculator can provide a repeatable manner and guidance on recasting.

All exceptions must present justification for the request and an expiration date. No exception can be permanent and have an expiration date to ensure no exceptions are permanently ignored. The Security Team will review all exceptions at least quarterly to validate that the exceptions are still appropriate. Exceptions will be removed when no longer required and the appropriate system administrators are notified. All risks accepted will be entered into the Risk Registry and reviewed at least annually.

Policy Revision

Version	Purpose/Changes	Editor	Date
1.0	Travis County Information Technology Services Information Security Policies Creation	Paul Knight	1/31/2019
1.1	Updated title of approver	Brandon Rogers	11/07/2019
1.2	Added IoT to Purpose	Larissa Derrick	11/15/19