Travis County Technology & Security Policies

Risk Analysis Policy

Policy #: TC-ITS-215 **Approved By**: Paul Hopingardner, County Executive, Technology & Operations
Version #: 1.4 **Effective Date**: May 30, 2015

Accountability & Responsibility

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

Purpose

The purpose is to conduct an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of sensitive information held by the organization.

Policy

Travis County will conduct an accurate and thorough assessment of risks and vulnerabilities to the confidentiality, integrity, and availability of sensitive information, such as ePHI, PII, and CJI. Such risk analysis activities will be conducted at least once per year or in response to environment and/or operations, security incidents, or occurrence of a significant event. This assessment must result in a comprehensive Risk Analysis Report that summarizes the risks and vulnerabilities to the confidentiality, integrity, and availability of sensitive information. This report must also identify recommended safeguards and prioritize all such risks and vulnerabilities. The risk analysis should be distributed to all persons who are responsible for mitigating identified risks.

Procedure(s)

Risk is defined as the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence. The minimal activities that Travis County will conduct in each phase are as follows:

Phase I: Documentation Phase

- Identify what sensitive information is collected
- Identify systems with sensitive information
- Document the purpose of these systems
- Document the flow of sensitive information

Phase II: Risk Assessment Phase

- Identify vulnerabilities and threats to sensitive information
- Describe the risks
- Identify controls
- Describe the level of risk

Phase III: Safeguards Determination Phase

- Recommend safeguards for sensitive information
- Determine residual risk to sensitive information

Phase IV: Audit Reporting

- Create and distribute audit reports to appropriate workforce members for review
- Retain audit reports for a minimum of six years from the date of its creation or when it was last in effect, whichever is later

Policy Revision

Version	Purpose/Changes	Editor	Date
1.0	Travis County Information Technology Services Information Security Policies Creation	Randy Lott	05/30/2015
1.1	Updated Policy paragraph to be more specific for when audits may need to be done.	ITS Policy Committee	09/16/2016
1.2	Added policy statement to include this sentence: The risk analysis should be distributed to all persons who are responsible for mitigating identified risks.	ITS Policy Committee	10/12/2016
1.3	Updated name of CIO	Randy Lott	12/18/2017

Version	Purpose/Changes	Editor	Date
1.4	Updated policy number from 120 to 215 and updated approver's title.	Joyce Miller	11/20/2019