# Security Incident Procedures Policy

**Policy #:** TC-ITS-245 **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 identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to Travis County, and document security incidents and their outcomes.

## Policy

Travis County will do the following:

- Identify, research, and respond to any suspected security incidents in a timely manner
- Mitigate, to the extent practicable, any harmful effects of any suspected or actual security incidents
- Maintain appropriate documentation for all security incidents

## Procedure(s)

Travis County will maintain procedures for identifying events that qualify as security incidents. A security incident is any breach of security policy or any activity that could potentially put sensitive information at risk of unauthorized use, disclosure, or modification.

A breach, such as one as defined under the HITECH Act or Texas Breach Law, or CJIS, may have occurred if the incident involved ePHI, PII, CJI or other sensitive information. A breach is defined as the unauthorized acquisition, access, use, or disclosure of protected information (as defined below), which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. If a breach has occurred, members of the workforce must immediately follow the instructions in TC-ITS-501, Data Breach Discovery Policy.

Incidents will be classified by the following severity level:

- **RED:** High risk of financial, data and reputation loss as well as downtime (Regulatory Data or Financial Fraud involved).
- **YELLOW:** Small risk of financial or data loss. Some downtime may be experienced. (No Regulatory Data or Financial Fraud involved).
- **GREEN:** Potential interruption of normal daily operations. Minimal financial, data, and reputation loss risks. Security concern that needs to be addressed.

Response level dictates how quickly the response needs to be and who should be activated to respond:

- **Level 1**: These are the most severe security incidents facing Travis County. All the TCSIR-Team will be involved in the immediate response effort. A FORMAL INCIDENT REPORT IS REQUIRED.
- **Level 2**: These are not as severe as Response Effort 1, but are still very serious. The response by the majority of the TCSIR-Team needs to be quick, if not immediate. A FORMAL INCIDENT REPORT IS REQUIRED.
- **Level 3**: These security incidents have some impact on the infrastructure, but do not pose a large threat for Travis County. A small amount of TCSIR-Team members will be involved in handling Severity 4 security incidents. NO FORMAL INCIDENT REPORT IS REQUIRED
- **Level 4**: Security incidents that will need to be investigated. NO FORMAL INCIDENT REPORT IS REQUIRED.

Please see the Travis County Incident Response Plan “Incident Threat Matrix” for determining Severity and Response Level.

All workforce members of Travis County will report any security incident to their department or office management team and to the ITS Service Desk. If ePHI or PII is involved, also notify the HIPAA Privacy Officer, HIPAA Security Officer, and the CIO, or their designee, that they become aware of or suspect, as soon as practical. If CJI is involved, notify the Travis County CJIS Local Agency Security Officer (LASO).

Workforce members will not disclose the incident information to anyone other than the Chief Information Officer or their designee, HIPAA Security Officer, HIPAA Privacy Officer, LASO, and their department or office management team, and will not disclose any information about the incident to anyone or in any place outside of Travis County.

Workforce members must report security violations as quickly as possible after discovery to their immediate supervisors, the ITS Service Desk Information Security group, or designees, as appropriate. If the violation is HIPAA-related, workforce members must also report to the HIPAA Privacy Officer and the HIPAA Security Officer, CJIS LASO or designees, as appropriate, depending on the type of information involved.

Travis County will maintain procedures for responding to serious and non-serious security incidents in order to prevent the escalation of the incident and to prevent future incidents of a similar nature.

Incidents characterized as serious by the CIO, HIPAA Privacy Officer and HIPAA Security Officer, LASO and/or the department or office management team or their designee, will be responded to immediately.

Travis County will attempt to mitigate any harmful effects, when possible, of security incidents that affect client information.

## 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 | Modified procedure to include event terminology. | Security Policy Team | 01/15/2016 |
| 1.2 | Merged Response and Reporting Policy (119) into this policy. | Security Policy | 08/19/2016 |
| 1.3 | Consolidated Severity Levels to RED, YELLOW and GREEN. Consolidated Response Levels to 1, 2, 3 and 4. Updated name of CIO. | Randy Lott | 12/18/2017 |
| 1.4 | Updated policy number from 125 to 245 and updated approver's title. | Joyce Miller | 11/20/2019 |