Travis County Technology & Security Policies

Audit Controls Policy

Policy #: TC-ITS-110 **Approved By**: Paul Hopingardner, County Executive, Technology & Operations
Version #: 1.2 **Effective Date**: May 30, 2015

Accountability & Responsibility

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

Purpose

The purpose is to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use sensitive information.

Policy

Travis County will identify critical systems that require event auditing capabilities, define the events to be audited on all such systems, and protect all collected logs from alteration or destruction.

Procedure(s)

At a minimum, event auditing capabilities will be enabled on all systems that process, transmit, and/or store sensitive information. Events to be audited may include, and are not limited to, logins, logouts, and file accesses, deletions, and modifications. Internal clocks will be mapped to a universal time to ensure accurate time stamps for audit records.

Audits may be conducted for the following reasons:

- Ensure confidentiality, integrity, and availability of sensitive information.
- Investigate possible security incidents and ensure conformance to Travis County security policies.
- Monitor user or system activity where appropriate.

Travis County will ensure the protection of all audit reports and log files and will review the usage of software and application tools to review audit files. If a malfunction occurs within the audit process, an alert is received and the system is either shut down, the oldest audit records are overwritten, or the system stops generating audit records.

When requested, and for the purpose of performing an audit, any access needed will be provided to authorized members of Travis County security team. This access may include the following:

- User level and/or system level access to any computing or communications device.
- Access to information (electronic, hardcopy, and so on) that may be produced, transmitted, or stored on Travis County equipment or premises.
- Access to work areas (labs, offices, cubicles, storage areas, and so on).
- Access to interactively monitor and log traffic on Travis County networks.

Travis County will protect all collected logs from improper alteration or destruction even by Travis County privileged users such as Administrators or root accounts. Audit records will be retained according to Travis County requirements and to support after the fact investigations.

Travis County logs should seek to follow “Write Once, Read Many” standards so that they cannot be altered once they are written.

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 title of approver.	Brandon Rogers	11/07/2019
1.2	Renumbered from 302 to 110.	Joyce Miller	11/20/2019