Sanction Policy

Policy #: TC-ITS-225 **Approved By**: Paul Hopingardner, County Executive, Technology & Operations
Version #: 1.3 **Effective Date**: May 30, 2015

Accountability & Responsibility

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

Purpose

The purpose is to ensure that appropriate disciplinary action (sanction) is applied to workforce members who do not comply with to the Travis County Technology and Security Policies for safeguarding sensitive information, such as ePHI, CJI and PCI.

Policy

Travis County appropriately disciplines employees and workforce members in a manner appropriate for the gravity of the violation for any violation of the-technology and security policies. Sanctions may include counseling, re-training, verbal or written warnings, reassignment to a job that does not have access to sensitive information, suspension of access to sensitive information, suspension of employment, and immediate termination of employment. These are implemented, in conjunction with other applicable polices related to personnel actions, like Chapter 9 of the Travis County Code, the Civil Service rules and regulations, Juvenile Probation Personnel Policies and any other relevant departmental disciplinary policies.

Workforce members who knowingly and willfully violate state or federal law for improper use or disclosure of a patient's information may be subject to criminal investigation and prosecution or civil monetary penalties.

Sanctions also apply to workforce members who fail to complete training.

Procedure(s)
Commissioners Court Departments

1. Travis County, through its Security or Privacy Officer, Department Head, or Human Resources Management Division (HRMD) fully investigates the circumstances around an alleged privacy or security violation after making a notification to the attention of the workforce member's Department head.

2. The Security Officer provides technical detail relating to the alleged policy violation to the Department Head for review. The Department Head initiates an inquiry or investigation into the alleged policy violation, through supervisory chains of command, HRMD, or the Compliance Officer, as appropriate.

3. If it is determined by investigating parties, that a policy violation has occurred, the investigating parties, in consultation with HR employee relations, evaluate the investigative information to determine severity of the violation and to execute the appropriate discipline.

    - The potential impact to Travis County of any violation or breach is considered in determining appropriate sanctions against workforce members. Other factors considered are the type of violation and the cause or motivation that caused the violation, such as:

Violation Type	Cause or Motivation
Errors in handling restricted or sensitive information or in maintaining security measures	• Unintentional • Lack of Training • Failure to Complete Training • Inexperience • Poor Judgement • Poor Process

Violation Type	Cause or Motivation
Policy Violation	• Intentional, but not malicious • Concern for Individual • Carelessness
Policy Violation with intent or gross negligence	• Malicious intent • Curiosity (snooping) • Financial Gain • Revenge • Protest • Gross Negligence

4. An intentional violation of these technology and security policies must be established by clear evidence (i.e., evidence that the disclosure was intentional and deliberate and the workforce member knew that the action violated the policies and procedures as set forth in the Travis County Technology and Security Policies.)

5. Workforce members failing to cooperate in a timely and fully cooperative manner to requests from parties investigating violations or breaches will be considered to be intentionally violating these technology and security policies.

6. The sanction for an unintentional failure to comply with these policies or procedures varies, depending on the relevant facts and circumstances. At a minimum, the workforce member is required to meet with the Security or Privacy Officer to review the violation and demonstrate, to the satisfaction of the Security or Privacy Officer, that he or she understands the relevant policies and procedures.

7. If a workforce member has previously violated these policies and procedures, the following procedures apply:
    - Second offense of noncompliance: The workforce member receives a written reprimand to be filed in such workforce member's personnel file.
    - Subsequent offenses: A pattern of repeated violations results in the workforce member's transfer to another position, suspension or termination.

8. If the Security or Privacy Officer is the workforce member who has committed the violation, the Security or Privacy Officer's supervisor or other appropriate official of Travis County, such as the Commissioners Court, determines and imposes sanctions for the Security or Privacy Officer.

9. All workforce member sanctions will be documented and retained for a period of at least 6 years from the date of its creation or the date when it was last in effect, whichever is later. An unproven or unsubstantiated allegation of a violation does not require documentation unless it is pursuant to another requirement under these policies such as a complaint.

Non-Commissioners Court Departments.

1. Travis County Covered Components appropriately and consistently discipline workforce members who are found to violate these technology and security policies in accordance with this sanctions policy.

2. Departments record all disciplinary actions taken in the workforce member's employment records. The Security or Privacy Officer is made aware of the sanctions in general terms for purposes of documenting corrective action.

Sanctions Against Workforce Members Not Directly Employed by Travis County

Commissioners Court Departments:

If a workforce member not directly employed by Travis County violates the County's technology and security policies and procedures, then the Security or Privacy Officer, in consultation with appropriate parties, such as the Purchasing Agent or County Attorney, considers the impact to the organization, causes and motivations related to the violations, and recommends to Department Heads over Covered

Components appropriate corrective actions which may include retraining, termination or modification of contracts, or termination or modification of volunteer agreements.

Non-Commissioners Court Departments:

If a workforce member not directly employed by Travis County violates the County's technology and security policies and procedures, then the Elected or Appointed Official or their designee, in consultation with appropriate parties, such as the Purchasing Agent or County Attorney considers the impact to the organization, causes and motivations related to the violations, and recommends to take corrective actions which may include retraining, termination or modification of contracts, or termination or modification of volunteer agreements. The Security or Privacy Officer is available for technical assistance.

1. Covered Components inform the Security or Privacy Officer of sanctions taken against workforce members not directly employed by Travis County. The Security or Privacy Officer documents these actions.

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	Revamped to mirror Privacy Sanction policy.	ITS Policy Committee	10/25/2016
1.2	Updated name of CIO	Randy Lott	12/18/2017
1.3	Updated policy number from 122 to 225 and updated approver's title.	Joyce Miller	11/20/2019