Identity and Access Control Policy

Policy #: TC-ITS-166 **Approved By**: Paul Hopingardner, County Executive, Technology & Operations
Version #: 1.8 **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 policies and procedures for creating a unique name and/or number for identifying and tracking user identity and for authorizing, granting, validating, terminating and documenting access to sensitive information based on their role or function.

Policy

Travis County will ensure that each individual who accesses sensitive information, such as ePHI, PII, or CJI, at Travis County will be granted some form of unique user identification, such as a login ID.

Travis County shall implement policies and procedures for authorizing, granting, validating, terminating and documenting access to sensitive information based on their role or function. Travis County members of the workforce are granted access only to the minimum necessary sensitive information which they are authorized in order to perform their job role or associated job function.

Travis County will terminate access to all systems and facilities when any member of the workforce or entity Travis County has other arrangements with has been terminated or no longer requires access to information or facilities in order to perform their assigned job role.

Travis County will configure all systems that support automatic logoff to require logoff after a predetermined period of time. If systems do not support automatic logoff capabilities, Travis County will request those capabilities from the appropriate vendor and document all vendor responses.

Procedure(s)

Authorizing

Travis County determines data owners for all sensitive information. The data owner ultimately determines which members of the workforce have authorization to access sensitive information subject to any applicable County policies related to oversight of that authority. For instance, access to HIPAA data is authorized by the Privacy Officer in accordance with applicable privacy policies.

Travis County uses Role Based Access Control (RBAC) methodologies for assigning authorization to sensitive information and that access will be the minimum necessary to complete their jobs.

Each individual's job description must be reviewed to determine the following:

- Individual rights
- The rights of group(s) that the individual belongs to

The principle of least privilege and separation of duties shall be factors that influence the access rights granted to an individual or an entity. The fundamental principle of "need to know" will be applied within Travis County to determine access privileges.

Travis County will give strong authentication preference to users that pose a higher risk to the organization. Such users include, but are not limited to, the following types:

- Users that have administrator rights to systems that contain sensitive information
- Users that have portable computing devices such as laptops that may be carried off the premises

Creating
Each individual who is authorized to access Travis County data and/or sensitive information, such as ePHI, PII, or CJI, at Travis County will be granted some form of unique user identification, such as a login ID.

At no time will any workforce member allow anyone else to use their unique ID. Likewise, at no time will any workforce member use anyone else's ID.

Travis County will develop a standard convention for assigning unique user identifiers.

Travis County will maintain a secure record of unique user identifiers assigned.

Travis County will track individual activities and record events as required by policies such as TC-ITS-130, Audit Controls Policy and TC-ITS-175, Information System Activity Review Policy.

Travis County will minimize the use of generic accounts, especially those that are privileged and generic such as Windows Domain Administrator or Unix Linux root accounts, to an absolute minimum required for the current activity. Travis County will seek to create unique, individual accounts for privileged access with similar access rights so that activities may be tied to a single individual.

Granting
Access to sensitive information will be granted only if the data owner authorizes that the individual has a legitimate business need for the information. Reasonable efforts will be made to limit the amount of information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Validating
A regular review by the data owner shall be conducted to ensure that access rights for each individual or entity are consistent with established policies, job roles, and functions and are the minimum necessary required to carry out their duties.

Travis County will continually assess potential risks and vulnerabilities to sensitive electronic authorized information in its possession and develop, implement, and maintain appropriate security measures so that access is only provided to members of the workforce who are authorized to view such information.

Automatic Logoff
Travis County will maintain procedures for automatic logoff of systems that contain sensitive information after a period of inactivity. The length of time that a user is allowed to stay logged on while idle will depend on the sensitivity of the information that can be accessed from that computer and the relative security of the environment that the system is located. Travis County will periodically inspect systems to ensure that the automatic session logoff capability is configured correctly.

Training
All members of the workforce will be appropriately trained so they understand Travis County's policies related to accessing authorized information only.

Documenting
All requests to add or modify access rights will be maintained with the change management system.

Transfers
Any transfers of a workforce member or other arrangement with Travis County must immediately result in the Human Resource Management Department (HRMD), Business entity (data owner), and the Information Technology Services (ITS) departments coordinating their activities within a timely manner to ensure the following:

- Access is revoked to all physical locations and electronic systems and applications no longer needed
- Any computing equipment, resources, documentation, or other assets issued or provided are returned as needed

Termination of access will be verified and segregation of duties will be applied to ensure immediate and complete termination of all access including electronic and physical.

Termination
Any termination of a workforce member or other arrangement with Travis County must immediately result in the Human Resource Management Department (HRMD), Business entity (data owner), and the Information Technology Services (ITS) departments coordinating their activities within 24 hours of termination to ensure the following:

- Password access is immediately revoked
- Access to all systems and applications is revoked
- Removal from any systems or applications that processed sensitive information
- All digital certificates are revoked
- Any tokens or smart cards issued are disabled and returned
- Any computing equipment, resources, documentation, or other assets issued or provided are returned
- Any keys, IDs, and badges provided during their employment are returned
- The workforce member is not provided any access to their desk or office or, if provided, the access is limited and carefully supervised

If listed items cannot be returned to Travis County for any reason, compensatory controls must be implemented. ITS will provide feedback to HRMD, and/or the affected department or office, on the success or failure of access termination.

Termination of access will be verified and segregation of duties will be applied to ensure immediate and complete termination of all access including electronic and physical. ITS will provide feedback to HRMD on the success or failure of access termination.

All procedures will be consistent and in coordination with Human Resources Policies and Travis County Code.

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	Merged Access Control & Validation Policy (201), Access Control Policy (301), Access Establishment & Modification Policy (103) and Information Access Management Policy (113).	ITS Policy Committee	05/20/2016
1.2	Merged Workforce Security Policy (131) into this policy.	ITS Policy Committee	06/24/2016
1.3	Renamed from Access Authorization Policy to Access Control. Merged Automatic Logoff Policy (303) into this policy.	ITS Policy Committee	7/29/2016
1.4	Merged Termination Procedure Policy (129).	ITS Policy Committee	8/19/2016
1.5	Merged Authorization and/or Supervisor Policy (106)	ITS Policy Committee	8/26/2016
1.6	Merged Unique User Identification Policy (309)	ITS Policy Committee	10/06/2016
1.7	Updated name of CIO	Randy Lott	12/18/2017
1.8	Updated policy number from 102 to 166 and updated title.	Joyce Miller	11/20/2019