Section	**IS Security Policies**	05/01/12	-Effective
		12/10/11	-Revised
Policy 1.00	**Data Classification**	Information Services	-Author

Introduction

Data Classification provides a framework for managing data assets based on value and associated risks and for applying the appropriate levels of protection as required by state and federal law as well as proprietary, ethical, operational, and privacy considerations. All TSSWCB data, whether electronic or printed, should be classified. The data owner, who is responsible for Data Classification, should consult with legal counsel on the classification of data as Confidential, Agency-Sensitive, or Public. Consistent use of data classification reinforces with users the expected level of protection of TSSWCB data assets in accordance with TSSWCB security policies.

Purpose

The purpose of the TSSWCB Data Classification Policy is to provide a foundation for the development and implementation of necessary security controls to protect information according to its value and/or risk. Security standards, which define these security controls and requirements, may include: document marking/labeling, release procedures, privacy, transmission requirements, printing protection, computer display protections, storage requirements, destruction methods, physical security requirements, access controls, backup requirements, transport procedures, encryption requirements, and incident reporting procedures.

Audience

The TSSWCB Data Classification Policy applies equally to all individuals who use or handle any TSSWCB Information Resource.

Ownership

TSSWCB data created, sent, printed, received, or stored on systems owned, leased, administered, or authorized by the TSSWCB are the property of the TSSWCB and its protection is the responsibility of the TSSWCB owners, designated custodians, and users.

Policy

Data shall be classified as follows:

Confidential. Sensitive data that must be protected from unauthorized disclosure or public release based on state or federal law, (e.g. the Texas Public Information Act) and other constitutional, statutory, judicial, and legal agreements.

Examples of "Confidential" data may include but are not limited to:

- Personally Identifiable Information, such as: a name in combination with Social Security Number (SSN) and/or financial account numbers
- Student Education Records
- Intellectual Property, such as: Copyrights, Patents and Trade Secrets
- Medical Records

Agency-Sensitive. [optional AGENCY defined category that **may be identified as: Agency "Security-Sensitive", "P**rivileged", or "Protected"**]**. Sensitive data that may be subject to disclosure or release under the Texas Public Information Act, but requires additional levels of protection.

Examples of "Agency-Sensitive" data may include **but are not limited to**:

- TSSWCB operational information
- TSSWCB personnel records
- TSSWCB information security procedures
- TSSWCB research
- TSSWCB internal communications

Public. Information intended or required for public release as described in the Texas Public Information Act.

Exception	Information owned or under the control of the United States Government must comply with the federal classification authority and federal protection requirements.
Disciplinary Actions	Violation of this policy may result in disciplinary action, which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of TSSWCB Information Resources access privileges, and to civil and criminal prosecution.
References	**National/Federal** Copyright Act of 1976 Foreign Corrupt Practices Act of 1977 Computer Fraud and Abuse Act of 1986 Computer Security Act of 1987 The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Gramm-Leach-Bliley Act of 1999 Sarbanes-Oxley Act of 2002 Family Education Rights and Privacy Act of 1974 Uniform Trade Secrets Act Payment Card Industry Data Security Standard (https://www.pcisecuritystandards.org/) **Texas** DIR Practices for Protecting Information Resources Assets (http://dir.state.tx.us/pubs/) DIR Standards Review and Recommendations Publications (http://dir.state.tx.us/pubs/) Texas Administrative Code, Title 1, Part 10, Chapter 202 – Information Security Standards Texas Business and Commerce Code, Chapter 48 – Consumer Protection Against Computer Spyware Act Texas Business and Commerce Code, Chapter 521 – Unauthorized Use of Identifying Information Texas Government Code, Chapter 441 – Libraries and Archives Texas Government Code, Chapter 552 – Public Information Act Texas Texas Government Code, Chapter 2054 – Information Resources Management Act Texas Penal Code, Chapter 33 – Computer Crimes Texas Penal Code, Chapters 33A – Telecommunications Crimes