**Data Classification and Management Policy**
**Version: 1.5.0**

## Overview

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. Texas Administrative Code § 202.21(b), requires all agencies to classify their data and to clearly define the responsibilities of data users, owners and custodians. All CPRIT data, whether electronic or printed, must be classified and managed properly.

## Purpose

The purpose of CPRIT's data classification policy is to provide common definitions, classifications, management of files, and security controls to assist data owners and custodians in providing proper stewardship of agency information. All CPRIT data, whether paper-based or electronic, stored or transmitted must adhere to a data classification standard that evaluates data assets based on value and associated risks so that the appropriate level of protection as required by state and federal law, agency policy and privacy considerations, can be applied.

## Scope

The CPRIT data classification policy applies to all users, owners and custodians of agency information.

## Policy

1. Data Classification Levels

   CPRIT classifies its official agency data into two categories, public information and confidential information. **By default, any data not explicitly classified, is considered to be classified as confidential.**

   Classification Levels (In Order of Least to Most Confidential):

   1. Level 1 – Public Information

      Public information is defined as data that is intended to be shared, without restrictions or is required for public release as described in the Texas Public Information Act. Due to the intent to share, there is no concept of unauthorized disclosure and it can be freely disseminated without potential harm to the agency, individuals, or any agency affiliates. Public information

data controls are generally limited to preventing unauthorized destruction or modification.

Examples of public information include, but are not limited to:

- Employment opportunities/job postings
- Biannual conference schedule
- Press releases

2. Level 2 – Confidential Information

   According to of the Texas Administrative Code Chapter 202, confidential information is "information that is excepted from disclosure requirements under the provisions of applicable state or federal law" such as the Texas Public Information Act (TPIA) and the Family Education Rights and Privacy Act (FERPA). Authorized confidential data disclosure should be limited to individuals with a demonstrable need-to-know or to serve a specific purpose. The unauthorized release or destruction of confidential information could cause irreparable harm to CPRIT or its reputation, or prevent the agency from fulfilling its primary mission.

   Examples of confidential information include, but are not limited to:

   - Access control credentials (e.g. passwords);
   - All grant applications and review documents, including grant application presentations and due diligence reports, if applicable;
   - All grantee programmatic progress reports (does not include HUB, equipment, matching, revenue sharing);
   - Request for Proposals (RFP) and other procurement solicitation responses;
   - Documents marked "confidential" by CPRIT or grant applicant or grantee;
   - Information Technology documents excepted from disclosure under Texas Public Information Act;
   - Human resources employee records;
   - Compliance investigations, including Red flag reports;
   - Attorney advice;
   - Credit card payment information;
   - Access control credentials; and
   - Personally identifiable information excepted from disclosure under Texas Public Information Act.

2. <u>Management of Confidential Data</u>

Confidential data shall be classified and maintained separately from public information. Only those users with authorized access shall handle confidential data. At no point shall a user download a confidential document onto his or her computer. Confidential data shall not be accessed or transmitted using the CPRIT Wireless network (WLAN).

3. Disclosure of Data

   Prior to disclosing, publishing or releasing any information, data owners should classify information according to its need for confidentiality. For non-public data, permission to disseminate must be granted by the Chief Executive Officer and General Counsel prior to release.

   Data classified as confidential should not be published, disclosed or otherwise disseminated to the public or any unauthorized individuals, under any circumstances other than those specifically authorized by law. Any suspected or confirmed disclosures should be immediately reported to CPRIT's General Counsel, Chief Compliance Officer, and Information Security Officer.

**Disciplinary Actions**

Violations of this policy may result in disciplinary actions that include loss of CPRIT access permissions or termination of employment. Additionally, violators may also face civil and criminal prosecution.

**Definitions**

**Authorized User:**

An individual who has been approved to handle confidential data in either printed or electronic format.

**Data Custodian:**

An individual assigned by management who is responsible for implementing physical and technical controls and policies to safeguard data as specified by data owners.

An example of a data custodians are server administrators who maintain applications, operating systems and who perform backups of information technology systems.

**Data Owner:**

An individual assigned by management to oversee the classification of, approve access to, and ensure proper handling of data.

An example of a data owner is a department or specific area manager such as the Chief Operating Officer.

**Data User:**

A data user is any person who has been authorized by a data owner to access or update information.

Users have the responsibility to:

1. Utilize assigned data resources only for purposes specified by the owner
2. Comply with any controls implemented by the owner
3. Prevent the disclosure of information classified as sensitive or confidential

**Data:**

A general term used to describe items such as, but not limited to, electronic and paper files/records and information that are routinely handled, printed, displayed, stored, transmitted or transported

## Appendix A: Document Revision History

| Date | Action | Document Version | Author |
|---|---|---|---|
| 10/24/2016 | Document Created | 1.0.0 | Therry Simien, Information Technology Officer |
| 10/25/2016 | Document Reviewed & Approved | 1.0.0 | Reviewed by Information Technology Governance Committee |
| 2/7/2017 | Document Revised | 1.0.5 | Reviewed by Information Technology Governance Committee |
| 9/8/2017 | Document Revised | 1.5.0 | Reviewed by Information Technology Governance Committee |
| 9/15/17 | Document Reviewed & Approved | 1.5.0 | Reviewed by Information Technology Governance Committee |