Department of Information Resources (DIR)
Policy Version: 1.0
Adopted: July 22, 2014
Next Review: July 22, 2017

# Data Classification and Management Policy

## Purpose

The purpose of the Data Classification and Management Policy is to establish a framework for properly classifying and managing data assets in accordance with Texas Administrative Code, Title 1, Chapter 202 (1 TAC 202). This document sets forth the policy for data classification and management within DIR.

## Scope

This policy applies to all Users of DIR-Owned Data while employed or contracted with DIR. All Users are responsible for understanding and complying with the terms and conditions of this policy. This policy applies to all Users, whether working onsite or offsite, and is not limited to business hours.

## Exemption

Information or data owned or under the control of the United States Government must comply with the federal classification authority and federal protection requirements.

## Policy

1. **Data Management Principles**
   Proper data management must
   - be based on the value and associated risks of managing the data
   - meet the appropriate levels of protection as required by state and federal laws
   - account for ethical, proprietary, and privacy considerations
   - recognize that data classifications are contextual, subject to change and should therefore be periodically reviewed

   All data, regardless of the form or format, which is created or used in support of DIR business activities, is owned by DIR. DIR-Owned Data is an asset and must be protected from its creation, through its useful life, to its timely and authorized disposal. DIR-Owned Data should be maintained in a secure, accurate, and reliable manner and be readily available for authorized use.

   The Information Security Officer (ISO) shall recommend appropriate standards, guidelines, and training regarding Data Management to the Information Resources Manager (IRM) for approval.

2. **Data Security Principles**
   Data security is the protection of data against accidental or malicious disclosure, modification, or destruction. DIR-Owned Data shall be protected based on its classification, i.e., its value, confidentiality, and/or sensitivity to DIR, and the risks of its loss or compromise. At a minimum, DIR-Owned Data is update-protected so that only authorized individuals can modify or erase it.

## 3. Data Classification Principles

DIR-Owned Data is classified based on its sensitivity, legal status, and retention requirements, and according to the type of access required by DIR Users.

DIR-Owned Data is classified as follows:

- **Confidential Data**
  Confidential data shall be protected from unauthorized disclosure or public release based on state or federal law, and other constitutional, statutory, judicial, and legal agreements and requirements.

  Examples of Confidential Data may include but are not limited to
  - Personally Identifiable Information (PII), such as a name in combination with Social Security number (SSN) and/or financial account numbers
  - intellectual property, such as vendor copyrights, patents, and trade secrets
  - passwords used for authenticating individuals
  - network architecture schematics

- **Sensitive Data**
  Sensitive Data may be subject to disclosure under the Texas Public Information Act, but prior to disclosure, will require additional review. Sensitive Data may include Confidential Data that has not yet been classified as such.

  Examples of Sensitive Data may include but are not limited to
  - operational information
  - personnel records
  - information security procedures
  - research
  - internal communications

- **Public Data**
  All other data that is not Confidential Data and is therefore subject to public disclosure pursuant to the Texas Public Information Act.

## 4. Data Classification Life Cycle

The classification of a data item can change over the course of its lifecycle. For example, during the procurement planning, evaluation, and negotiation phases ,most procurement-related documents and communications are considered Confidential Data. The resulting Request for Offers (RFO) are classified as Public Data, while vendor responses to an RFO often have large portions declared as Confidential Data. Once a contract is awarded most, if not all, of the planning, evaluation, and negotiation documents become Public Data. Following contract award, those portions of the vendor responses not declared as Confidential Data are classified as Public Data. Public information requests for confidential portions of vendor responses may need to be submitted to the Office of the Attorney General for a determination as to their confidentiality under Texas law.

## 5. Data Encryption

All electronicly stored or transmitted data classified as Confidential Data or Sensitive Data shall be encrypted while it is either stored or transported on unsecured computing devices, and

during remote transmission, using an approved Cryptographic Algorithm. DIR-approved encryption tools available through IT Services.

All cryptographic Keys (except for Public Asymmetric Keys) as well as the resources used to generate and store Cryptographic Keys shall be considered as Confidential Data. Public Asymmetric Keys may be considered public data.

The minimum recommended encryption key will be Advanced Encryption Standard (AES) 128-bit or stronger as defined by National Institute of Standards and Technology ISO/IEC 18033-3.

Exportation of Cryptographic technologies outside of the United States is restricted by federal regulations.

6. **Approval of Release of DIR-Owned Data**
   Data identified as Confidential Data or Sensitive Data shall not be released outside of DIR without prior approval of the Executive Director.

   Users who create data as part of their authorized duties or receive legitimate data from an outside source shall classify and protect the data in accordance with this policy. Users should consult with DIR legal counsel regarding any questions on the proper classification or disclosure of data. Users are prohibited from improperly receiving or sharing data that is protected under applicable copyright and trademark laws.

7. **Document Retention and Disposal**
   Documents or mediums that contain Confidential Data or Sensitive Data must be disposed or destroyed in a secure manner. Prior to disposal of such data, Users shall consult with DIR legal counsel and the Records Management Officer (RMO) regarding any questions relating to the retention and proper disposal of said data. The RMO shall maintain the record of all discarded and destroyed media as defined in DIR records retention guidelines.

## Compliance

The Executive Director and each member of management are responsible for ensuring User adherence to this policy.

## Disciplinary Action

DIR reserves the right to revoke access at any time for violations of this policy and for conduct that disrupts normal operation of DIR Systems or violates state or federal law.

Users who violate this policy may be subject to disciplinary action, up to and including termination of employment or contract with DIR.

DIR cooperates with appropriate law enforcement if any User may have violated federal or state law.

Instances of failure to adhere to this policy will be brought to the attention of the appropriate manager. The manager may seek consultation/advice from Human Resources and General Counsel.

## Change Management

This policy is subject to change. All changes to this policy shall follow DIR policy. The ISO is responsible for communicating the approved changes to the organization.

## Definitions and Acronyms

### Authentication Protocol

A process by which a secure method of communicating between two entities is employed.

### Confidential Data

Data that is collected and maintained by an agency that must be protected against unauthorized disclosure and is not subject to public disclosure under the provisions of applicable state or federal law, e.g., the Texas Public Information Act (Chapter 552, Texas Government Code).

### Cryptographic Key

A unique piece of data that determines the functional output of a cryptographic algorithm.

### DIR-Owned Data

Any email, document, or information that is created or otherwise altered, either on DIR equipment or personal equipment in support of DIR's business.

### Encryption

The process of converting data into a cipher that prevents unauthorized access.

### Medium

A particular form of storage for digitized information.

### Personally Identifiable Information

Information used solely or in conjunction with other information that can uniquely identify, contact, or locate an individual.

### Personal Health Information

Information that refers to demographic information, medical history, test and laboratory results, insurance information, and other data that is collected by a health care professional to identify an individual and determine appropriate care.

### Sensitive Data

Data that is collected and maintained by an organization that must be protected against unauthorized disclosure, except for public release under the provisions of applicable state or federal law, e.g., the Texas Public Information Act.

### System

An interconnected set of information resources including hardware, software, data, applications, or communications infrastructure, under the same direct management control, that shares common functionality.

### User

Any individual, including, but not limited to, DIR personnel, temporary employees, employees of

independent contractors, vendors, or volunteers, who is authorized to access DIR assets and data for legitimate government purposes. This definition excludes guest network users.

## References

- Computer Fraud and Abuse Act
- Computer Security Act
- Copyright Act of 1976
- Family Education Rights and Privacy Act
- Federal Information Processing Standards (FIPS) Publication 199
- Federal Information Security Management Act (FISMA)
- Gramm-Leach-Bliley Act
- Health Insurance Portability and Accountability Act (HIPAA)
- International Standards Organization 27001:2005
- Payment Card Industry Data Security Standard
- State of Texas Executive Order RP58
- Texas Administration Code (TAC) Title 1, Chapter 202
- Texas Business and Commerce Code, Chapters 48 and 521
- Texas Government Code, Chapters 441, 552, and 2054
- Texas Penal Code, Title 7, Chapter 33 and 33A
- Texas Public Information Act
- Uniform Trade Secrets Act

## Version History

Version 1.0 – July 22, 2014 – Adopted policy.