STATE OF MISSOURI
ADMINISTRATIVE POLICY

POLICY TITLE: Data Classification	AUTHORIZED BY: Tim Robyn **Chief Information Officer**
POLICY : OCS – 001001	PAGES: 3
ISSUED: 02/17/2014	REVISED:
Category: Information Technology Security	**Originating Unit:** OA ITSD Office of Cyber Security

I. General Statements

The State of Missouri collects an enormously wide range of data in thousands of different agency processes. Many of these processes collect sensitive, personal data while others collect data that can be directly consumed by the public. Since state data has varying sensitivity and levels of importance, data classification indicates the appropriate levels of confidentiality, integrity, and availability that should be applied to the data. Data classification assists with the effective allocation of agency and ITSD resources and ensures the proper implementation of security controls from the time the data is collected or generated to the time the data is destroyed.

II. Purpose

Data classification is the process where data is appropriately categorized based on its sensitivity and importance to an agency process. By appropriately categorizing data, agency management (data owner) and the custodian (ITSD) can apply the appropriate safeguards to ensure the confidentiality, integrity, and availability of the data throughout its lifecycle.

III. Scope

All agency processes with their corresponding data stores are within the scope of data classification. If an agency determines that a process and its corresponding data does not need to go through the classification process, it shall be categorized as unclassified.

IV. Responsibilities

Data Owner: The data owner is an agency representative that has ownership and authority over a specific business process. The data owner is ultimately responsible for ensuring the protection of the data that is used by their covered business process. The data owner chooses the proper classification level for their data. The data owner is also responsible for ensuring that all necessary security controls are in place, defining the appropriate security and backup requirements per classification, approving any data transfer transactions, data access management auditing, and user management criteria.

Data Custodian: The data custodian is responsible for maintaining and protecting the data provided by the data owner. Information Technology Services Division (ITSD) and other information systems vendors are the data custodians of state data. The duties of the data custodian include the implementation and maintenance of security controls, performing regular backups of the data, restoring data from backups, retaining records of activity, and fulfilling all of the requirements provided by the data owner. In regards to data classification, the data custodian is responsible for implementing the necessary controls and processes at the various classification levels. The data custodian does not classify data as this responsibility is handled by the data owner.

V. Data Classification Levels

State data can be classified by using three different levels of sensitivity: restricted (high), private (medium), and public (low). The controls and the cost to maintain the data classification vary greatly between the different levels. Each classification has separate handling requirements and procedures in regards to data access, use, and destruction. If data has not been classified using one of the defined levels, the data is considered unclassified.

Restricted Classification Level

The restricted classification level is reserved for data that is protected by law or by industry standards. Laws at the state and federal level protect tax data, healthcare data, education data, social security data, and other categories. Standards such as the Payment Card Industry - Data Security Standard (PCI-DSS) protect credit card payment processes and their corresponding data. Restricted data at rest and in motion will utilize NIST approved encryption algorithms unless otherwise specified by the data owner. Data retention and backup requirements will be tailored to the needs of the data owner. The data custodian understands that by not following the data owner's requirements certain laws may be broken, but it is up to the data owner to ensure that the data custodian understands the laws pertaining to the data and the punishment for not abiding by the laws.

Examples of Restricted Data
- Data provided by the Social Security Administration (SSA)
- Data provided by the IRS - Federal Tax Information (FTI)
- Personal health information (PHI)
- Student records
- Criminal background checks
- Personally identifiable information that is defined by 407.1500, RSMo

Private Classification Level

The private classification level is reserved for data that is not protected by law or industry but is deemed sensitive because it is personally identifiable, a matter of public safety, or for other reasons defined by the agency. Any data collected from citizens that falls outside of the restricted classification level would fit within the private classification level. Private data at rest and in motion will utilize NIST approved encryption algorithms unless otherwise specified by the data owner. Data retention and backup requirements will be tailored to the needs of the data owner.

Examples of Private Data
- Citizen data collected by the state that falls outside of the restricted level
- Citizen data provided by business partners
- Data regarding critical infrastructure
- Employee data that falls outside of public records (health, withholdings, PII)

Public Classification Level

The public classification level is for data that does not fit within the restricted or private classification levels. Data within this level does not contain personally identifiable information nor does its release into the public increase the risk of a public safety event. Data falling within this category should be considered immediately sunshinable without any redaction. Public data does not require encryption at rest or in motion. Data retention and backup requirements will be tailored to the needs of the data owner.

Examples of Public Data
- Summarized statistics
- Employee salary information
- State expenditures
- State meetings and events at state office buildings
- Licensing and registration information for businesses and professionals (without PII)

VI. Compliance

Data classification compliance ultimately rests with the data owner in ensuring the data is appropriately classified and that the data custodian is properly managing the data and applying due care.

This document and subsequent procedures shall be in alignment with NIST 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories.