# Office of Technology Services
# Policy

## Data Classification

---

## Policy:
All data owned, maintained, or held in trust by state agencies shall be classified according to the level of sensitivity and criticality of the data as prescribed in the guidelines of this policy. Each state agency shall develop and maintain a data classification policy that meets or exceeds the data sensitivity and criticality levels described in this policy.

## Scope:
All agencies and entities under the authority of the Office of Technology Services pursuant to the provisions of R.S. 39:15.1 et seq., shall comply with this policy.

## Requirements:
Data Sensitivity Levels:
Data shall be classified into the following four sensitivity levels:

UNRESTRICTED
This type of information is actively made public by state agencies and is published and distributed without restriction. Release of this data has no measurable adverse impact on individuals, an agency, or the state.

Examples of UNRESTRICTED data include but is not limited to:
- Approved press statements
- Agency public websites
- Published materials

INTERNAL
The unauthorized disclosure of information would be expected to have a **limited** adverse effect on individuals, an agency, or the state. Any data not classified as RESTRICTED, CONFIDENTIAL, or UNRESTRICTED shall be classified as internal data.

Examples of INTERNAL data include but is not limited to:
- Internal memos not containing CONFIDENTIAL or RESTRICTED data
- Meeting minutes not containing CONFIDENTIAL or RESTRICTED data
- Agency contact information

CONFIDENTIAL (SENSITIVE)
The unauthorized disclosure of information would be expected to have a **serious** adverse effect on individuals, an agency, or the state.

# Office of Technology Services
# Policy

Examples of SENSITIVE data include but is not limited to:

- Usernames and password to resources not containing RESTRICTED Data
- Employee Performance Review
- Client/Attorney Communications
- Source Code
- Audit or Risk assessment reports

RESTRICTED
The unauthorized disclosure of information would be expected to have a **severe** or **catastrophic** adverse effect on individuals, an agency, or the state. Restricted data requires strict adherence to legal obligations such as federal, state, or local law, specific contractual agreements, or data specifically designated as RESTRICTED data in applicable state policy.

Examples of RESTRICTED data include but is not limited to:

- Protected Health Information (PHI)
- Federal Tax Information (FTI)
- Payment Card Information (PCI)
- Criminal Justice Information (CJI)
- Personal Information

Data Criticality Levels:
Data shall be classified into the following three criticality levels:

Level A: Low Critical
The unauthorized modification, destruction, or unavailability of information would be expected to have a **limited** adverse effect on individuals, an agency, or the state.

Level B: Moderate Critical
The unauthorized modification, destruction, or unavailability of information would be expected to have a **serious** adverse effect on individuals, an agency, or the state.

Level C: High Critical
The unauthorized modification, destruction, or unavailability of information would be expected to have a **severe** or **catastrophic** adverse effect on individuals, an agency, or the state.

## Definitions:

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data element is not encrypted or redacted:

- Social security number
- Driver's license number

# Office of Technology Services
# Policy

- Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account

"Personal information" shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

## Responsibilities:

Each State Agency is responsible for the following:

- Establishing policies and procedures to ensure compliance with this policy.
- The data owner or appropriate delegate shall determine the appropriate classification level of data and shall review as necessary to determine if reclassification is necessary.
- The data custodian is responsible for implementing and maintaining the requirements for the data classified by the data owner.

## Exceptions:

Request for exceptions to this policy shall be justified, documented, and submitted in writing to the Chief Security Officer. Exceptions to this policy require written approval granted by the State Chief Information Officer.

## Related Polices, Standards, Guidelines:

IT POL 1-04 Data Sanitization
IT POL 1-08 Authentication
IT POL 1-10 Authorized Access
IT POL 1-22 Data in Transit
IT STD 1-13 Encryption
IT STD 1-17 Data Sanitization

## References:

National Institute of Standards and Technology: FIPS PUB 199
RS 51:3071 et. seq. (Database Security Breach Notification Law)

**Owner:** OTS

**Review Cycle:** As needed.

**Effective Date for this Provisional Policy:** October 21, 2014