Data Categorization

Standard ID
IOT-CS-SEC-102

Published Date
9/27/2006

Effective Date
9/27/2006

Last Updated
5/19/2017

Next Review Date
5/19/2018

Policy
08.0 Data Security (PR.DS)
  08.4 PR.DS-4
    08.4.1 Asset Availability
  08.5 PR.DS-5
    08.5.1 Asset Confidentiality
  08.6 PR.DS-6
    08.6.1 Asset Integrity

Purpose
Owners of information systems must appropriately categorize data to assure expected outcomes. Data categorization consists of two aspects, availability and confidentiality. Categorization ultimately drives system design incorporating appropriate redundancy of key components and needed levels of security.

Scope
IOT Supported Entities

Statement
Data shall be classified according to the definitions listed below:

Availability
There are three Availability categories:
  Critical – Systems will be recovered in 6 business hours or less. This service level requires that the agency replicate data at the DR facility have the necessary processing capabilities (servers), complete DR Testing, and agency sign off the DR documentation with their system recovery procedures to meet their performance objectives in a disaster situation.
  Necessary – Systems are restored in 21 days or less. Recovery of this class of system uses a backup system to disk and then restores to Virtual Servers. This service level doesn’t offer any DR Testing.
  Non-critical – systems with no firm expectation set regarding duration restored on a best efforts basis.

Confidentiality
There are four Confidentiality categories:
  Confidential – systems holding the most sensitive information intended strictly for use within the State or State agency. This information is exempt from disclosure under the provisions of the Freedom of Information Act, HIPAA, or other applicable federal laws or regulations. Its unauthorized disclosure could seriously and adversely impact the State, the
State agency, its business partners, its customers, or individual persons. Examples of confidential information include: Health care, law enforcement, and taxpayer personal and financial information.

*Sensitive* – systems holding information requiring special precautions to assure the integrity of the information and protection from unauthorized modification or deletion. It is information that requires a higher than normal assurance of accuracy and completeness. Examples of sensitive information include financial transactions and regulatory actions.

*Private* – systems holding personal information intended for use within the State or State agency. Its unauthorized disclosure could seriously and adversely impact the State or State agency and/or its employees.

*Public* – systems holding other information not clearly fitting into any of the above three classifications. Disclosure, in some cases may be limited by policy, but disclosure does not negatively impact the State or State agency, its employees, and/or its customers. Public information falls in one of two areas:

1. Public-Controlled: Information is Public but accuracy must be maintained and access must be controlled by specific procedures. Example: BMV driver’s records.
2. Public-Published: Accuracy is not critical and the information is freely published or posted. Example: Agency telephone listings.

Below are Availability and Confidentiality Decision Trees:
Availability Decision Tree

The following questions are designed to assist in determining the minimum Availability category for the data you maintain. You may assign a higher level to the data at your discretion. Please note that the integrity of the data must be maintained regardless of the category assigned.

1) Does the data need to be available 24/7/365 with no interruption of service and no acceptable data loss? Less than 6 hours of unavailability can be tolerated in a crisis situation. This type of information calls for redundancy and immediate failover. Examples would include critical medical information in a hospital, criminal information required by law enforcement, or data that without access would cause financial loss or legal issues.

   - YES
     - STOP
     - Categorization: CRITICAL
   - NO
     - Continue

2) Does the data need to be available the majority of the time but some interruption is acceptable? Up to 7 days of unavailability can be tolerated in a crisis situation. Some data loss is acceptable as it can be reconstructed from source information. Examples would include most regular business transactions, especially non-financial transactions.

   - YES
     - STOP
     - Categorization: NECESSARY
   - NO
     - Continue
     - Categorization: NON-CRITICAL
Confidentiality of Data Decision Tree

The following questions are designed to assist in determining the minimum Confidentiality category for the data you maintain. You may assign a higher level to the data at your discretion. **Please note that the integrity of the data must be maintained regardless of the category assigned.** Aggregates of data should be classified as to the most secure classification level (e.g. when data of mixed classification exist in the same database, file, report, etc., the classification of that database, file, or report should be that of the highest level of classification).

1) **Would the loss or unauthorized disclosure of the data be a violation of federal or state laws/regulations/rules or contractual agreements or result in any business, financial or legal loss?**

   - [ ] YES
   - [ ] NO

   **Stop**

   **Category: Confidential**

2) **Would the loss or unauthorized disclosure of the data cause issues of personal credibility, reputation or other issues of personal privacy?**

   - [ ] YES
   - [ ] NO

   **Stop**

   **Category: Sensitive**

3) **Is data intended for internal use only?**

   - [ ] YES
   - [ ] NO

   **Stop**

   **Category: Private**

   **Continue**

   **Category: Public**

**Roles**
Information Asset Owners/System Owners

**Responsibilities**
System owner shall confirm data is categorized appropriately and the Information Systems Inventory (ISI) is current and complete.
Management Commitment
Management shall confirm system owners are appropriately classifying data in accordance with this standard.

Coordination Among Organizational Entities
Agency shall coordinate internally and with vendors in regards to data categorization and who can access certain data types.

Compliance
Availability Data Categorization will be used by the agencies to prioritize their systems/applications part of their Continuity of Operation Plan (COOP) with Indiana Department of Homeland Security (IDHS) and also work with Indiana Office of Technology (IOT) on Disaster Recovery Plan (DRP) for those prioritized systems/applications. A failure to maintain the information can risk agency’s systems being included in disaster recovery planning.

Exceptions
No exceptions.