



# DEPARTMENT OF ADMINISTRATION

## Enterprise Policy

DOIT-05-02-2006

### DIVISION OF INFORMATION TECHNOLOGY

#### Data Categorization

Date of Last Revision 09/29/2006

**Bijay Kumar**  
(401) 574-9220  
bijay.kumar@doit.ri.gov

#### 1. Purpose

- a. All state data shall be categorized based on the need for availability and level of confidentiality.

#### 2. Objectives

- a. Establish the appropriate requirements for security and management of data.

#### 3. Scope

- a. This policy applies to all state agencies that fall under the Executive Branch of Rhode Island state government.

#### 4. History

- a. This policy shall supersede all previous "State" Data Categorization Policies and shall be effective for all state employees, contractors, subcontractors, casual and seasonal employees, and ALL USERS.

#### 5. References

- a. HIPAA 164.308 Administrative Safeguards:
  - (a) (7) (i) Contingency plan.
  - (ii) implementation specifications:
    - (E) Applications and data criticality analysis

#### 6. Definitions

- a. State data is categorized based on three (3) levels of **AVAILABILITY** and four (4) levels of **CONFIDENTIALITY**.

- b. The **CONFIDENTIALITY** levels are defined as follows:

- (i.) **Confidential** - Data with the highest level of security and protection. The unauthorized loss or disclosure of this information could pose a risk to the State or individual that it references.

These data elements are the most sensitive to integrity and confidentiality risks. Access is tightly restricted with the most stringent security safeguards at the system as well as the user level. Failure to maintain the integrity and confidentiality could have severe financial, health or safety repercussions. Very strict rules must be adhered to in the usage of this data.

Examples of this data include the contents of state law investigative records and communications systems.

**(ii.) Sensitive** - Data that requires special precautions to ensure the integrity and protection from unauthorized modification or deletion

These data elements include those protected by federal and state statute or regulation. Access to these data elements is restricted to authenticated and authorized individuals who require access to that information in the course of performing their duties. These are the data elements removed from responses to information request for reasons of privacy.

Security threats to this data include violation of privacy statutes and regulations in addition to unauthorized alteration or destruction. If this data were accessed by unauthorized persons, it could cause financial loss or allow identity theft. Unauthorized disclosure could provide significant gain to a vendor's competitors.

Examples:

1. Social security numbers
2. Attorney files
3. Food Assistance programs data
4. Credit card numbers
5. Health and Medical data (protected through HIPAA)
6. Educational records (protected by FERPA)

**(iii.) Private** - Data that is not for public use, control, or participation. This information can be thought of as belonging to an individual rather than the general public

This category of data includes the majority of the data contained with the state government electronic databases. Direct access to this data is restricted to authenticated and authorized individuals who require access to that information in the course of performing their duties.

Security threats to this data include unauthorized access, alteration and destruction concerns.

Examples:

1. Most data elements in state personnel records
2. Driver history records
3. Occupational licensing data

**(iv.) Public** - Data with the lowest level of security and protection. This information can be generally viewed by anyone with minimum controls to ensure integrity.

The greatest threat to this data is from unauthorized or unintentional alteration, distortion or destruction of this data. Security efforts appropriate to the criticality of the system containing this data must be taken to maintain its integrity.

Examples of data at this level include many agency public websites.

c. The **AVAILABILITY** levels are defined as follows:

- (i.) **Critical** - Data needs to be available seven days / week and 24 hours/ day. Any loss of access is critical. This data is critical to public health or safety and must be protected by a vital plan that would allow resumption of operations within a very short timeframe.
- (ii.) **Necessary** - Data can be down or not available for up to one (1) week. This data is required in order to administer functions within state government that need to be performed. Business continuity planning allows state government to continue operations in these areas within a certain period of time until the data can be restored.
- (iii.) **Non-Critical** - Data can be down or not available for longer than one (1) week. This data does not play any role in the scheme of the health, security, or safety of Rhode Island citizens.

**7. Policy and Control Requirements**

a. **Compliant Activities:**

- (i.) Data owners shall categorize all data under their control according to the following Categorization Matrix:

		<b>Confidentiality</b>			
		<b>Confidential</b>	<b>Sensitive</b>	<b>Private</b>	<b>Public</b>
<b>Availability</b>	<b>Critical</b> - Data needs to be available seven days/week and 24 hours/day. Any loss of access is critical.	Data with the highest level of security and protection. The unauthorized loss or disclosure of this information could pose a risk to the State or individual that it references.	Data that requires special precautions to ensure the integrity and protection from unauthorized modification or deletion.	Data that is not for public use, control, or participation. This information can be thought of as belonging to an individual rather than the general public.	Data with the lowest level of security and protection. This information can be generally viewed by anyone with minimum controls to ensure integrity.
	<b>Necessary</b> - Data can be down or not available for up to one (1) week.				
	<b>Non-critical</b> - Data can be down or not available for longer than one (1) week.				

**8. Exceptions to Policy**

- a. Exceptions to this policy may be granted solely by the Chief Information Security Officer (CISO) or the CISO's designee.

**9. Policy Violations and Disciplinary Actions**



- a. A State employee found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

**10. Implementation Responsibility**

- a. Data owners shall categorize their data according to the above Categorization Matrix. These categorizations shall be reviewed on a regular basis and updated as necessary.
- b. The Division of Information Technology (DoIT) is responsible for establishing data categorization standards and procedures.
- c. DOIT and agency members are responsible for implementing security procedures to protect data based on the data's categorization.
- d. State Agencies shall coordinate with the DOIT to provide security

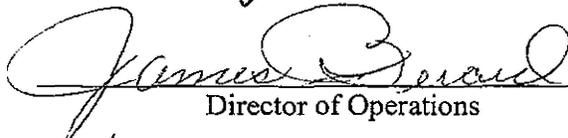
**11. Compliance Responsibility**

- a. The DOIT and the State Agencies shall be responsible for implementing and enforcing this policy within their supported areas

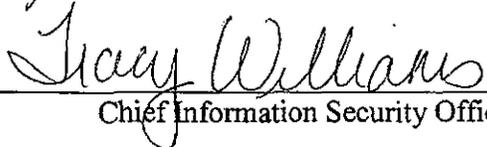
**12. Signatures**

  
Assistant Director of Planning, Policy & Technology

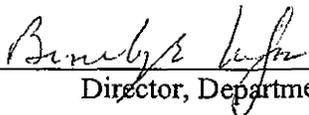
1/9/07  
Date

  
Director of Operations

1/9/07  
Date

  
Chief Information Security Officer

1/22/07  
Date

  
Director, Department of Administration

2/2/07  
Date