# Idaho Technology Authority (ITA)

# ENTERPRISE POLICY – P4000 SECURITY-GENERAL

**Category: P4130 – INFORMATION SYSTEMS CLASSIFICATION POLICY**

**CONTENTS:**



## I. AUTHORITY

Authority: Idaho Code § 67-5745(C)(3)

## II. ABSTRACT


This policy establishes information systems classification categories for State of Idaho agencies. A common security classification framework and associated terminology promotes the effective management of information and information systems to minimize the risk of unauthorized releases of sensitive information.

By classifying information systems, information owners can utilize a common set of security controls to protect information assets based on its level of sensitivity and value. Additional classification guidance can be referenced in the Data Classification and Labeling Guidelines (ITA Guideline G505).

This policy does not circumvent an agency's responsibility to follow internal public records request policies and processes. Information classification under this policy is not sufficient for an agency's determination of exemption from the Public Records Act. [Idaho Code § 74-103(15) (2015)]


## III. DEFINITIONS

**Information Custodian** - A person having personal custody and control of the information or information system in question. If no such designation is made by the public agency or independent public body corporate and politic, then custodian means any public official having custody of, control of, or authorized access to information and

information assets and includes all delegates of such officials, employees or representatives. [Idaho Code § 74-101(3) (2015)].

**Information Owner –** A person responsible for determining who should have access to information they own, and what those access privileges should be. Responsibility for implementing security measures may be delegated, though accountability remains with the identified owner of the data.

**Information System –** A discrete set of information resources organized for the collection, processing, maintenance, use sharing, dissemination, or disposition of information.

**Sensitivity:** A measure of the importance assigned to the information by its owner for the purpose of denoting the need for protection.

## IV. POLICY

Agencies shall use this policy as a framework to classify information and information systems to support assignment of appropriate security controls to mitigate risks of unauthorized disclosures and to ensure proper information handling by information users and information custodians.

### I. Responsibilities

#### a. Information Custodian

Ensure that information and information systems under their control are protected with corresponding security controls supporting the information owner's security classification levels.

#### b. Information Owner

All State information and information systems must have an owner. The information owner must:

- Validate decisions regarding the assignment of security controls, access privileges of users, and participate in ongoing decisions regarding information management,
- Execute formal information sharing agreements with other agencies prior to exchanging information that is protected by privacy, confidentiality, or other protective constraints,
- Perform periodic classification level reviews based upon changes in the sensitivity, value, and impact (low, medium or high) to the agency according to the Federal Information Processing Standards 199 (FIPS) model. FIPS199 defines impact levels representing the data breach worst case scenario for an agency.
- Classify information systems based on the "high water mark" (highest impact level) of the systems associated information.

When the designated information owner is no longer responsible due to departure, transfer or reassignment, the agency will appoint a new information owner to mitigate lapses in accountability and responsibility for information assets.

**c. Agencies**

In order to implement the requirements specified within this policy, agencies shall:

- Establish policies and procedures for managing the assignment of classification levels within the agency.
- Ensure that information belonging to different classification levels be logically separated or protected at the highest impact level of the systems associated information.
- If using another agency's information or information assets, observe and maintain the appropriate security for the classification levels assigned by other agency's information owner.
- Provide training to information owners and information handlers on this policy and handling procedures associated with all information classification levels.
- Ensure that all information and information assets are disposed of in a manner consistent with the classification level and comply with established State of Idaho policies, statutes, rules and regulations for disposal.

## II. Classification Levels

The Classification schema included in this policy differentiates between levels of sensitivity, value and impact.

a. **Classification Level 1:** "Unrestricted" includes, but is not limited to, any information relating to the conduct or administration of the public's business prepared, owned, used or retained by any state agency, independent public body corporate and politic or local agency regardless of physical form or characteristics. The agency's worst case scenario for a breach of confidentiality, integrity, and availability is considered low impact (FIPS-199).

**Examples:** Press releases, brochures, pamphlets, public access web pages, and materials created for public consumption.

**Classification Level 2:** "Limited" includes sensitive information that may or may not be protected from public disclosure but if made easily and readily available may jeopardize the privacy or security of agency employees or individuals. The agency's worst case scenario for a breach of confidentiality, integrity, or accessibility is considered medium impact (FIPS-199).

**Examples:** Enterprise risk management planning documents, published internal audit reports, detailed financial transactions, email, non-public phone numbers, or building schematics, names and addresses that are not protected from disclosure.

b. **Classification Level 3:** "Restricted' includes sensitive information intended for agency use that may be exempted from public use and disclosure. Unauthorized disclosure may jeopardize the privacy or security of agency employees, organizations, or individuals. Direct access is limited to internal parties authorized in the performance of their duties. External agencies requesting this information for authorized agency business must be under contractual obligation of confidentially or confidentiality with the disclosing agency (for example, confidentiality/non-disclosure agreement) prior to receiving the information. The agency's worst case scenario for a breach of confidentiality, integrity, or accessibility is considered high impact (FIPS-199).

   **Examples:** Network diagrams, information systems and telecommunications systems configuration information, security plans, administrator level passwords, personally identifiable information, bank account numbers, child welfare and legal information about minors, student education records, social security numbers, other information exempt from public disclosure.

   **Classification Level 4: "Critical"** includes extremely sensitive information. Information disclosure could potentially cause major damage or injury up to and including death to the named individual, or agency employees. The agency's worst case scenario for a breach of confidentiality, integrity, or accessibility is considered high impact (FIPS-199).

   **Examples:** Disclosure that could result in loss of life, disability or serious injury or regulated information with significant penalties for unauthorized disclosure. Included is information that is typically exempt from public disclosure.

## V. EXEMPTION PROCESS

Refer to ITA Policy P1010 (Information Technology Policies, Standards, and Guidelines Framework).

## VI. PROCEDURE REFERENCE

- Federal Information Processing Standards (FIPS-199)
- Idaho Code §§ 74-101 through 74-126
- ITA Policy P1030 (Electronic Document Management)
- ITA Guideline G505 Data Classification and Labeling Guideline

## VII. CONTACT DATA

For more data, contact the ITA Staff at (208) 332-1876 or security@cio.idaho.gov.

## REVISION HISTORY

Effective Date: April 26, 2016