Idaho Technology Authority (ITA)

ENTERPRISE GUIDELINES – G500 SECURITY PROCEDURES

Category: G505 Data Classification and Labeling Guidelines

CONTENTS:

I. Rationale
II. Guideline
III. Procedure Reference
IV. Contact Information
Revision History

I. RATIONALE

The intention of the State of Idaho's public records law Idaho Code § 74-102 is to make all records maintained by state agencies and political subdivisions available for public access. This policy of openness should be balanced against the need for privacy of its citizens.

II. GUIDELINE

Each agency shall establish policies, procedures, and practices for managing information assets. The policies, procedures, and practices should:

- Establish processes for identifying agency information assets and the assignment of classification levels to all data;
- Establish procedures in support of decision-making regarding controls, access privileges of users, and ongoing information management;
- Ensure the information is reviewed for value and updated to manage changes to risks associated with emerging threats, vulnerabilities or changes in the environment.
- Establish practices for periodic reclassification based on privacy impact analysis, changing agency priorities or new statutes, regulations and security standards; and
- Enforce state archive document retention rules regarding proper disposition of all information assets.

Classification Level Labeling

Information should be properly labeled so that users are aware of the classification. Effective labeling ensures that the user is aware of the classification level and associated handling requirements. Labeling should effectively notify the user of the data classification and can be at the document, file, and screen, application depending on how the information is accessed or processed.

Data Handling

Users handling data have the responsibility to ensure that it is protected from unauthorized or accidental disclosure, modification or loss. Data confidentiality, integrity, and availability while processing, storing, and transmission of data over state information assets are protected in accordance with its classification.

Agencies utilizing another agency's information should handle the data in according to the data owner's classification.

For low-impact information systems (FIPS PUB 199), agencies should, at a minimum, employ appropriately tailored security controls from the low baseline of security controls (See Table 1.) defined in NIST Special Publication 800-53 Rev. 4 and should ensure that the minimum assurance requirements associated with the low baseline are satisfied.

ID	CONTROLS	ID	CONTROLS
AC	AC-1	MP	MP-1
AT	AT-1, AT-2, AT-3, AT-4	PE	PE-1, PE-6, PE-8
AU	AU-1, AU-6	PL	PL-1, PL-2, PL-4
CA	CA-1, CA-2, CA-3, CA-5, CA-6, CA-7, CA-9	PS	PS-1, PS-6, PS-7
CM	CM-1, CM-2, CM-4, CM-8	RA	RA-1, RA-3, RA-5
CP	CP-1, CP-3, CP-4	SA	SA-1, SA-2, SA-3, SA-4, SA-4(10), SA-5, SA-9
IA	IA-1	SC	SC-1, SC-39
IR	IR-1, IR-2, IR-5	SI	SI-1, SI-4, SI-5
MA	MA-1		

Table 1. Low-impact tailored security controls.

For moderate-impact information systems (FIPS PUB 199), agencies should, at a minimum, employ appropriately tailored security controls (see Table 2) from the moderate baseline of security controls defined in NIST Special Publication 800-53 Rev. 4 and should ensure that the minimum assurance requirements associated with the moderate baseline are satisfied.

ID	CONTROLS	ID	CONTROLS
AC	AC-1	MP	MP-1
AT	AT-1, AT-2, **AT-2(2)**, AT-3, AT-4	PE	PE-1, PE-6, **PE-6(1)**, PE-8
AU	AU-1, AU-6, **AU-6(1)**, **AU-6(3)**, **AU-7**, **AU-7(1)**	PL	PL-1, PL-2, **PL-2(3)**, PL-4, **PL-4(1)**, **PL-8**
CA	CA-1, CA-2, **CA-2(1)**, CA-3, CA-5, CA-6, CA-7, **CA-7(1)**, CA-9	PS	PS-1, PS-6, PS-7
CM	CM-1, CM-2, **CM-2(1)**, **CM-2(3)**, **CM-2(7)**, **CM-3**, **CM-3(2)**, CM-4, CM-8, **CM-8(1)**, **CM-8(3)**, **CM-8(5)**	RA	RA-1, RA-3, RA-5, **RA-5(1)**, **RA-5(2)**, **RA-5(5)**
CP	CP-1, CP-3, CP-4, **CP-4(1)**	SA	SA-1, SA-2, SA-3, SA-4, **SA-4(1)**, **SA-4(2)**, **SA-4(9)**, SA-4(10), SA-5, **SA-8**, SA-9, **SA-9(2)**, **SA-10**, **SA-11**
IA	IA-1	SC	SC-1, **SC-2**, SC-39
IR	IR-1, IR-2, **IR-3**, **IR-3(2)**, IR-5	SI	SI-1, SI-4, **SI-4(2)**, **SI-4(4)**, **SI-4(5)**, SI-5, **SI-7**, **SI-7(1)**, **SI-7(7)**, **SI-10**, **SI-16**
MA	MA-1		

Table 2. Moderate-impact tailored security controls.

For high-impact information systems (FIPS PUB 199), Agencies should, at a minimum, employ appropriately tailored security controls (see Table 3.) from the high baseline of security controls defined in NIST Special Publication 800-53 Rev. 4 and should ensure that the minimum assurance requirements associated with the high baseline are satisfied.

ID	CONTROLS	ID	CONTROLS
AC	AC-1	MP	MP-1
AT	AT-1, AT-2, AT-2(2), AT-3, AT-4	PE	PE-1, PE-6, PE-6(1), **PE-6(4)**, PE-8
AU	AU-1, AU-6, AU-6(1), AU-6(3), **AU-6(5)**, **AU-6(6)**, AU-7, AU-7(1), **AU-10**	PL	PL-1, PL-2, PL-2(3), PL-4, PL-4(1), PL-8
CA	CA-1, CA-2, CA-2(1), **CA-2(2)**, CA-3, CA-5, CA-6, CA-7, CA-7(1), **CA-8**, CA-9	PS	PS-1, PS-6, PS-7
CM	CM-1, CM-2, CM-2(1), **CM-2(2)**, CM-2(3), CM-2(7), CM-3, **CM-3(1)**, CM-3(2), CM-4, **CM-4(1)**, CM-8, CM-8(1), **CM-8(2)**, CM-8(3), **CM-8(4)**, CM-8(5)	RA	RA-1, RA-3, RA-5, RA-5(1), RA-5(2), **RA-5(4)**, RA-5(5)
CP	CP-1, CP-3, **CP-3(1)**, CP-4, CP-4(1), **CP-4(2)**	SA	SA-1, SA-2, SA-3, SA-4, SA-4(1), SA-4(2), SA-4(9), SA-4(10), SA-5, SA-8, SA-9, SA-9(2), SA-10, SA-11, **SA-12**, **SA-15**, **SA-16**, **SA-17**
IA	IA-1	SC	SC-1, SC-2, **SC-3**, **SC-7(18)**, **SC-7(21)**, **SC-24**, SC-39
IR	IR-1, IR-2, **IR-2(1)**, **IR-2(2)**, IR-3, IR-3(2), IR-5, **IR-5(1)**	SI	SI-1, SI-4, SI-4(2), SI-4(4), SI-4(5), SI-5, **SI-5(1)**, **SI-6**, SI-7, SI-7(1), **SI-7(2)**, **SI-7(5)**, SI-7(7), **SI-7(14)**, SI-10, SI-16
MA	MA-1		

Table 3. High-impact tailored security controls.

Agencies should employ all security controls in the respective security impact level.

Data Isolation

Information of different classification levels should be logically or physically segregated by classification level.

Disposal

Information regardless of medium should be disposed of in a manner consistent with the classification level and in accordance with NIST SP 800-88 Rev.1.

III. PROCEDURE REFERENCE

- ITA Policy P4130 (Data Classification)
- Idaho Code §§ 74-101 through 74-126
- FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems
- NIST Special Publication 800-53 Rev. 4.
- NIST SP 800-88 Rev. 1 Guidelines for Media Sanitization

IV. CONTACT INFORMATION

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

REVISION HISTORY

Established: February 16, 2016