Idaho Technology Authority (ITA)

ENTERPRISE POLICY 4500 SECURITY –COMPUTER AND OPERATIONS MANAGEMENT

Category: P4560 DATA BREACH MANAGEMENT

CONTENTS:

I. AUTHORITY

Authority: Idaho Code § 67-5745(C)(3); Idaho Code § 28-51-106(1)

II. ABSTRACT

Each State agency must implement, maintain, and enforce reasonable procedures to protect the confidentiality, integrity, and availability of sensitive information. Appropriate protection is critical since unauthorized access to personal information is likely to result in substantial harm or inconvenience to an individual to whom the information relates.

III. DEFINITIONS

Data Breach - For the purposes of this policy, a data breach is a “breach of the security of the system” as defined in Idaho Code section 28-51-104 or an unauthorized disclosure of personally identifiable information as defined in a law governing an agency.

*Personally Identifiable Information (PII)***:** PII is:

> “Personal information” as defined in Idaho Code section 28-51-104;
>
> Information about an individual exempt from disclosure in a public record pursuant to the Idaho Public Records Act, Idaho Code title 74, chapter 1; and,

Information about an individual defined as confidential, private, or a similar designation in the laws governing an agency.

Personal information may include any of the following information related to a person:

1. Date of birth
2. Social Security number
3. Driver's license number
4. Financial services account numbers, including checking and savings accounts
5. Credit or debit card numbers
6. Personal identification numbers (PIN)
7. Electronic identification codes
8. Automated or electronic signatures
9. Biometric data
10. Passwords
11. Parents' legal surname prior to marriage
12. Home address or phone number
13. Any other numbers or information that can be used to access a person's financial or health resources, obtain identification, act as identification, or obtain goods or services.

Per Idaho Code § 28-51-104, "The term 'personal information' does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media."

IV. POLICY

This policy applies to all State personnel, contractors, and third-party vendors that have access to State information systems and the sensitive data contained herein. The policy is designed to protect data relating to citizens and to prescribe circumstances when notification of data security breaches is required.

Unless overridden by statutory or regulatory obligations, the following requirements apply when there has been a data breach.

An agency at its discretion may implement a policy that is more restrictive than this policy. *Agency responsibilities:*

1. Notify affected individuals shall be made expediently and without unreasonable delay following the discovery of a data breach if the agency believes that the information has or will be misused.
2. Notifications to the Idaho Attorney General's Office shall not be later than 24 hours after discovery of a breach regardless of the determination of misuse.

3. Notification to the Office of the Chief Information Officer (OCIO) (security@cio.idaho.gov) shall not be later than 24 hours after discovery of a breach regardless of the determination of misuse.
4. Notifications may be delayed when a law enforcement agency determines that notification would impede a criminal investigation. In such as case, notice must be made as soon as possible after a law enforcement agency advises the notification will no longer impede the investigation.
5. Notification may be provided by one or more of the following methods:
   - In accordance with the agency's policies or the rules, regulations, procedures, or guidelines (ITA Guideline G580 [Cyber Security Breach Notification]); or
   - Pursuant to the rules, regulations, procedures, or guidelines established by the agency's primary or functional federal regulator.
6. Notification is NOT required:
   - When the breached data is in a form that is unusable, unreadable, or indecipherable to unauthorized individuals; meaning data that is either encrypted or destroyed in accordance with State policies and standards.
   - If, after an appropriate investigation or after consultation with relevant federal, state, and local agencies responsible for law enforcement, the agency determines that the misuse of the personal information has not occurred and is not reasonably likely to occur.

V. EXEMPTION PROCESS

Some State agencies may have special conditions or extraordinary requirements that prevent compliance with an ITA standard or policy. Agencies may request an exemption from an approved policy by submitting a completed Exemption Request Form, according to the guidelines, for consideration by the ITA. Agencies may request an exemption from an approved standard by submitting a completed Exemption Request Form, according to the guidelines, for consideration by the ITLC (Information Technology Leadership Council) (a subcommittee of ITA). The justification must include measurable business reasons that show a different option is in the best interest of the agency and the State of Idaho.

Situations that may lead to exemptions include:

1. Federal restrictions and requirements;
2. Legislative or regulatory mandates that require exceptional measures;
3. Compliance with the standard would adversely affect the ability of the agency to accomplish mission critical functions; or
4. Compliance would cause a major adverse financial impact on the agency that is not offset by statewide savings.

Exemption from this policy does not apply to mandatory reporting required by Idaho Code § 28-51-106(1).

VI. PROCEDURE REFERENCE

Standards:

- Acceptable encryption technologies are described in FIPS PUB 140-2
- Acceptable destruction methods are described in NIST SP 800-88 (Revision 1)

Guidelines:

- ITA Guideline G120 (Exemption Process)
- ITA Guideline G580 (Cyber Security Breach Notification)

Processes:

- ITA Policy P4510 (Cyber Security Incident Reporting)

VII. CONTACT INFORMATION

For more information, contact the ITA Staff at (208) 332-1876.

REVISION HISTORY

05/09/2017 – Revised to update Section III. Definitions; and Section IV. Policy.

Effective Date: December 8, 2015