Idaho Technology Authority (ITA)

ENTERPRISE GUIDELINES – G500 SECURITY PROCEDURES

Category: G580 – CYBERSECURITY BREACH NOTIFICATION

CONTENTS:

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

I. DEFINITIONS

Agency – Any public agency as defined in Idaho Code § 67-831, to include the following entities:

- State agency – Every state officer, department, division, bureau, commission and board or any committee of a state agency including those in the legislative or judicial branch, except the state militia.

- Local agency – Any county, city, school district, municipal corporation, district, public health district, political subdivision, or any agency thereof, or any committee of a local agency, or any combination thereof.

Data Breach - For the purposes of this policy, a data breach is a security incident in which personal information is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Verbal, non-verbal, or written dissemination of confidential client data by a staff member may also be considered a data breach. The inappropriate sharing of sensitive information in conversation, posting or disclosing confidential information to a public website, sending protected information to incorrect recipients, misplacing information technology (IT) assets such as laptop computers or mobile devices or careless disposal of documents or IT resources may all lead to compromised information with harmful and costly results.

Encryption – A cryptographic procedure used to convert plain text into cipher text in order to conceal the original information.

Personal Information - Includes 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. Fingerprints
11. Passwords
12. Parents' legal surname prior to marriage
13. Home address or phone number
14. Any other numbers or information that can be used to access a person's financial resources, obtain identification, act as identification, or obtain goods or services. Identifying 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.

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.

II. RATIONALE

Identity theft continues to be one of the fastest growing crimes within the United States. In an effort to minimize the impact of identity theft stemming from cyber security breaches, agencies are subject to Idaho Code sections 28-51-105 through 28-51-107, which address the specific notification requirements to Idaho residents when their personal information has been disclosed as the result of a cyber security breach.

These guidelines provide suggested procedures and templates for agencies to use when determining the applicability of and compliance with this statute. These guidelines are developed specifically for state government agency use and do not directly apply to individual or commercial entities.

Agencies should consult with the Office of the Attorney General for specific questions related to compliance with Idaho Codes 28-51-105 through 28-51-107. Furthermore, each agency's director and public information officer should oversee any communications sent on behalf of the agency to its customers or employees.

III. GUIDELINE

This guideline is divided into three sections to assist an agency in preparing for and conducting notifications resulting from a cyber security breach. These sections are:

- *Protecting Personal Information:* Outlines recommended actions to safeguard the personal information of Idaho's residents. These recommendations are designed to help the agency avoid a cyber security breach.

- *Planning for Notification:* Provides a recommended list of activities that the agency should conduct now to prepare itself in the event that a cyber security breach does occur, resulting in the need for notification to its customers or employees.

- *Notification:* Identifies the recommended and statutorily-required actions when notifying Idaho residents upon a cyber security breach.

1. Protecting Personal Information:

A. Minimize the amount of personal information collected to data that is necessary to accomplish the agency's mission, and minimize the retention time period of this information (in accordance with the State of Idaho's record retention requirements).

B. Conduct an internal inventory of all agency systems, storage media and data sources (e.g., databases, files, directories, etc.) that contain personal information.

   i. Periodically review and update the internal inventory to ensure all personal information is identified. This inventory should be conducted on a routine basis depending on the business needs of the agency; however, such an inventory should be reviewed at least annually.

   ii. Use the inventory results to assess the continued need to collect and/or store identified personal information.

C. Review, implement and enhance (as necessary) appropriate physical and technological security measures to protect personal information.

   Note: Idaho Code 28-51-105 does not stipulate specific security measures that must be enacted to protect personal information. Nonetheless, agencies are highly recommended to implement robust security measures to minimize the likelihood of a cyber security breach, thereby reducing the probability of needing to conduct a notification.

   i. Restrict access of agency personnel to specific personal information needed to accomplish their particular job responsibilities.

(1) Implement access controls and privileges (i.e., system permissions/rights) to limit internal access to personal information.

(2) Remove access privileges immediately for former employees and contractors.

ii. Encrypt personal information (when stored or transmitted).

(1) Per Idaho Code 28-51-104, a "breach of the security of the system" does not apply if the personal information is encrypted; therefore, it is in the agency's best interest to encrypt such data whenever possible.

(2) Idaho Code 28-51-104 does not specify the type of encryption required. However, "best practice" states that encryption should be based on current, Federal Information Processing Standards (FIPS-140-2)-approved encryption algorithms.

iii. Protect and/or restrict personal information on laptops or other portable computers and devices.

(1) Evaluate the need for personal information to be used or stored on portable computers and devices.

(2) Establish policies to limit or restrict the downloading of personal information to portable computers and devices.

(a) Clearly identify the locations in which such portable computers and devices can be used or stored (e.g., workplace, field offices, etc.). Portable computer and devices that contain personal information should not be used and/or stored at home, in automobiles, or at other non-work related locations.

(3) Implement procedures to physically secure portable computers and devices.

(a) Consider requiring the use of laptop security cables to deter thieves from stealing portable computers.

(4) Use encryption on all portable computers and devices (reference section 1.C.ii above for encryption guidance).

iv. Establish a proactive vulnerability management process to maintain relevant security updates and patches on systems that contain personal information.

(1) Reference ITA Policy P4520 (Patching and Vulnerability Management) and ITA Guideline G570 (Patching and Vulnerability Management), for required and recommended vulnerability management procedures.

v. Establish and review the agency's business continuity procedures.

(1) Update the business recovery plan to ensure personal information is appropriately secured throughout the business recovery process.

(a) Ensure personal information is stored and transmitted securely, if backed up and restored as part of the business recovery plan.

(b) Reference ITA Policy P2020 (Business Recovery Planning), for additional requirements and recommendations.

(2) Encrypt all backup copies that contain personal information (reference section 1.C.ii above for encryption guidance).

D. Implement security monitoring capabilities (e.g., intrusion detection systems, logging of server activity, etc.) to identify possible indications of a cyber security breach.

i. Log all access to personal information.

ii. Log all downloads of personal information to other resources (e.g., computers, PDAs, backup media/tapes, etc.).

iii. Review logs on a daily and monthly basis for suspicious activity. Investigate any activity that could result in the compromise of personal information.

E. Establish appropriate agency-level security policies, standards, and guidelines to assist in the protection of personal information.

i. Clearly identify acceptable practices for accessing, storing, transmitting, and using personal information.

F. Promote an on-going awareness program to inform all agency members of applicable ITA and agency security policies, standards, guidelines, and notification procedures.

i. Incorporate all new, temporary, and contract employees in this awareness program.

G. Require all third-party contractors, partners, and service providers who handle personal information on behalf of the agency to adhere to ITA and agency security policies, standards, guidelines and procedures.

i. Enforce adherence to security policies and procedures via contractual requirements.

ii. Monitor third-party compliance with such policies and procedures.

H. Dispose of computer equipment, media, and records containing personal information in a secure manner.

i. Reference ITA Guideline G550 (Cleansing Data from Surplus Computer Equipment), for recommendations on how to securely dispose of computer systems and media.

I. Periodically conduct third-party security assessments or audits to verify the effectiveness of implemented security measures and identify opportunities to improve the agency's protection of personal information.

2. <u>Planning for Notification:</u>

A. Designate a specific person or function as responsible for coordinating the agency's cyber security breach notification policies and procedures.

B. Review and update contact information of all individuals whose personal information is retained by the agency.

i. Depending upon the type of notification desired by the agency, the following contact information should be collected to provide the most flexibility when required to conduct a notification:

(1) Physical address,

(2) Telephone number, and

(3) Electronic mail address.

C. Identify how the notification text (to individuals affected by a cyber security breach) will be created and approved.

i. Include the following information in the notification to affected individuals:

(1) General description of what occurred,

(2) Type of personal information involved (e.g., Social Security number, driver's license number, etc.),

(3) What the agency has done to protect the personal information from further unauthorized acquisition/breach,

(4) Information on what the person can do to protect themselves from identity theft. Include the contact information for the following entities:

(a) Major credit reporting agencies.

(b) Federal Trade Commission (http://www.consumer.gov/idtheft).

(5) Contact information for the agency.

ii. Use clear and concise language within the notification.

(1) Avoid government and/or agency-specific jargon or acronyms.

(2) Avoid technical language.

iii. Reference notification templates in Appendix A, *Suggested Notification Templates,* for sample letters. Notification letters should be customized to clearly articulate the specific circumstances and recommendations.

D. Determine the best means of communication (e.g., electronic mail, letters, telephone, etc.) to the agency's customers.

E. Adopt an agency incident response plan that specifically outlines procedures for responding to incidents in which unauthorized access to (or acquisition of) personal information may have occurred.

i. Establish written procedures requiring immediate notification to the agency's key decision makers when a security incident is suspected or confirmed.

ii. Identify appropriate law enforcement contacts to notify when a cyber security incident may involve illegal activity.

(1) Appropriate law enforcement agencies may include the following:

(a) Idaho State Police, Cyber Crime Unit, (208)884-7000.

(b) Federal Bureau of Investigation, (208)344-7843.

(c) United States Secret Service, (208)334-1403.

(d) Local police or sheriff's department.

iii. Identify appropriate state government officials to contact following a cyber security incident [reference ITA Policy P4510 (Cyber Security Incident Reporting), for additional incident reporting requirements].

iv. Develop a method to document actions taken during the incident response and notification process. Communicate the need and requirement for such documentation to all personnel involved in this process.

F. Establish a requirement to conduct a post-mortem review of the incident response and notification actions in order to identify any necessary changes to the agency's policies, processes or technologies.

G. Review the agency incident response plan at least annually, or whenever a significant change occurs within the agency's business practices.

3. <u>Notification:</u>

A. Upon becoming aware of a potential breach, immediately implement the agency's incident response plan, to include immediately reporting the suspected breach to the agency's key decision makers.

B. Conduct a prompt and reasonable investigation.

i. Identify if any personal information has been illegally acquired (or believed to have been acquired), to include but not limited to the following scenarios:

(1) Indication that personal information is in the physical possession or control of an unauthorized person (e.g., stolen computer, stolen backup tape, etc.).

(2) Indication that personal information has been downloaded or copied.

(3) Indication that personal information has been used by an unauthorized person (e.g., opening of a fraudulent account, report of identity theft, etc.).

ii. If illegal activity may have been involved in the incident, report the incident to appropriate law enforcement entities.

(1) When contacting law enforcement, inform the law enforcement official in charge of the investigation that the agency intends to notify affected individuals as soon as possible. If the law enforcement official informs the agency that such notice would impede the criminal investigation:

(a) Ask the official to inform the agency when it can notify the affected persons without impeding the investigation, and

(b) Be prepared to conduct notification immediately upon being so informed by law enforcement.

iii. Determine the likelihood that personal information has been or will be misused.

(1) In accordance with Idaho Code 28-51-105, notification is only required if the agency determines that misuse of the personal information has occurred or is reasonably likely to occur. In determining this likelihood of misuse, consider the type of breach and the potential motives of the suspected person(s) who acquired the information.

(2) Err on the side of caution when determining the likelihood of misuse.

C. Implement appropriate actions to contain and control the system(s) impacted by the breach.

i. If possible, restrict the system's network access. Ideally, the affected system(s) should be removed from the network. However, if the system(s) cannot be removed due to critical business needs, the agency should isolate the system(s) as much as possible to protect other systems from being compromised.

D. Assess the scope of the breach to determine the number of persons affected, the type of information compromised, and other relevant facts.

i. Assemble a complete and accurate list of affected individuals. This list should serve as the master document for conducting and tracking notification.

(1) If specific persons cannot be identified, identify and notify all those in the groups likely to have been affected (e.g., all potential persons whose information was likely stored in the files involved).

(2) Make a reasonable effort to include only those persons impacted by the breach in order to avoid false positive notification. A false positive notification is when the notification is sent to an individual who has not been affected by the breach.

ii. Determine the method for notification based upon the scope of the breach.

(1) Individually notify those affected, whenever possible.

(2) Notice must comply with one of the following types (as specified in Idaho Code 28-51-105):

(a) Written notice to the most recent address the agency has in its records, or,

(b) Telephonic notice, or,

(c) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures (as set forth in 15 U.S.C. § 7001), or

(d) Substitute notice (reference the next section, 3.D.ii.(3), for definition and restrictions on substitute notice).

(3) Substitute notice may be used only if the agency can demonstrate that the cost of providing notice will exceed $25,000, or the number of Idaho residents to be notified exceeds 50,000, or the agency does not have sufficient contact information for the persons affected. Substitute notice consists of:

(a) Electronic mail notice if the agency has the electronic mail addresses for the affected Idaho residents; and

(b) Conspicuous posting of the notice on the web site page of the agency; and

(c) Notice to major statewide media (television, radio, print).

E. Consider contacting the major credit reporting agencies if the scope of the breach involves 10,000 or more individuals.

i. Make arrangements with the credit reporting agencies during the preparation of the notice. *Do not delay notice for this reason.*

ii. Contact the following consumer credit reporting agencies:

(1) Experian, BusinessRecordVictimAssistance@experian.com

(2) Equifax, Chris Jarrard, Vice President, US Customer Services, (678)795-7090, chris.jarrard@equifax.com

(3) TransUnion, fvad@transunion.com (with “Database Compromise” as the subject of the electronic mail)

F. Prepare and distribute the notification in accordance with the agency’s external communications process.

i. Confirm the final notification list before sending the notice to ensure the list is accurate.

ii. Maintain a document that positively identifies each individual notified and the method of notification used (unless substitute notice has been used).

IV. PROCEDURE REFERENCE

Guidelines for cyber security breach notification procedures are detailed in ITA Information Technology Enterprise Guidelines G510 (Cyber Security Incident Reporting Template), G550 (Cleansing data from Surplus Computer Equipment), and G570 (Patch and Vulnerability Management).

Policies for cyber security breach notification procedures are detailed in ITA Information Technology Enterprise Policies P2020 (Business Recovery Planning), P4510 (Cyber Security Incident Reporting), P4520 (Patch and Vulnerability Management), and P4560 (Data Breach Management).

1. *Idaho Code 28-51-104:* Definitions

2. *Idaho Code 28-51-105:* Disclosure of Breach of Security of Computerized Personal Information by an Agency, Individual or Commercial Entity

3. *Idaho Code 28-51-106:* Procedures Deemed in Compliance with Security Breach Requirements

4. *Idaho Code 28-51-107:* Violations

V. CONTACT INFORMATION

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

REVISION HISTORY

07/01/18 – Updated Idaho statute reference.

10/20/15 – Revised to update Definitions and Reference information

07/01/13 – Changed “ITRMC” to “ITA”.

6/16/09 – Added Procedure Reference, Contact Information and Revision History to this guideline; changed the layout and deleted References and Timeline.

Effective Date: September 13, 2006

CYBER SECURITY BREACH NOTIFICATION TEMPLATE
APPENDIX A

SAMPLE LETTER 1
Data Illegally Acquired: Credit Card (or Financial Account) Number Only

Dear _____,

We are writing because of a recent security incident at *[name of organization]*.

[Describe what happened in general terms, what type of personal information was involved, and what you are doing in response.]

To protect yourself from the possibility of identify theft, we recommend that you immediately contact *[credit care or financial account issuer]* at *[phone number]* and close your account. Tell them that your account may have been compromised. If you want to open a new account, ask *[name of account issuer]* to give you a PIN or password. This will help control access to the account.

To further protect yourself, we recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at a number below. This will let you automatically place fraud alerts with all of the agencies. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Experian	Equifax	TransUnion
888-397-3742	800-525-6285	800-680-7289

For more information on identify theft, we suggest that you visit the Federal Trade Commission at www.consumer.gov/idtheft. If there is anything *[name of organization]* can do to assist you, please call *[toll-free number]*.

[Closing]

SAMPLE LETTER 2
Data Illegally Acquired: Driver's License (or Idaho ID Card) Number

Dear _____,

We are writing because of a recent security incident at *[name of organization]. [Describe what happened in general terms, what kind of personal information was involved, and what you are doing in response.]*

Since your Driver's License *[or Idaho Identification Card]* number was involved, we recommend that you immediately contact your local DMV office to report the theft. Ask them to put a fraud alert on your license.

To further protect yourself, we recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at a number below. This will let you automatically place fraud alerts with all of the agencies. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Experian	Equifax	TransUnion
888-397-3742	800-525-6285	800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquires from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a report of identify theft. *[Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.]* Get a copy of the policy report. You may need to give copies to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft, we suggest that you visit the Web site of the Federal Trade Commission at www.consumer.gov/idtheft. If there is anything *[name of your organization]* can do to assist you, please call *[toll-free phone number].*

[Closing]

SAMPLE LETTER 3
Data Illegally Acquired: Social Security Number

Dear _____,

We are writing because of a recent security incident at *[name of organization]. [Describe what happened in general terms, what kind of personal information was involved, and what you are doing in response.]*

To further protect yourself, we recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at a number below. This will let you automatically place fraud alerts with all of the agencies. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Experian	Equifax	TransUnion
888-397-3742	800-525-6285	800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquires from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a report of identify theft. *[Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.]* Get a copy of the policy report. You may need to give copies to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft, we suggest that you visit the Web site of the Federal Trade Commission at www.consumer.gov/idtheft. If there is anything *[name of your organization]* can do to assist you, please call *[toll-free phone number].*

[Closing]