STATE OF HAWAIʻI
INFORMATION PRIVACY AND SECURITY COUNCIL

Category	Security, Breach	Title	**Breach Best Practices**
Document:	IPSC2009-02	Revision:	**2009.08.28-01**
Posted URL:	http://ipsc.hawaii.gov		
Status Under Review		Revised on:	August 28, 2009
Authority:	State of Hawaiʻi IPSC	Exceptions:	Temporary Allowed
Applicability	☒State Government Agencies ☒All .... Guideline □Excluding: None .... Not Applicable □Including: None .... Not Applicable ☒State Funded Entities .... Guideline ☒Other: County Government Agencies & Attached .... Guideline		

I. PURPOSE

This document will outline the recommended best practices to ensure that agencies protect personal data that may be in its possession. While not a comprehensive plan for data protection, this best practices document should serve as a starting reference point for the development of detailed data protection policies, procedures, and guidelines within the operational framework of the organization.

The Information Privacy and Security Council (IPSC), is tasked with ensuring that all state and county agencies are in compliance with applicable laws governing the handling of personal data and information. This best practices document is being provided to agencies as a reference source for activities related to the handling of sensitive data. These best practice recommendations include:

Notification of affected individuals when breaches occur;

The **reduction** of the use of personal data in the functions of an organization’s day to day business activities;

The **redaction** of personal information from business related documents.

II. SCOPE

This guideline meets only the requirements imposed by the State of Hawaii. Agencies/Departments that work with federal information of a confidential or sensitive nature must ALSO ensure that their internal practices, procedures, policies and guidelines are in compliance with all requirements and policies at the federal level.

III. TERMS AND DEFINITIONS

Personal Data – A person's first name and last name used in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- Social Security Number
- Drivers License Number
- Account Number, credit or debit card number, access code, or any other number, code, or password that would allow access to use an individual's credit or financial information

In addition to the list above as identified in the Hawai'i Revised Statutes, agencies may be subject to the inclusion of items defined in Federal Regulations including:

- Date of birth
- Home/cell/mobile phone and personal mail address

Personal data also includes information described in Chapter 92F-14 of the Hawai'i Revised Statutes.

Data Breach - The unintentional release of secure information to an insecure environment such as theft or loss of digital media such as computer tapes, hard drives, or laptop computers containing such media upon which such information is stored unencrypted.

Redaction – The complete removal from the document of the social security number, driver's license, number of Hawaii identification card, account number or debit card number, access code, and or password.

Identity Theft - A crime used to refer to fraud that involves someone pretending to be someone else in order to steal money or get other benefits.

IV. General Best Practices

User Education - Agencies should take an active role in educating their users on the handling of sensitive and confidential information that is used in their day to day business functions. Users should be made aware of the agency's policies, procedures, practices and guidelines of handling confidential information as part of the initial on-boarding process (upon hire) and periodically thereafter.

Initial System Design - The reduction of the use of personal information can start at the initial stages of systems design and development. While this recommendation may be feasible for design efforts just getting underway, existing systems may be hard pressed and unable to go through a major redesign effort without adding significant cost. Never the less, developers and application designers should make every effort to reduce the use of personal information as data elements within the application design structures.

Develop Security Policies – Organizations should be actively developing, maintaining, and revising their security policies in response to new and emerging trends and threats related to confidential information in their possession or area of responsibility.

Develop System Access Policies – System Access Policies (including related forms and documentation) should be designed with the expressed purpose of granting systems access on a "need to have" basis only. Requestors should identify the specific purpose needed for systems access and supervisors or managers should be brought into the fold (via the approval process) for sign off and acknowledgment of the requested access.

Organizations should also periodically audit the systems access catalog to ensure that access to confidential information is adequate and appropriate.

Accounts inactive for a more than 60 days should be disabled and deleted after an additional 30 days of non-use.

Implement Automated Auditing Features – Organizations should implement automated auditing features within their application framework to ensure that systems access remains appropriate. These auditing features would track new, existing, transferring, or terminated employees throughout their employment lifecycle and match these status changes with recommendations to the system administrator for appropriate action.

Limit the use of Self Service Applications - Self service applications may open up internal operational systems to outside intrusion and attacks. Therefore, agencies should limit access to self service applications or isolate and separate web based self service applications from its core operational systems. This can be achieved by the use of DMZ zones and proxy server machines which redirects network traffic out and away from the internal operational systems to zones specifically created to isolate traffic originating from outside the systems firewalls.

Implement Confidentiality Agreements between parties – Data stored, transferred through, or otherwise handled by third parties should be covered under the respective department's data handling procedures for personal information. Agencies should develop confidentiality agreements to be executed with all vendors doing business with the department, or having access to the department's systems and confidential data and information. These agreements should be fully executed prior to the delivery of services to the department by the vendor.

Implement Data Encryption Technologies for all data transfers and distributions - Agencies should incorporate file encryption methods in all data transfers to and from their respective data systems. The encryption should be based on standard encryption methods and algorithms. Decryption key safe keeping and exchange should be considered proprietary and confidential information, and should be handled appropriately by the individual agencies and their data exchange partners.

V. Breach Best Practices

Involving Law Enforcement Agencies – Agencies should notify law enforcement agencies within applicable timeframes as specified by law. Agencies may be required to hold off on notifying affected parties until investigations are completed or underway by the involved law enforcement authorities.

Notifications - Agencies should develop an in-house Breach Notification matrix which identifies the specific chain of events for notifications should an information breach occur. At a minimum, the matrix should identify specific parties, timelines, actions, and additional notes deemed necessary in responding to personal information breaches.

Handling Concerns - Agencies should establish in house practices for handling concerns from persons affected by the data breach. At a minimum these practices should outline the internal processes and procedures to handle, address, and respond to the concerns of the affected party or parties.

Agencies should make these practices readily available on their websites or other easily accessible information sources.

VI. Redaction Best Practices

Organizations should develop a set of redaction best practices to ensure that they are in compliance with applicable laws concerning the protection of personal data and information in their possession. These best practices could include:

> **Use of Strike Through as a redaction method** – Most commercially available word processing application software offer some form of strike through editing capabilities. While these tools may be adequate for document development, it may not be a suitable form of redaction as required by law. Agencies should be careful in the use of these editing tools to ensure that redacted text is absolutely undecipherable.
>
> **Use of Block Out as a redaction method -** Agencies may use a block out technique to hide or conceal confidential information in order to comply with applicable laws.

However, this method of redaction may not be feasible for documentation that contains many printed pages.

Use of Text Removal as a redaction method - Agencies may choose to remove confidential information from documents (via the document editing process) prior to generating the final hardcopy output. In printed hardcopy form, these documents would not contain any confidential information.

VII. Reduction Best Practices

Organizations should seek to reduce the use of personal data in their day to day business functions wherever possible and feasible. In areas where it is absolutely necessary to use personal information, organizations should be prudent in developing practices and procedures to ensure that the data in their possession is both secure and safe from unauthorized use and abuse. Best practices to reduce the use of personal information include:

Use of alternate unique identifiers for personal information – Agencies should utilize alternate unique identifiers in their systems designs, system modifications, upgrades, migrations, etc. Alternate unique identifiers would essentially render personal information indecipherable by replacing existing information with that recognizable (or translatable) by the system utilizing conversion keys or translate and crosswalk tables.

Hiding fields from view according to end-user security levels – Current technology allows systems designers and developers to tie in filed level access to an end-users security settings and access rights. Agencies should utilize these features to “hide” sensitive data fields and restrict access only to users having a need-to-know/see access as part of their normal job function.

Designating certain fields as read-only – System control functions should be utilized to “lock” certain data fields as a preventative measure against unauthorized change or modification. Additional system audit functions should also be turned on for specific fields in order to identify end-users who may be making changes or modifications.

Truncation of personal data fields – Agencies should make it standard practice to truncate or mask personal data from terminal display or hardcopy output reports. This would especially apply to data fields or reports displaying personal information to include data such as social security numbers, personal bank account numbers, mailing and home addresses.

VIII. MONITORING

All State and County government agencies have the right to monitor, review, audit, and/or disclose any and all aspects of use of the agency's technology resources in accordance with the applicable policies of the agency.

IX. ENFORCEMENT

Violations of State and County government agency policies will be governed by policies specific to each agency and applicable laws & regulations.

X. REFERENCES AND ATTACHMENTS

State Information

Department of Accounting and General Services, dated June 4, 2007, Policy Re Act 135 (Notification of Security Breaches), 136 (Destruction of Personal Information Records), and Act 137 (Social Security Number Protection), Session Laws of Hawaii 2006.

Department of Human Resources Development, dated May 28, 2008, Policies and Procedures on the Acceptable Usage of Information Technology Resources, Revision 1, Policy No. 103.001

Security Breach of Personal Information, Hawaii Revised Statute Chapter 487R (July 1, 2007).

Uniform Information Practices Act (Modified), Hawaii's Open Records Law, Hawaii Revised Statutes 92F (June, 2008).

Federal Information

United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication, Security Requirements for Cryptographic Modules (FIPS PUB 140-2)

United States Department of Commerce, National Institute of Standards and Technology, An Introduction to Computer Security (NIST SP800-12)

United States Department of Commerce, National Institute of Standards and Technology, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (NIST SP800-22)

United States Department of Commerce, National Institute of Standards and Technology, Contingency Planning Guide for Information Technology Systems (NIST SP800-34)

United States internal revenue Service, Tax Information Security Guidelines for Federal, State and Local Agencies and Entities, (Publication 1075)

XI. COMMENTS AND SUGGESTIONS

Comments, recommendations, proposals, or suggestions regarding the contents of this document may be sent via email to:

IPSC@hawaii.gov

or in writing to:

Information Privacy and Security Council
c/o Information and Communication Services Division
1151 Punchbowl Street, Room B10
Honolulu, HI 96813

XII. REVISION HISTORY

Creation Date:	Date Last Updated	Date last reviewed
August 28, 2009	August 28, 2009	August 28, 2009
Revision History		
Revision date	**Revision**	**Author**
Aug 28, 2009	2009.08.28-01 First Issue	Information Privacy & Security Council

Russ K Saito

Russ K. Saito, Chairperson
Information Privacy and Security Council

8/28/09

Date