STATE OF HAWAIʻI
Information Privacy and Security Council

Category	**Personal Data**	Title	**Personal Data Privacy Guideline**
Document:	**IPSC2011-01**	Revision:	**2011.04.20**
Posted URL:	Enter Permanent Source URL for this document		
Status	Under Review	Revised on:	April 20, 2011
Authority:	**State of Hawaiʻi IPSC**	Exceptions:	Temporary Allowed
Applicability	☒State Government Agencies ☒All ..... Guideline ☐Excluding: ..... Not Applicable ☐Including: ..... Not Applicable ☒State Funded Entities ..... Guideline ☒Other: Counties ..... Guideline		

I. PURPOSE

This document will provide agencies with general guidelines to be used in the development of their own internal policies and procedures concerning the handling and protection of Human Resources (HR) data and information. This guideline is not meant to represent a comprehensive scope of parameters in the handling, protection, storage, transfer, or disposal, of personal data, instead, its purpose is to provide agencies with a starting point in the development of their own handling guidelines.

II. SCOPE

This guideline meets only the requirements imposed by the State of Hawaiʻi. Agencies/Departments that work with federal information of a confidential 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

"**IT resources"** means all hardware, software, documentation, programs, information, data, and other devices that are owned or provided by the State. These resources include

those that enable remote and local communication such as hubs, switches, routers, and concentrators or access between various platforms and environments such as the mainframe, minicomputers, servers, Local Area Networks ("LANs"), Wide Area Networks ("WANs"), and personal computers.

"Personal Data" as defined in _____, means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social Security Number;

(2) Driver's license number or Hawaii identification card number;

(3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account;

(4) Date of birth;

(5) Home/cell/mobile phone and personal mail address.

"Authorized Users" – Authorized Users are defined as those users granted access to Personal Information or Data stored (either electronically or in hard copy format) within a physical location or an electronic computer system or transmitted through an electronic communications system.

"Users" mean all employees who are authorized to use or access the State's IT resources.

"Data Exchanges" – A "Data Exchange" is defined as a transfer of information between two government entities or between a government entity and non-government entity including vendors, consultants, financial institutions and other entities doing business with the transferring/receiving agency. The content of the information is usually in a point-time format.

"Data Interfaces" – A "Data Interface" is defined as an active transfer of information between a government entity and any other entity

"Data Retention Policy" – A "Data Retention Policy" contains explicit parameters for the retention of data and information pertinent to government operations and business and includes the Statewide Records Retention Schedule

"Data Disposal Policy" – A "Data Disposal Policy" contains explicit parameters for the proper disposal of data and information containing personal or confidential data or information.

IV. GUIDANCE

Permissible use of Personal Information – Government agencies shall develop policies and procedures that define the permissible use of Human Resources Information. These

policies should indicate the specific purpose to gather, store, manipulate, and transfer personal information within and external to an agencies business functions.

Implementing Safeguards to Protect Personal Information – Agencies should implement safeguards to protect Human Resources Information, including:

- Regular reviews of their data and information protection polices
- Conduct regular reviews of the confidentiality agreements, acceptable use policies, vendor agreements and contract boilerplate documents, etc.
- Conduct audits of existing safeguards and protection measures and make adjustments as needed
- Conduct audits of existing security policies and procedures
- Periodic review and revision of existing security policies and procedures especially in light of new and emerging security treats and vulnerabilities
- Conduct regular and periodic training for end users to insure that current and new policy measures are clearly communicated
- Conduct periodic reviews of agency document retention and data retention policies
- Conduct periodic reviews of agency data and information disposal policies
- Implement policies that prohibit the storage, manipulation, or transfer of personal data and information on agency owned equipment, storage media (both offline and online) without the expressed permission from the agency head or higher authority

Reasonable Expectations to protect Personal Information – Organizations should communicate to their end users that there exist a reasonable expectation that uses will not violate existing policies and procedures, and shall include:

- Sign-off by end users and acknowledgement of existing policies and procedures
- Review of current policies and procedures on an a regular basis with the user community
- Inclusion of the security and data protection measures as part of an individual's performance evaluation standards

Recommended Monitoring Procedures – Agencies shall take reasonable measures in implementing monitoring procedures and/or technologies to ensure that all Human Resources information is safe and secure. Monitoring procedures may include:

- Monitoring via electronic means such as system scanners including firewalls, security appliances, content filtering, etc.

- Implementation of manual tracking logs that are maintained by all personnel handling Human Resources information

- Implementation of automatic tracking log systems that are part of the systems design architecture

Revocation of Access to Personal Data Resources

Organizations should implement procedures that result in the revocation of system, data, and information access as a first step in the investigative process in determining the extent of the data breach or violation. System access may be either curtailed or totally revoked according initial assessments of the violation. End users shall be informed of the revocation action as soon as the investigation begins and should be kept abreast of the outcomes of the investigation of both the preliminary and final findings of the investigation.

In the case of long term investigative actions, alternate work duties should be assigned to the individual that do not involve access to confidential information or secure system access. Final authorization of the permanent access revocation (as well as further disciplinary or legal action) should be the responsibility of the agency or department head.

Policy Violation Guidelines

It is recommended that agencies develop clear Policy Violation Guidelines specific to their operations and to the severity and seriousness of the violation. These guidelines should clearly state the consequences possible should policy violations occur and may include outcomes such as:

- Temporary or Permanent Revocation of system access

- Disciplinary action such as work suspension

- Discharge from employment

- Criminal Prosecution

Final authorization of the permanent access revocation (as well as further disciplinary or legal action) should be the responsibility of the agency or department head.

V. RESPONSIBILITIES

Department or Agency Head

Agency or Department Heads should develop policies and procedures that protect Human Resources data and information within their agency or department. This guideline may be used as an outline in the development of the department policy.

Agency Responsibilities

Agency specific policies that are developed should be communicated and transmitted to all agency personnel handling, transferring, compiling, filing or otherwise coming into contact with Human Resources information. It is further recommended that departments and agencies review their employment status parameters to ensure that regulations governing access to Human Resources data is still valid and relevant.

User Responsibilities

Users should be made aware of agency policies and procedures pertaining to Human Resources data and information. Agencies should conduct regular data security awareness training to include specific subject matter related to the handling of HR information as well as handling guidelines for Human Resources information and data.

Vendors, Contractors, Consultants, and other users

Vendors, Contractors, Consultants, and all other non-employee personnel doing work for or having access to confidential Human Resources data shall be made aware of agency policies, procedures, guidelines, best practices, etc., prior to engaging in any work for the agency. Agency personnel responsible for the engagement should obtain prior approvals (internal) prior to the commencement of any work activities or granting systems access.

VI. REFERENCES AND ATTACHMENTS

Chapter 84-12, Hawaii Revised Statutes, Standards of Conduct

Chapter 92F-14, Hawaii Revised Statutes, Uniform Information Practices Act

Department of Human Resources Development, Acceptable Usage of IT Resources dated May 28, 2008

VII. REVISION HISTORY

Creation Date:	Date Last Updated	Date last reviewed
March 15, 2011	March 15, 2011	April 20, 2011

Revision History		
Revision date	**Revision**	**Author**
April 20, 2011	Initial Issue	IPSC

Bruce Coppa, Chairperson
Information Privacy and Security Council

April 20, 2011
Date