	DEPARTMENT OF PUBLIC SAFETY	EFFECTIVE DATE: APR 7 2011	POLICY NO.: ADM.09X.10
	DEPARTMENT ADMINISTRATIVE POLICY AND PROCEDURES	SUPERSEDES (Policy No. & Date): NEW	
	GENERAL SECURITY POLICY		Page 1 of 5

1.0 PURPOSE

The Hawai'i Department of Public Safety (PSD) Security Information Technology Policies are documented in the PSD Policies Manual Chapter 9, entitled Information Technology Security and is maintained by the Management Information System Unit.

The PSD IT Security Policies will apply to all PSD Division, Branches, Staff Offices and attached agencies. All references to "PSD staff" in the PSD IT Security Policies will refer to these components.

These PSD IT Security Policies will address appropriate and reasonable IT industry security practices for the IT Systems and for the PSD staff.

The purpose of this policy is to establish Information Technology Security policies that ensure the confidentiality, integrity and availability of electronic confidential information.

2.0 REFERENCES

.1 DHS Policy & Procedure 8.2.01 August 23, 2006.

3.0 DEFINITIONS

"Confidential Information" Personnel information, identifiable health information, attorney/client privileged information, technical information that could allow unauthorized access, information deemed confidential by Federal or State law or administrative rules, and all information that would be exempt from public disclosure by HRS §92F -13, the Uniform Information Practices Act

"Electronic Confidential Information" Confidential information (see definition above) created, maintained, stored, transmitted, or disposed of through electronic media.

"Information Communication and Services Division (ICSD)" A branch of the Department of Accounting and General Services that provides IT and Communication Services to all the State Departments.

"MIS" is the PSD Management Information Systems unit responsible for managing the Information Technology resources of the Department.

PSD P & PM	GENERAL SECURITY POLICY	POLICY NO.: ADM.09X.10
		EFFECTIVE DATE: APR 7 2011
		Page 2 of 5

“Safeguard” Steps taken to prevent security breaches. This may include hardware, software, physical structure and/or procedures.

“Security Measure” similar to safeguard.

“User” means all State employees in the PSD including all outside personnel. Outside personnel includes, but not limited to, employees from other agencies, volunteers, contractors, and vendors who are authorized to use or access State IT resources.

4.0 SCOPE

This policy applies to all employees of the PSD who are authorized to use or access the State’s IT resources.

Outside personnel including employees from outside agencies, volunteers, contractors and vendors shall obtain prior written approval from the PSD before accessing the State’s IT resources.

5.0 GENERAL PROVISIONS

.1 PERMISSION AND ACCEPTANCE

The use of any of the State’s IT resources implies that the user accepts and agrees to all the terms and conditions as contained in this policy.

.2 STATE AS OWNER, CUSTODIAN AND LICENSEE

The State, and not the employee, is the sole owner, custodian, and in cases of software, the licensed user of all IT resources.

.3 NO EXPECTATION OF PRIVACY

Users are on notice that there is no proprietary interest and no reasonable expectation of privacy while using any of the IT resources that are provided by the State. The State considers all information and data processed, transmitted, received, and stored on the State’s IT resources, including but not limited to, processed documents, electronic and voice mail, and Internet communications as owned by the State. The State may obtain access to any of its resources at any time. The State may disclose any of its IT resources to law enforcement or other authorized third parties without prior consent of the users.

PSD P & PM	GENERAL SECURITY POLICY	POLICY NO.: ADM.09X.10
		EFFECTIVE DATE: APR 7 2011
		Page 3 of 5

.4 MONITORING AND ENFORCEMENT

The State is the owner or custodian of data and information that is stored on, processed by, or transmitted through the State's IT resources. The State may at any time, and without prior notice, examine data and information such as electronic mail, individual file directories, and other information for purposes such as, but not limited to, ensuring compliance with applicable rules, regulations, policies and procedures, monitoring the performance of the IT resources, and conducting investigations.

The State has the right to monitor, review, audit, and/or disclose any and all of the aspects of the computing and networking resources including, but not limited to, monitoring access by users to the Internet sites that are visited, viewing the contents of electronic mail, documents, files, blog entries, chat groups, or news groups, and inspecting materials that are downloaded and uploaded by users.

.5 REVOCATION OF ACCESS TO IT RESOURCES

The State reserves the right, without advance notice to users, to revoke access to IT resources, to override users passwords without notice, or to require users to disclose passwords and/or codes to facilitate access to information that is processed and stored in the department's IT resources.

.6 POLICY VIOLATIONS

Violation of this policy by users may result in immediate revocation or curtailment of computer usage, and other disciplinary action in accordance with provisions of the collective bargaining agreement and also the possibility of civil and criminal liability.

.7 AMENDMENTS AND REVISIONS OF THIS POLICY

The State reserves the right to amend or revise this policy from time to time, as the need arises.

PSD P & PM	GENERAL SECURITY POLICY	POLICY NO.: ADM.09X.10
		EFFECTIVE DATE: APR 7 2011
		Page 4 of 5

6.0 POLICY

.1 GENERAL TERMS

All electronic confidential information must be available and accessible only to individuals authorized to have access. Authorized individuals must ensure that all electronic confidential information remains confidential and follow all the PSD policies and applicable State and Federal laws, regulations and rules, related to privacy and security of such information.

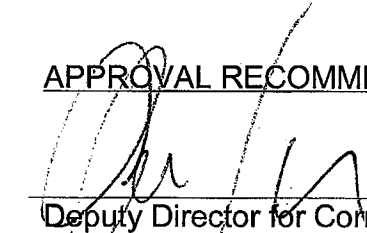
.2 REQUIREMENTS

- a. **Policies and Procedures:** The PSD will implement IT Security policies and procedures that will guide the Department to protect its electronic confidential information.
- b. **Flexibility of Approach:** The PSD will establish policies and procedures based on its review of its systems, equipment, system capabilities and the resources available with which to implement these policies and procedures.
- c. **Implement Safeguards:** The PSD must implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic confidential information which it creates, receives, maintains and transmits.
- d. **Ensure External Agencies Safeguards:** The PSD will ensure that all external agencies including users, vendors and subcontractors, to whom it provides electronic confidential information, agree in writing to implement reasonable and appropriate security measures to protect the Department's electronic confidential information.
- e. **Maintenance:** The PSD will periodically review and update all policies and procedures as needed, especially in response to technical, operational or environmental changes affecting the security of electronic confidential information. All implemented security measures will be reviewed periodically and modified, as needed, to ensure reasonable and appropriate protection of electronic confidential information.

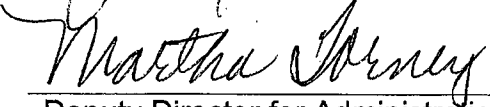
PSD P & PM	GENERAL SECURITY POLICY	POLICY NO.: ADM.09X.10
		EFFECTIVE DATE: APR 7 2011
		Page 5 of 5

- f. Consistency of Policies: The PSD will comply, to the extent that is reasonable and appropriate, to the State of Hawai'i Information Communication and Services Division's Information Technology Security Policies.


APPROVAL RECOMMENDED:


 Deputy Director for Corrections

3/16/11
 Date

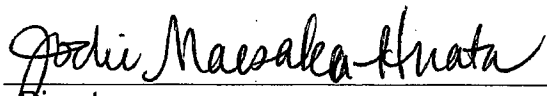

 Deputy Director for Administration

2/14/11
 Date


 Deputy Director for Law Enforcement

3/11/11
 Date

APPROVED:


 Director

4/7/2011
 Date

Policy No. ADM.09X.10
Attachment I

GENERAL SECURITY

ACKNOWLEDGEMENT FORM

I, _____ have read

Department of Public Safety Policy No. ADM.09X.10 General Security Policy, and I understand and agree to comply with all of the terms and conditions set forth therein. I agree that all network activity, conducted with State resources is the property of the State of Hawai'i and therefore, I acknowledge and understand that I do not consider such activity to be private.

I further understand that the State's information technology shall be used primarily to conduct State business and to provide services to the citizens of Hawai'i. These resources shall only be used for legal purpose and shall not be used in any manner or of purpose that is illegal, dishonest, disruptive, threatening, damaging to the reputation of the State, inconsistent with the mission of the State, or likely to subject the State to liability.

The State of Hawai'i reserves the right to monitor and log all network activity, including e-mail and internet browsing, with or without notice or consent, and therefore, users shall have no expectation of privacy in the use of these resources.

Signature

Date

Print Name