

	DEPARTMENT OF PUBLIC SAFETY	EFFECTIVE DATE: APR 7 2011	POLICY NO.: ADM.09U.10
	DEPARTMENT ADMINISTRATION POLICY AND PROCEDURES	SUPERSEDES (Policy No. & Date): NEW	
	ACCEPTABLE USAGE OF IT RESOURCES POLICY	Page 1 of 13	

1.0 PURPOSE

The purpose of this policy is to define the acceptable and prohibitive usages of the IT resources. These stipulations are necessary to minimize the risk to the Department of Public Safety (PSD) systems and connected State agencies.

The use of the State's Information Technology (IT) resources by its employees is a privilege and shall be used for furthering the State business and serving the citizens of Hawaii. Usage shall be limited to legal purposes only and shall not be for illegal, dishonest, disruptive, and threatening purposes, damaging to the reputation of the State, inconsistent with the mission of the State, or likely to subject the State to legal liability.

2.0 REFERENCES

Department of Human Resources Development Acceptable Usage of IT Resources Policies and Procedures Rev. No 1 05/28/08

3.0 DEFINITIONS

"IT resources" means all hardware, software, documentation, programs, information, bandwidth, data, and other devices that are owned or provided by the State. These resources includes, but not limited to, those that enable remote and local communications such as switches, routers and concentrators, or access between platforms and environment such as the mainframe, microcomputers, server, Local Area Network ("LAN"), Wide Area Network ("WAN") and personal computers.

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

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

- Social Security Number.

PSD P & PM	ACCEPTABLE USAGE OF IT RESOURCES POLICY	POLICY NO.: ADM.09.U.10
		EFFECTIVE DATE: APR 7 2011
		Page 2 of 13

- Driver's license number or Hawaii identification card number.
- Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.
- Date of birth.
- Home/work/mobile phone numbers and personal mail addresses.
- Personal data also includes information described in Chapter 92F-14 of the Hawaii Revised Statutes. Unencrypted email is not secured transmission.

“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 other 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 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.

PSD P & PM	ACCEPTABLE USAGE OF IT RESOURCES POLICY	POLICY NO.: ADM.09.U.10
		EFFECTIVE DATE: APR 7 2011
		Page 3 of 13

.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 IT 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 user.

.4 MONITORING AND ENFORCEMENT

The State is the owner and 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.

PSD P & PM	ACCEPTABLE USAGE OF IT RESOURCES POLICY	POLICY NO.: ADM.09.U.10
		EFFECTIVE DATE: APR 7 2011
		Page 4 of 13

.6 POLICY VIOLATION

Violation of this policy by users may result in immediate revocation or curtailment of computer usage, disciplinary action that may include discharge from employment, and/or 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.

6.0 POLICY

.1 GENERAL TERMS

a. MANAGEMENT INFORMATION SYSTEMS

The PSD, MIS administrator or supervisors or their designees shall be responsible for:

1. Authorizing the use of IT resources for specific employees.
2. Disseminating this policy and any amendments.
3. Ensuring that users of IT resources are familiar with the provisions of this policy and any amendments hereto, including developing procedures to ensure that all affected employees are aware of this policy and any amendments.
4. Supervising the use of IT resources, including taking reasonable precautions to safeguard the resources under their jurisdiction against unauthorized access, use, disclosure, modification, duplication or destruction.
5. Ensuring that current and new users are informed of appropriate uses of the State's IT resources.
6. Enforcing this policy and any amendments.

PSD P & PM	ACCEPTABLE USAGE OF IT RESOURCES POLICY	POLICY NO.: ADM.09.U.10
		EFFECTIVE DATE: APR 7 2011
		Page 5 of 13

7. Taking appropriate corrective action for violations of this policy and any amendments.

b. **USERS RESPONSIBILITY**

1. All users shall become familiar with this and other supporting and applicable IT resource policy(s). Questions relating to the applicability of this policy may be directed to the PSD's Office of Personnel. Questions related to the technical aspects of the IT resources may be directed to the PSD's MIS office and/or PSD's designated office.
2. Avoid deliberately performing acts that waste IT resources or unfairly monopolize resources to the exclusion of others. Such acts include, but not limited to, printing multiple copies of documents, using the electronic mail system for sending mass mailings or chain letters, spending excessive amounts of time on the Internet, engaging in online chat groups, video streaming or otherwise creating network traffic, unless it is in the course of work.
3. Avoid copying and/or downloading audio, video and picture files, unless these actions are work-related.
4. Users should routinely delete outdated and unnecessary computer files to free up IT resources to help keep systems running more efficiently and smoothly.
5. Users have the responsibility to act lawfully, ethically, respectfully and responsibly in the use of the State's IT resources.
6. Maintain the confidentiality of classified materials including personal data.
7. Transmit or disclose classified and/or confidential information including personal data through secured electronic communication media only to another party who is authorized to receive or view such information.

PSD P & PM	ACCEPTABLE USAGE OF IT RESOURCES POLICY	POLICY NO.: ADM.09.U.10
		EFFECTIVE DATE: APR 7 2011
		Page 6 of 13

8. Immediately report an encounter or receipt of unlawful, unethical or questionable materials to a supervisor or the PSD designee.
9. Take all reasonable precautions to protect the State's IT resources from unauthorized access, use, disclosure, modification, duplication and/or destruction.
10. Assist and cooperate in the protection of the IT resources and follow PSD procedures in matters such as, but not limited to, logging off and powering down while away from the computer and at the end of each workday; scanning files obtained from external sources for viruses and signs of other malicious codes prior to accessing the information, and making backup copies of files and data on the hard drives of their respective personal computers.
11. Protect passwords from disclosures to any other individual, as users shall be held responsible for all computer transactions that are made with their user ID's and passwords. Passwords shall not be of the type that can easily be determined; shall not be recorded where they can easily be obtained; and shall be changed immediately upon suspicion that an unauthorized person is aware of the user's password.

.2 PERSONAL USAGE

- a. Employees, in general, are permitted incidental and minimal personal usage of IT resources if such usage does not adversely affect the program's operation or does not cause harm or embarrassment to the State.
- b. Personal use of IT resources by an employee shall not interfere with his/her job duties or the operations of the State.
- c. Good judgment shall be exercised in using the State's IT resources.

PSD P & PM	ACCEPTABLE USAGE OF IT RESOURCES POLICY	POLICY NO.: ADM.09.U.10
		EFFECTIVE DATE: APR 7 2011
		Page 7 of 13

- d. An employee is not authorized personal use of IT resources that results in expenses or charges to the State and an employee shall not engage in prohibited activities. Employees shall be responsible for the payment of any charges and any additional cost that is incurred as a result of their personal use.
- e. Users who engage in the personal use of the State's IT resources shall make it clear to all concerned that their activity or communication is not being sanctioned nor used for official State business.

.3 PROHIBITED ACTIVITIES

- a. State explicitly prohibits all activities that are in violation of any federal, State or other applicable laws, rules, regulations and established policies and procedures. Such activities include, but are not limited to:

1. UNAUTHORIZED PROCEDURES

- (a) Circumventing the security controls of the State's IT resources, including but not limited to, cracking other users passwords, decoding encrypted files, or using software application programs to secretly penetrate computer and information systems.
- (b) Accessing directories and files of other users in order to read, browse, modify, copy or delete any data or information without the explicit approval of the individual user and/or the PSD Director or designee.
- (c) Illegally copying materials that are protected under copyright law or from making such materials available to others for copying.
- (d) Illegally sending (uploading) materials that are protected under copyright law, including trade secrets, proprietary financial information or similar materials without the express prior approval from the PSD Director or designee.

PSD P & PM	ACCEPTABLE USAGE OF IT RESOURCES POLICY	POLICY NO.: ADM.09.U.10
		EFFECTIVE DATE: APR 7 2011
		Page 8 of 13

- (e) Illegally receiving (downloading) materials that are protected under copyright law, including trade secrets, proprietary financial information, or similar materials without the express prior approval from the PSD Director or designee.
- (f) Users who are unaware if the information is copyrighted, proprietary or otherwise inappropriate for transfer, shall resolve all doubts in favor of not transferring the information and consult with their supervisor or the PSD Director or designee.
- (g) Users are strictly prohibited from installing hardware such as, but not limited to, communication cards, memory boards and modems, and software such as commercial, shareware, and freeware, on any computer system without the express approval of the PSD Director or designee.

2. Users shall sign the Acceptable Usage of IT Resources form (see Attachment 1): before using, connecting, removing, performing, distributing or otherwise operating IT devices, systems or services such as, but not limited to, the following:

- (a) **Thumb/Flash/USB Portable Storage Devices**
Including portable storage devices that attach to the computer via a USB (Universal Serial Bus) connection or any other computer interface device or type.
- (b) **Wireless Connectivity**
Including all computing devices utilizing radio frequency, microwave frequency, or infrared frequency communications methods and technologies.
- (c) **Portable Computers**
Including Laptop, Sub-notebook, Tablet, or

PSD P & PM	ACCEPTABLE USAGE OF IT RESOURCES POLICY	POLICY NO.: ADM.09.U.10
		EFFECTIVE DATE: APR 7 2011
		Page 9 of 13

Portable Personal Computing devices or systems.

- (d) Internet
Via commonly available browsers such as Microsoft Internet Explorer, Mozilla Firefox, Apple Safari, and Opera.
- (e) Remote Terminal Access
Either via dial-up, LAN/WAN or wireless based access methods and terminal emulation and session emulation software applications.
- (f) Electronic Mail (E-mail)
Including the State's e-mail system, departmental e-mail and Internet e-mail accessed using State equipment.
- (g) Data Transfers and System Interfaces
Including all data transfers and systems interfaces to and from state computer systems and storage devices
- (h) Handheld Devices:
Including all State owned and State authorized cellular, wireless, mobile phones including PDA's, smart phones and iphones.
- (i) Magnetic Media
Including disk, tape, cartridge, library or disk/tape libraries or arrays.
- (j) CD and DVD
Including all storage media utilizing laser encoding methods and techniques.
- (k) Hard Copy
Including all hardcopy report output, compilations, publications, assembled and unassembled reports, and other confidential paper-based information generated by the State's computer system.

PSD P & PM	ACCEPTABLE USAGE OF IT RESOURCES POLICY	POLICY NO.: ADM.09.U.10
		EFFECTIVE DATE: APR 7 2011
		Page 10 of 13

- (l) Social Networks (e.g. Facebook and Twitter) including all online weblogs (BLOGS), discussion boards, bulletin board systems, forums and FAQ columns.
 - (m) Instant Messaging/Chat Including Microsoft Instant Messaging and other online chat and messaging services.
3. Users are strictly prohibited from using the State's IT resources for any personal or private financial gain, commercial or profit-making activities, and political, religious, or other solicitations.
4. Unlawful and Unethical Conduct
- (a) Users shall behave in a professional manner and shall exercise courtesy when using any electronic communication media.
 - (b) Exercise the same degree of care, judgment, and responsibility in composing and transmitting electronic communications as would be done when composing and sending written communication.
 - (c) Users shall strictly refrain from the usage of profanity and/or vulgarity when using any IT resources.
 - (d) Users shall assume that an electronic message will be saved and reviewed by someone other than the intended recipient(s).
 - (e) Users are strictly prohibited from using the State's IT resources to intentionally access, download from the Internet, display, transmit, or store any information that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, pornographic, violent, intimidating, libelous, defamatory or is otherwise unlawful, inappropriate, and offensive, including but not limited to, offensive

PSD P & PM	ACCEPTABLE USAGE OF IT RESOURCES POLICY	POLICY NO.: ADM.09.U.10
		EFFECTIVE DATE: APR 7 2011
		Page 11 of 13

material concerning gambling, sex, sexual orientation, race, color, national origin, religion, age, disability, or other characteristics that are protected by law.

- (f) The users departmental policies such as the sexual harassment, workplace violence, and equal employment opportunity and affirmative action policies shall apply fully to the use of IT resources. Users are strictly prohibited from any actions that may violate such policies while using the State's IT resources.
- (g) Users are strictly prohibited from making defamatory comments or taking actions such as forwarding of electronic mail that facilitate the publication or spread of such comments.
- (h) Users are strictly prohibited from sending, distributing or forwarding any and all e-mail via the State's electronic e-mail systems that the reasonable person would consider sexually explicit, profane, or offensive in any way, shape or form.
- (i) Users shall not attempt, subvert, engage in, or contribute to any activity that would compromise the security of the State's IT resources.
- (j) Users shall not deliberately crash, sabotage, or damage any computer system.
- (k) Users shall not use any software that is designed to destroy data, collect data, facilitate unauthorized access to information resources, or disrupt computing processes in anyway or use invasive software that may cause viruses or other damage or expense.

PSD P & PM	ACCEPTABLE USAGE OF IT RESOURCES POLICY	POLICY NO.: ADM.09.U.10
		EFFECTIVE DATE: APR 7 2011
		Page 12 of 13

5. THEFT

- (a) Users are strictly prohibited from removing any hardware, software, attached peripherals, supplies, and documentation without the express approval of the PSD Director or designee.

6. MISREPRESENTATION

- (a) Users are strictly prohibited from making unauthorized statements or commitments on behalf of the State or posting an unauthorized home page or similar web site.

4. DISCLAIMER OF LIABILITY FOR INTERNET USE

Users who access the Internet do so at their own risk. The State shall not be responsible for materials viewed or downloaded by users from the Internet. Users are cautioned that pages might contain offensive, sexually explicit, and inappropriate materials.

PSD P & PM	ACCEPTABLE USAGE OF IT RESOURCES POLICY	POLICY NO.: ADM.09.U.10
		EFFECTIVE DATE: APR 7 2011
		Page 13 of 13

APPROVAL RECOMMENDED:

Martha Torrey

Deputy Director for Administration

2/14/11

Date

John M. Hill

Deputy Director for Corrections

3/14/11

Date

[Signature]

Deputy Director for Law Enforcement

3/11/11

Date

APPROVED:

Jodie Maresca-Huata

Director

4/7/2011

Date

Policy No. ADM.09.U.10
Attachment I

ACCEPTABLE USAGE OF IT RESOURCES

ACKNOWLEDGEMENT FORM

I, _____ have read

Department of Public Safety Policy No. ADM.09.U.10 Acceptable Usage of IT Resources 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 Hawaii 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 Hawaii. 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 Hawaii 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

Department /Division: _____