	DEPARTMENT OF CORRECTIONS AND REHABILITATION DEPARTMENT ADMINISTRATION POLICY AND PROCEDURES	EFFECTIVE DATE: January 01, 2024	POLICY NO.: ADM.09U.10
		SUPERSEDES (Policy No. & Date): ADM.09U.10 of 04/07/2011	
	SUBJECT: ACCEPTABLE USAGE OF IT RESOURCE POLICY		Page 1 of 10

1.0 PURPOSE

The purpose of this policy is to define the acceptable and prohibitive usage of IT resources. These stipulations are necessary to minimize the risk to the Department of Corrections and Rehabilitation (DCR) 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 SCOPE

This policy applies to all employees of the DCR 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 DCR before accessing the State's IT resources.

3.0 REFERENCES, DEFINITIONS & FORMS

.1 References

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

.2 Definitions

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

NOT CONFIDENTIAL

DCR P & P M	SUBJECT:	POLICY NO.:
	ACCEPTABLE USAGE OF IT RESOURCE POLICY	ADM.09U.10
		EFFECTIVE DATE: January 01, 2024
		Page 2 of 10

- b. "ITS" is the DCR Information Technology Systems unit responsible for managing the Information Technology resources of the Department.
- c. "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.
 - 1. Social Security Number
 - 2. Driver's license number or Hawaii Identification card number
 - 3. Account number, credit or debit card numbers, access code, or password that would permit access to an individual's financial account.
 - 4. Date of birth
 - 5. Home/work/mobile phone numbers and personal mail addresses.
 - 6. Personal data also includes information described in Chapter 92F-14 of the Hawaii Revised Statutes. Encrypted email is not secure transmissions.
- d. "User" means all State employees in the DCR including all outside personnel. Outside personnel includes but is not limited to, employees from other agencies, volunteers, contractors, and vendors who are authorized to use or access State IT resources.

4.0 POLICY

.1 General Terms

a. Management Information Systems

The DCR, ITS 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.

NOT CONFIDENTIAL

DCR P & P M	SUBJECT: ACCEPTABLE USAGE OF IT RESOURCE POLICY	POLICY NO.: ADM.09U.10
		EFFECTIVE DATE: January 01, 2024
		Page 3 of 10

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

.2 Users Responsibility

- a. 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 DCR's Office of Personnel. Questions related to the technical aspects of the IT resources may be directed to the DCR's ITS office and/or DCR's designated office.
- b. Avoid deliberately performing acts that waste IT resources or unfairly monopolize resources to the exclusion of others. Such acts include but are 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.
- c. Avoid copying and/or downloading audio, video, and picture files, unless these actions are work-related.
- d. Users should routinely delete outdated and unnecessary computer files to free up IT resources to help keep systems running more efficiently and smoothly.

NOT CONFIDENTIAL

DCR P & P M	SUBJECT: ACCEPTABLE USAGE OF IT RESOURCE POLICY	POLICY NO.: ADM.09U.10
		EFFECTIVE DATE: January 01, 2024
		Page 4 of 10

- e. Users have the responsibility to act lawfully, ethically, respectfully, and responsibly in the use of the State's IT resources.
- f. Maintain the confidentiality of classified materials including personal data.
- g. 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.
- h. Immediately report an encounter or receipt of unlawful, unethical, or questionable materials to a supervisor or the DCR designee.
- i. Take all reasonable precautions to protect the State's IT resources from unauthorized access, use, disclosure, modification, duplication and/or destruction.
- j. Assist and cooperate in the protection of the IT resources and follow DCR 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.
- k. 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.

.3 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.

NOT CONFIDENTIAL

DCR P & P M	SUBJECT: ACCEPTABLE USAGE OF IT RESOURCE POLICY	POLICY NO.: ADM.09U.10
		EFFECTIVE DATE: January 01, 2024
		Page 5 of 10

- c. Good judgment shall be exercised in using the State's IT resources.
- d. An employee is not authorized for 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 because 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.

.4 Prohibited Activities

- a. The 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 DCR 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 DCR Director or designee.

NOT CONFIDENTIAL

DCR P & P M	SUBJECT: ACCEPTABLE USAGE OF IT RESOURCE POLICY	POLICY NO.: ADM.09U.10
		EFFECTIVE DATE: January 01, 2024
		Page 6 of 10

- e) Illegally receiving (downloading) materials that are protected under copyright law, including trade secrets, proprietary financial information, or similar materials without expressed prior approval from the DCR 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 DCR 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 DCR 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 Portable Personal Computing devices or systems.

NOT CONFIDENTIAL

DCR P & P M	SUBJECT: ACCEPTABLE USAGE OF IT RESOURCE POLICY	POLICY NO.: ADM.09U.10
		EFFECTIVE DATE: January 01, 2024
		Page 7 of 10

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, and mobile phones including PDAs, smartphones, 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.

NOT CONFIDENTIAL

DCR P & P M	SUBJECT: ACCEPTABLE USAGE OF IT RESOURCE POLICY	POLICY NO.: ADM.09U.10
		EFFECTIVE DATE: January 01, 2024
		Page 8 of 10

l) Social Networks (e.g., Facebook and Twitter) including all Online weblogs(SLOGS), 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 material concerning gambling, sex, sexual orientation, race, color, national origin, religion, age, disability, or other characteristics that are protected by law.

NOT CONFIDENTIAL

DCR P & P M	SUBJECT: ACCEPTABLE USAGE OF IT RESOURCE POLICY	POLICY NO.: ADM.09U.10
		EFFECTIVE DATE: January 01, 2024
		Page 9 of 10

- f) The user's departmental policies such as sexual harassment, workplace violence, 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 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-mails via the State's electronic 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, disrupt computing processes in any way, or use invasive software that may cause viruses or other damage or expense.

5. Theft:

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

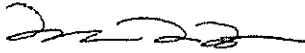
6. Misrepresentation:

Users are strictly prohibited from making unauthorized statements or commitments on behalf of the State or posting an unauthorized home page or similar website.

NOT CONFIDENTIAL

DCR P & P M	SUBJECT: ACCEPTABLE USAGE OF IT RESOURCE POLICY	POLICY NO.: ADM.09U.10
		EFFECTIVE DATE: January 01, 2024
		Page 10 of 10

APPROVAL RECOMMENDED:



JAN 0 1 2024

Deputy Director for Administration

Date

APPROVED:



JAN 0 1 2024

DIRECTOR

Date

NOT CONFIDENTIAL