	DEPARTMENT OF CORRECTIONS AND REHABILITATION **DEPARTMENT ADMINISTRATION POLICY AND PROCEDURES**	**EFFECTIVE DATE:** **January 01, 2024**	**POLICY NO.:** **ADM.09X.10**
		SUPERSEDES (Policy No. & Date): **NEW**	
	GENERAL SECURITY POLICY		**Page 1 of 5**

1.0 PURPOSE

The Hawaii Department of Corrections and Rehabilitation (DCR) Security Information Technology Policies are documented in the DCR Policies Manual Chapter 9, entitled Information Technology Security, and is maintained by the Management Information System Unit.

The DCR IT Security Policies will apply to all DCR divisions, Branches, Staff Offices, and attached agencies. All references to "DCR staff" in the DCR IT Security Policies will refer to these components. These DCR IT Security Policies will address appropriate and reasonable IT industry security practices for the IT Systems and for the DCR 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 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 outside 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. DHS Policy & Procedure 8.2.01 August 23, 2006.

.2 Definitions:

a. "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."

NOT CONFIDENTIAL

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

c. "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.

d. "ITS" is the DCR Information Technology Systems unit responsible for managing the Information Technology resources of the Department.

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

f. "Security Measure" is similar to safeguard.

g. "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:

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 DCR policies and applicable State and Federal laws, regulations, and rules, related to the privacy and security of such information.

.2 Requirements:

a. Policies and Procedures: The DCR will implement IT Security policies and procedures that will guide the Department to protect its electronic confidential information.

b. Flexibility of Approach: The DCR 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 DCR must implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic confidential information that it creates, receives, maintains, and transmits.

d. Ensure External Agencies Safeguards: The DCR 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 DCR 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.

f. Consistency of Policies: The DCR 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.

5.0 PROCEDURES

General Provisions:

.1 Permissions 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 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.

.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 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.

DCR P & P M	SUBJECT: GENERAL SECURITY POLICY	POLICY NO.: ADM.09X.10 EFFECTIVE DATE: January 01, 2024 Page 5 of 5

APPROVAL RECOMMENDED:

JAN 0 1 2024

Deputy Director for Administration Date

APPROVED:

JAN 0 1 2024

DIRECTOR Date

NOT CONFIDENTIAL