	<b>DEPARTMENT OF CORRECTIONS AND REHABILITATION</b> <b>DEPARTMENT ADMINISTRATION POLICY AND PROCEDURES</b>	<b>EFFECTIVE DATE:</b> January 01, 2024	<b>POLICY NO.:</b> ADM.09X.20
		<b>SUPERSEDES (Policy No. &amp; Date):</b> AM.09X.20 of April 07, 2011	
<b>SUBJECT:</b> <b>NETWORK SECURITY POLICY</b>		Page 1 of 5	

## 1.0 PURPOSE

The purpose of the Department of Corrections and Rehabilitation (DCR) Network Security Policy is to establish the rules for the maintenance, expansion, and use of the network infrastructure and to prevent any unauthorized use of Information Technologies (IT) resources. These stipulations are necessary to preserve the integrity, availability, and confidentiality of DCR information.

The DCR network infrastructure is the central utility for all users of DCR Management IT. It is important that the infrastructure, which includes cabling and the associated equipment such as routers and switches continues to develop with sufficient flexibility to meet user demands while at the same time remaining capable of capitalizing on anticipated developments in high-speed networking technology to allow the future provision of enhanced user services.

The use of the State's 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 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. ETS DOC No. 509 (Secure Access Policy – Next Generation Network).
- b. DHRD Policy No. 103.001 (Acceptable Usage of Information Technology Resources).

**NOT CONFIDENTIAL**

DCR P & P M	<b>SUBJECT:</b>  <b>NETWORK SECURITY POLICY</b>	<b>POLICY NO.:</b> ADM.09X.20
		<b>EFFECTIVE DATE:</b> January 01, 2024
		Page 2 of 5

.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, server, Local Area Network ("LAN"), Wide Area Network ("WAN") and personal computers.
- b. "ITS" is the DCR Information Technology Systems unit responsible for managing the IT resources of the Department.
- c. "Remote Access" any user accessing the State DCR network through a network device or medium outside of DCR via the internet.
- d. "User" means all State employees in the DCR including all outside personnel. Outside personnel includes, but is not limited to, volunteers, contractors, and vendors who are authorized to use or access State IT resources.

**4.0 POLICY**

.1 General Terms:

- a. ITS is responsible for the DCR network infrastructure and will continue to manage further developments and enhancements to this infrastructure.
- b. ITS is responsible for providing a dependable network infrastructure capable of supporting future departmental growth, all cabling must be installed by ITS or an approved contractor.
- c. All network-connected equipment must be configured to a specification approved by ITS.
- d. All hardware connected to the network is subject to ITS management and monitoring standards.
- e. All changes or configurations to the network shall only be done by ITS.

**NOT CONFIDENTIAL**

DCR P & P M	<b>SUBJECT:</b>  <b>NETWORK SECURITY POLICY</b>	<b>POLICY NO.:</b> ADM.09X.20
		<b>EFFECTIVE DATE:</b> January 01, 2024
		Page 3 of 5

- f. The network infrastructure supports a well-defined set of approved networking protocols. ITS must approve any use of non-sanctioned protocols.
- g. All network devices including routers, switches, modems, and ITS equipment must be protected and secured from non-DCR individuals.
- h. The networking addresses for the supported protocols are allocated, registered, and managed centrally by ITS.
- i. Firewalls shall be installed, configured, and managed by ITS.
- j. No router, switch, hub; or wireless access point is allowed to connect to the DCR network without the written approval of ITS.
- k. Only ITS or vendors with written ITS approval can install network hardware or software that provides network services.
- l. ITS shall be responsible for securing the network to ensure users do not violate any State policies, perform illegal activities, and do not use IT resources outside of business interests.
- m. DCR users shall be responsible for and subject to any consequences should any access be misused.

**.2 Requirements:**

- a. Network access must be strictly controlled. Control will be enforced via password authentication.
- b. ITS will create and manage all network operations and securities.
- c. ITS will have available up-to-date anti-virus scanning software for the removal and scanning of suspected viruses.

**NOT CONFIDENTIAL**

DCR P & P M	<b>SUBJECT:</b>  <b>NETWORK SECURITY POLICY</b>	<b>POLICY NO.:</b> <b>ADM.09X.20</b>
		<b>EFFECTIVE DATE:</b> <b>January 01, 2024</b>
		<b>Page 4 of 5</b>

## 5.0 PROCEDURES

### General Provisions:

a. 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.

b. 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.

c. No Exceptions 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 the prior consent of the users.

d. Monitoring and Enforcement:

1. 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.

**NOT CONFIDENTIAL**

DCR P & P M	SUBJECT:  <b>NETWORK SECURITY POLICY</b>	POLICY NO.: <b>ADM.09X.20</b>
		EFFECTIVE DATE: <b>January 01, 2024</b>
		<b>Page 5 of 5</b>

2. The State has the right to monitor, review, audit, and/or disclose all 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 or uploaded by Users.

e. 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.

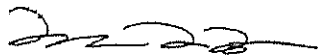
f. Policy Violation:

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.

g. 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.

APPROVAL RECOMMENDED:



**JAN 0 1 2024**

Deputy Director for Administration

Date

APPROVED:



**JAN 0 1 2024**

DIRECTOR

Date

**NOT CONFIDENTIAL**