1.0 PURPOSE

The use of the State's Information Technology Remote Access 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. This policy is written for remote access into the Department of Corrections and Rehabilitation (DCR) system by the Department's Information Technology Systems (ITS) Staff and authorized outside employees.

The purpose of this policy is to define standards for connecting to the DCR network from any outside host and to prevent any unauthorized use of IT resources.

2.0 SCOPE

This policy applies to all DCR employees and third parties who are authorized to remotely connect to the DCR network to use or access DCR's information technology resources for business purposes. Types of remote access include:

.1 Systems Administration: ITS Personnel who are authorized to perform remote administration of information technology systems.

.2 Non-DCR Employees: employees from outside agencies, volunteers, contractors, and vendors who have written authorization from ITS.

3.0 REFERENCES, DEFINITIONS & FORMS

.1 References:

DHRD Policy No. 103.001: Acceptable Usage of Information Technology Resources. https://dhrd.hawaii.gov/wp-content/uploads/2023/02/0103001-021323.pdf.

.2 Definitions:

a. "Agency" refers to any State, Federal, or City entity.

b. "IT resources" means all hardware, software, documentation, programs, information, 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.

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

d. "Remote Access" any user accessing the State DCR network through a network device or medium outside of DCR via the internet.

e. "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. Outside Agencies and Users shall read and sign this policy entitled Remote Access Security Policy. DCR approval must be granted before any remote access will be allowed.

b. It is the responsibility of the User with remote access privileges to DCR's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to DCR.

c. The User shall be responsible for all non-authorized users in that they do not violate any State policies, do not perform illegal activities, and do not use the access outside of business interests. DCR employees are responsible for the consequences should the access be misused.

.2 Requirements:

a. Users shall follow all DCR Remote Access Procedures when connecting to the network.

b. All personal computers that are connected to the DCR internal network via remote access technologies must use the most up-to-date anti-virus.

c. Secure remote access must be strictly controlled. Control will be enforced via password authentication.

d. This remote access right is granted only to the user who has been given permission and no one else.

e. At no time should any user provide their login or email password to anyone.

f. Users with remote access privileges must ensure that their personal computers or workstations, which are remotely connected to the DCR network, are not connected to any other network at the same time, with the exception of the personal network that is under the complete control of the user.

5.0 PROCEDURES

.1 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 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.

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.

6.0 AGREEMENT

a. Acceptance of Terms and Conditions:

1. DCR occasionally provides users, and outside personnel including employees from outside agencies, volunteers, vendors, and contractors, with authorized remote access to the DCR network for work or project-related business.

2. User agrees and understands that it is voluntary to utilize any personal equipment, telephone line, and/or Internet service in the course of remotely, maintaining, assisting, and servicing DCR from a remote location such as home or at any other locations outside of DCR. The User shall understand that they will not be compensated for any damage or usage of personal property, such as personal equipment, telephone line, or internet connection services. DCR is not responsible for working on any employee-owned equipment.

3. The User is solely responsible for any claims, damages, or liability in connection with the User's remote access, including, but not limited to interruption of service, loss of data, or unauthorized release or acquisition of data, and further agrees to work with DCR to mitigate the effects of any service interruption or loss of data to the satisfaction of DCR.

b. Scheduling and Scope of Service:

Upon receiving proper authorization for remote access for the DCR System, DCR ITS will work with the outside agency to set up the remote access.

c. Limitations of Liability:

DCR's divisions, branches, and staff shall not be liable for any direct, indirect, punitive, incidental, special, or consequential damages, whether foreseeable or unforeseeable, based on claims (including, but not limited to, claims for damages for loss of profits or loss of business opportunities, the provision of or failure to provide services, mistakes, omissions, interruptions, deletion or corruption of files, errors, or defects) arising out of or in any way connected with the remote access granted to an Agency whether based on contract, tort, strict liability or otherwise.

d. No Unlawful or Prohibited Use:

As a condition of the user's remote access to DCR computing equipment, the user represents and warrants that they will not attempt to access any application other than the one(s) designated in this Remote Access Agreement.

e. Verification and Monitoring of Work:

All work performed by the Agency while connected to the DCR computing application is subject to monitoring and verification by DCR.

f. General Provision:

Agreements and any documents referenced herein constitute the entire agreement between DCR and said Agency pertaining to the subject matter hereof and it supersedes all prior or contemporaneous communications and proposals, whether electronic, oral, or written, between the DCR and Agency.

APPROVAL RECOMMENDED:

JAN 0 1 2024

Deputy Director for Administration Date

APPROVED:

JAN 0 1 2024

DIRECTOR Date