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 Hawai'i. 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 the remote access into the Department of Public Safety (PSD) system by the Department's Management Information System (MIS) Staff and authorized outside employees.

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

2.0 REFERENCES

3.0 DEFINITIONS

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

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

"Remote Access" is when a user accesses the State PSD network through a network device or medium outside of PSD via Internet.

"User" means all State employees in the PSD including all outside personnel. Outside personnel include, but not limited to, volunteers, contractors, and vendors who are authorized to use or access State IT resources.

4.0 SCOPE

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

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

.2 Non-PSD Employees: employees from outside agencies, volunteers, contractors, and vendors who have a written authorization from MIS.

5.0 GENERAL PROVISIONS

.1 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.

.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 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 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, 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. Outside Agency's and Users shall read and sign this policy entitled Remote Access Security Policy. PSD approval must be granted before any remote access will be allowed.

b. It is the responsibility of the User with remote access privileges to PSD's network to ensure that their remote

access connection is given the same consideration as the user's on-site connection to PSD.

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. PSD employees are responsible for the consequences should the access be misused.

.2 REQUIREMENTS

a. User shall follow all PSD Remote Access Procedures when connecting to the network.

b. All personal computers that are connected to PSD 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 to only 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 is remotely connected to PSD network, is not connected to any other network at the same time, with the exception of personal network that are under the complete control of the user.

7.0 AGREEMENT

.1 ACCEPTANCE OF TERMS AND CONDITIONS

The State of Hawai'i, PSD occasionally provides users, and outside personnel including employees from outside agencies, volunteers, vendors and contractors, an authorized remote access to PSD network for work or project related business.

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 PSD from a remote location such as home or at any other locations outside of PSD. The user shall understand that they will not be compensated for any damages or usages to personal property, such as personal equipment, telephone line or Internet connection services. PSD is not responsible for working on any employee owned equipment.

The user is solely responsible for any claims, damages or liability in connection with 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 PSD to mitigate the effects of any service interruption or loss of data to the satisfaction of PSD.

.2 SCHEDULING AND SCOPE OF SERVICE

Upon receiving proper authorization for remote access for the PSD System, PSD MIS will work with the outside agency to setup the remote access.

.3 LIMITATIONS OF LIABILITY

PSD'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.

.4 NO UNLAWFUL OR PROHIBITED USE

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

.5 VERIFICATION AND MONITORING OF WORK

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

Policy No. ADM.09X.30
Attachment I

REMOTE ACCESS SECURITY POLICY ACKNOWLEDGEMENT FORM

I, _____ have read

Department of Public Safety Policy No ADM.09.X.30 Remote Access Security 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 Hawai'i 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 Hawai'i. 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 Hawai'i 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.

Applications Requested:	
(1)	(3)
(2)	(4)
Start Date:	End Date:

_____ _____
Signature Date

_____
Print Name

APPROVAL AND AUTHORIZATION

Branch Administrator:	_____ Name	_____ Signature	_____ Date
MIS Officer:	_____ Name	_____ Signature	_____ Date
Deputy Director:	_____ Name	_____ Signature	_____ Date