1.0 PURPOSE

The purpose of the Department of Public Safety (PSD) 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 PSD information.

The PSD network infrastructure is the central utility for all users of PSD 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 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.

2.0 REFERENCES

3.0 DEFINITIONS

"IT resources" means all hardware, software, documentation, programs, information, bandwidth, 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 IT resources of the Department.

"Remote Access" any user accessing 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 includes, 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 employees of the PSD 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 PSD before accessing the State's IT resources.

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 or 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 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.

.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. MIS is responsible for the PSD network infrastructure and will continue to manage further developments and enhancements to this infrastructure.

b. MIS is responsible to provide a dependable network infrastructure capable to support future departmental growth, all cabling must be installed by MIS or an approved contractor.

c. All network-connected equipment must be configured to a specification approved by MIS.

d. All hardware connected to the network is subject to MIS management and monitoring standards.

e. All changes or configuration to the network shall only be done by MIS.

f. The network infrastructure supports a well-defined set of approved networking protocols. MIS must approve any use of non-sanctioned protocols.

g. All network devices Including routers, switches, modems and MIS equipments must be protected and secured from non PSD individuals.

h. The networking addresses for the supported protocols are allocated, registered and managed centrally by MIS.

i. Firewalls shall be installed, configured and managed by MIS.

j. No router, switch, hub, or wireless access point is allowed to connect to the PSD network without the written approval of MIS.

k. Only MIS or vendors with written MIS approval can install network hardware or software that provides network services.

l. MIS shall be responsible to secure the network to ensure users do not violate any State policies, perform illegal activities, and does not use IT resources outside of business interests.

m. PSD 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. MIS will create and manage all network operations and securities.

c. MIS will have available up to date anti-virus scanning software for the removal and scanning of suspected viruses.

APPROVAL RECOMMENDED:

Deputy Director for Administration — Date: 2/14/11

Deputy Director for Corrections — Date: 3/16/11

Deputy Director for Law Enforcement — Date: 3/11/11

APPROVED:

Director — Date: 4/7/2011

Policy No. ADM.09.X.20
Attachment I

NETWORK SECURITY POLICY

ACKNOWLEDGEMENT FORM

I, _____ have read

Department of Public Safety Policy No: ADM.09.X.20 Network 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 Hawaii. 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 Hawaii 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.

_____ _____
Signature Date

_____
Print Name

Department /Division: _____

PSD 2008 (4/2010)