Number: 08.04

STATE OF HAWAII

1959

UA·MAU·KE·EA·O·KA·AINA·I·KA·PONO

NETWORK SECURITY

December 2003

TABLE OF CONTENTS

Number: 08.04
Effective: 12/01/2003

Department of Accounting and General Services
Information and Communication Services Division

Information Technology Standards

1 INTRODUCTION

This document is identified as IT Standards, 08.04 in the State of Hawaii IT Standards publication. It addresses the basic issues related to securing the State's Network and safeguarding information assets that use the Network.

1.1 Network Security Overview

The purpose, scope, definition of terms, and summary overview for information security are presented in IT Standards, 08.01, Information Technology Security Overview.

The definition of the State's network is repeated here because it is so closely bound to this document. The term "Network" (with a capitol "N") refers to the hardware and associated software that is managed by or under the control of the Information and Communication Services Division (ICSD). The Network is used for information transport and access, and inter-agency, intra-agency or extra-agency electronic communication.

1.2 Exclusions

This document is limited to standards concerned with the security of the State Wide Area Network (WAN) which is under the operational control of ICSD. For standards relating to information stored in computer systems, refer to IT Standards, 08.02 Information Security, or 08.03, Personal Computer Security.

1.3 Comments and Suggestions

Any State of Hawaii Information Technology Standards document, reference manual or users guide mentioned in this document are available through the departmental user agency data processing coordinator (DP Coordinator). Standards are also accessible on-line by clicking on Information Technology Standards on the ICSD home page at:

http://www.hawaii.gov/dags/icsd/

Statewide Forms are accessible on-line at Forms Central on the Government in Hawaii home page at:

http://www.hawaii.gov/forms/

Comments, recommendations, proposals, or suggestions regarding the contents of this document may be sent either via email to icsd.admin.ppmo@hawaii.gov or in writing to:

Information and Communication Services Division
Project Planning and Management Office
1151 Punchbowl Street, B10
Honolulu, Hawaii 96813-3024

2 NETWORK SECURITY RESPONSIBILITIES

The areas of responsibilities for the security of information that use the Network as a means to transport information are specified in State of Hawaii IT Standards 08.02, Information Security and are not repeated here. They include the reference to the Hawaii Revised Statutes, Chapter 92-E, Fair Information Practice, (Confidentiality of Personal Record).

2.1 Network Security Administrator

The Network Security Administrator is the person within ICSD who is responsible for the Network security administration functions. The Network Security Administrator may delegate Network security duties and tasks.

Network Security Administrator responsibilities apply to the Network and include:

a. Ensuring the security of the State's information assets that pass through the Network.

b. Ensuring the physical security of Network equipment under the control of ICSD.

c. Installing, upgrading, managing, maintaining, and ensuring the security software which runs on VPN concentrators, routers, and other Network equipment under the control of ICSD Networking.

d. Managing, assigning, and maintaining the list of network addresses.

e. Maintaining an inventory list of computers, terminals, PCs, modems and other access devices attached to the Network. This Network Hardware Inventory List is to include only devices that are physically attached directly to the Network.

f. Providing the Security Administrator (see IT Standards 08.02, Section 3.5, Security Administrator, with an updated copy of the Network Hardware Inventory List on an annual basis or upon request as the need arises.

3. NETWORK ACCESS AND ATTACHMENT

To ensure that Network security responsibilities for information assets are effective and maintained, the following standards are established for networks under the operational control of ICSD.

3.1 Network Equipment

a. Network equipment, which is the property of ICSD and is located or housed at an agency, is not available for agency internal use without prior approval of the ICSD Network Security Administrator.

b. ICSD is responsible for Network equipment up to the media termination of the Network. Agency equipment responsibility starts at and includes any cables that connect the agency's firewall or Virtual Local Area Network (VLAN) router to the Network.

c. The connection from an agency's internal network to the Network must be through a firewall that is owned, maintained and managed by the agency. All Network security policies will be implemented on the agency's firewall.

d. An agency is responsible to ensure that no security breaches occur onto the Network because of public or private access granted to its own internal network or through an entry point into its network.

3.2 Network Software

a. The management of Network equipment configurations and of facility requirements is the responsibility of ICSD. Suggested changes to these may be communicated to ICSD. ICSD is responsible for effecting such changes.

b. An agency is responsible to ensure that no security breaches occur onto the Network because of access granted by ICSD to its users.

c. An agency is responsible to ensure the proper download, installation, upgrade, maintenance, and use of VPN client and other software required by users to securely access the Network.

3.3 Network Addresses

a. ICSD is responsible for assigning the internal Network addresses t an agency.

b. The internal Network address is to be used by an agency for all traffic directed within the Network.

c. An agency is responsible for the translation of all addresses on its own internal networks to its assigned Network address.

d. Specific addresses that are managed by ICSD are reserved for Network use and operating requirements.

3.4 Network Monitoring

a. Network activity will be routinely monitored, logged, and audited for compliance with security policy, for improving response time, and for administrative and management purposes.

b. Information and data entering the Network is subject to inspection for nuisance and malicious code. Such inspection shall include, but is not necessarily limited to scanning for virus, Trojan horse, and macro infections.

4 INTERNET ACCESS

To ensure that access to/from information assets is secure, efficient and effective, the following standards are established for use of networks under the operational control of ICSD.

4.1 Address Management

a. Coordinating, assigning, and managing of Network addresses is done through the Network Security Administrator.

b. Addresses previously assigned to an agency may be recovered by ICSD, where appropriate.

4.2 Outbound Access to the Internet

a. Agency access through the Network firewall to the Internet is subject to address translation.

b. It is the sole responsibility of the Agency to manage and ensure the security of direct Internet connections.

c. All traffic from an agency to the Internet that originates from an access device within the Network must be directed to the Network firewall or to the agency's firewall.

d. Requests to enable access to the Internet from a Network enabled device are to be submitted to and approved by the ICSD Administrator. Such requests will be forwarded to the ICSD Security Administrator for appropriate processing.

4.3 Inbound Access from the Internet

a. Inbound access from the Internet to an agency through the Network firewall must follow security policies and requires coordination with ICSD. (See IT Standards, 08.01, Information Security Overview; and 08.02, Information Security.)

b. The ICSD Security Administrator will handle the coordination of the review of such requests.

c. Only traffic directed to the public address blocks assigned to an agency by ICSD will be forwarded to the agency for the Network Internet connection.

4.4 Virtual Local Area Networks (VLAN)

a. Communication via the Network between parts of an agency that are in physically separate locations is allowed but must be transmitted through a routed interface.

b. VLAN connectivity to the Network must follow guidelines and policies established by ICSD. The guidelines take into account the purpose of the VLAN and may require a router (or Layer 3 switch), firewall, or neither one, depending upon the situation.