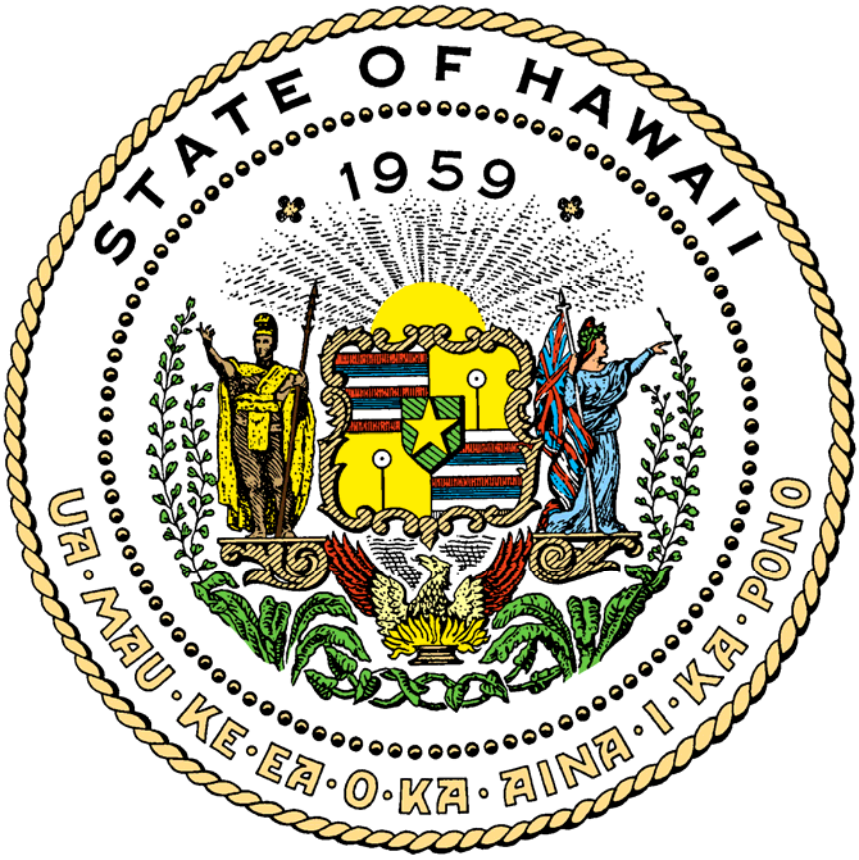
Number: 08.01



INFORMATION SECURITY OVERVIEW

December 2003

TABLE OF CONTENTS

Department of Accounting and General Services
Information and Communication Services Division
Information Technology Standards

1 INTRODUCTION

This is the Information Security Overview document within the State of Hawaii Information Technology Standards (IT Standards) developed by the Department of Accounting and General Services (DAGS), Information and Communication Services Division (ICSD). The IT Standards is a publication of the State of Hawaii, Executive Branch. It contains policies, responsibilities, and guidelines pertaining to computer assets under the operational control of DAGS.

1.1 Security Policy Highlights

This section provides a recap of the Information Security and Network Security policies. This document is designed to be a quick reference to present the intent of these policies. For the comprehensive details of the policies, refer to IT Standards 08.01, Information Security and 08.04, Network Security.

1.1.1 Information Security Policy Recap

- A User must have his own Logon-ID and password to access information.
- Logon-ID/Password is to be used only by the person to whom it is assigned.
- Passwords will expire on a regular basis.
- Users will be logged off for terminal inactivity.
- Remote dial-in/dial-out access requires prior approval.
- Logon-IDs that are not used will be deleted.
- Production files are not allowed to be used for testing.
- Files downloaded and install diskettes must be scanned for viruses.
- Systems for internal use by State employees will be protected by a firewall.
- The Owner is the agency that specifies the information content.
- The Owner determines the sensitivity of information and who can access it.
- Access to information is contingent upon compliance with security policies.
- Identification and authentication of users is required to grant access via the Internet to systems that are for internal use by State personnel.
- Approval is required for Users and Information to pass through the Network.
- Network and computer User activity are monitored, logged, and audited.

- Information entering the Network is inspected to ensure security.

1.1.2 Network Policy Recap

- Network equipment that belongs to ICSD will be managed by ICSD, even though it is physically housed at an agency site.
- ICSD issues, controls, and manages Network addresses, configurations, and facilities.
- An agency must use its assigned address to traverse the Network.
- ICSD is responsible for Network equipment up to the media termination.
- Agency responsibility starts at cables at its site that connect the Agency to the Network.
- Previously assigned addresses may be relinquished to ICSD in order to use the Network to access the Internet.
- The ICSD Administrator is the approving authority for granting Internet access from devices within the Network.
- Access to the Internet originating from within the Network must go through the Network firewall.

1.2 Computer Assets

The following types of security for computer assets are addressed:

a. Security for assets stored in electronic files housed in mainframe computers, mini-computers, servers, personal computers, and computer networks.

b. Physical security for computer hardware, associated equipment, and facilities used to process, store, manipulate, and transmit information.

c. Security for Network equipment and associated software used for the transport of or access to information. This includes the security of electronic messages and communications.

1.3 Terms and Definitions

The definitions for the terms such as "policy," "procedure," "standard," "convention" and "guideline" are contained in IT Standards Number 01.01, Standards for Writing Manuals.

For ease of reference, some of the more prevalent terms used in the Information Security Standards documents are listed below.

Agency. A department, office, commission, board, or other identifiable entity within the organizational structure of the State.

Central site. The primary location at which the mainframe computer and mini-computer hardware is housed and application information is processed. Currently this is in the Kalanimoku Building, 1151 Punchbowl Street, Honolulu, Hawaii.

Computer system. The computer hardware and associated operating software that are used for the processing, storing, accessing, and manipulation of data and other information.

Information assets. Information stored as data, image, text, video, or voice. Software used to process such information. Components and technologies within State or vendor supplied information processing equipment, terminals, computer systems, application systems, networks, supporting facilities, and information processing services.

Logon-ID. The identification code that is used to grant access to computer systems or information is referred to by various names throughout the Information Technology industry. Among these are: the "User Identification Code" (UID), the user "Logon-Identification" (Logon-Id, Logon-ID, logon or ID), and "Accessor ID" (ACID). All these terms are considered synonymous. For simplicity and clarity, hereafter, the term Logon-ID is used to designate the identification code for accessing information on a computer system.

Network. The hardware and associated software that is managed by or under the control of ICSD. The Network is used to transport and to access information. It is also used for electronic messaging and communication within, between, and among agencies. To distinguish between the generic use of the word network, the term begins with a capitol "N" when used in reference to the equipment or processes mentioned above.

System. Unless otherwise specified, "system" refers to the application software, programs, and support documentation designed for the manipulation of information or data for specific areas such as tax, accounting, inventory, budgeting, etc.

Virtual Local Area Network or
Virtual Private Network. A network comprised of parts which are located in two or more physically separate locations and which uses communication lines external to

the network to establish communication between the parts. At the time when communication is established, software is invoked to secure the communication so that the parts function as if they are physically located at one site.

1.4 Abbreviations and Acronyms

CSL	Computer Security Liaison
DAGS	Department of Accounting and General Services
H.A.R.	Hawaii Administrative Rules
HRS	Hawaii Revised Statutes
ICSD	Information and Communication Services Division, DAGS
IT	Information Technology
PC	Personal Computer
PSB	Production Services Branch of ICSD, DAGS
SEC	System Security Section of ICSD, DAGS
SSB	Systems Services Branch of ICSD, DAGS
TSB	Telecommunication Services Branch of ICSD, DAGS
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

2 INFORMATION SECURITY OVERVIEW

IT Standards pertaining to security address the issues needed to safeguard, protect, and secure the State's information assets.

2.1 Purpose

IT Standards security documents define the position of DAGS regarding the security of information, programs, software, and files stored in computers or transiting the networks for which DAGS is responsible.

It is the intent of the IT Security Standards to:

a. Define the roles and responsibilities of user and IT;

b. Establish the minimum security requirements for the protection of the State's information assets;

c. Prevent the misuse and loss of information assets;

d. Formulate the basis for audits and self-assessment;

e. Preserve the State's management options and legal remedies for asset loss or misuse.

2.2 Scope

The IT security policies, standards and procedures presented in these IT Standards apply to all information assets and services under the jurisdiction or control of ICSD, including product support, field support and process control.

2.3 Applicability

The IT Security Standards apply to:

a. Any person responsible for analyzing, designing, developing, implementing, and/or maintaining application systems or programs;

b. Any person responsible for analyzing, designing, developing, installing, implementing, and/or maintaining computer operating systems software, support programs, and networks;

c. Any user of the State information processing hardware, software, networks, facilities, or resources;

d. Any owner or user of the State's information assets;

e. Any individual making inquiry only access of the State's information assets;

f. Any vendor that supplies computer and/or related services to the State;

g. Any person who is responsible for developing, implementing, or maintaining data processing standards, procedures, conventions, or guidelines.

2.4 Information Technology Security Content

The IT Standards security documents contain the basic policy statements that must be followed when designing, developing, and implementing electronic solutions that manipulate, make available, or access information assets to satisfy the needs of the State or the mandates of the Executive, Judiciary, and Legislative branches of the State government.

The IT Standards that address IT security comprise Chapter 8 of the IT Standards. These Standards address acceptable use, information security, physical security, personal computer security, and network security.

2.4.1 Information Security Content

IT Standards, 08.02 Information Security provides the standards that are necessary to ensure the security and integrity of software, programs, and information which passes through or is housed on PCs, servers, networks, mini-computers, and mainframe computers.

The areas of responsibility defined for ensuring the security of the State's information assets are listed below. These areas are covered in detail in IT Standards 08.02, Information Security. The areas are:

1. Owner
2. Computer Security Liaison
3. Custodian
4. User
5. Security Administrator

IT Standards 08.02 also provides the security policies that will be followed when designing systems and requesting access to computer resources that are under the administrative control of ICSD.

2.4.2 Network Security Content

IT Standards 08.04, Network Security, provides the policies, standards and procedures that are necessary to ensure the physical security and integrity of network hardware, equipment, and software.

IT Standards 08.04 also provides the physical security procedures that will be followed when individuals use computer resources that are under the administrative control of ICSD.

2.5 Security Policy Responsibilities

ICSD is tasked with encouraging user friendly access to electronically stored information assets by providing connectivity between computer systems and networks. ICSD must also provide sufficient security to safeguard information

assets and prevent actual and/or potential security breaches of the information resources under its protection.

ICSD System Security Section (SEC) is responsible to develop, define, recommend, establish, implement, review, maintain, and enforce policies, standards and procedures relating to IT security for information assets under the control of DAGS. The SEC Chief is the Security Administrator for ICSD.

ICSD Production Services Branch (PSB) is responsible to develop, define, recommend, establish, implement, review, maintain, and enforce policies, standards and procedures relating to central site physical security for information assets under the control of DAGS. The PSB Chief is the Physical Security Administrator for ICSD.

ICSD Telecommunication Services Branch (TSB) is responsible to develop, define, recommend, establish, implement, review, maintain, and enforce policies, standards and procedures relating to Network security for information assets under the control or jurisdiction of DAGS. The TSB Chief is the Network Security Administrator for ICSD.

Each individual who has access to information on a State computer system is responsible to actively support and comply with the security policies, standards and procedures that are established for the protection of the State's information assets.

3 PHYSICAL SECURITY OVERVIEW

IT Standards, 08.07 Physical Security addresses issues needed to physically safeguard, protect, and secure both IT personnel and tangible computer assets.

Physical computer assets include computer hardware and associated equipment, such as, mainframe computers, mini-computers, servers, personal computers, terminals, workstations, networks, connectivity and peripheral equipment, removable storage media, hard copies of documentation, and support facilities.

3.1 Purpose

The physical security IT Standards documents present the written references which define the position of DAGS regarding the security of physical equipment, computers, associated hardware, and resources for which DAGS is responsible.

It is the intent of the physical security IT Standards to:

a. Define the roles and responsibilities of User and IT personnel;

b. Establish the minimum requirements for the protection of the State's physical assets as they relate to the misuse or loss of computer hardware or equipment;

c. Formulate the basis for audits and self-assessment;

d. Preserve the State's management options and legal remedies for asset loss or misuse.

3.2 Scope

The physical security IT Standards documents provide the policies, standards and procedures that will be followed by individuals who use, service and/or maintain the State's information processing hardware, equipment, facilities, and/or resources.

3.3 Applicability

The physical security policies, standards and procedures apply to:

a. All physical computer assets that support business activities, including product support, field support and process control;

b. All owners and users of the State's computer and information assets;

c. All individuals making inquiry only access which uses or is made through State owned equipment;

d. All State vendor suppliers of computer hardware and/or equipment.

The State's computer hardware and equipment include, but are not limited to, vendor supplied information processing equipment; work stations and terminals; personal computers; mainframe computer systems and mini-computer systems; servers; supporting peripheral equipment such as tape drives, disk drives, CD ROM drives and printers; networking routers, switches, hubs and connectivity equipment; and processing facilities.

3.4 Physical Security Content

The physical security IT Standards documents contain the basic policy statements that will be followed when designing, developing and implementing electronic solutions that will access or use computer assets to satisfy the needs of the State or the mandates of the Executive or Legislative branches of the State government.

Specifically, the physical security IT Standards documents provide the policies, standards and procedures that are necessary to ensure the physical security and integrity of computer hardware and equipment as specified in Section 2, Information Security Overview, of this document.

The physical security IT Standards documents provide the physical security procedures that will be followed when individuals use computer resources that are at the central site or are under the administrative control of ICSD.

3.5 Physical Security Responsibilities

ICSD must provide sufficient security to safeguard computer hardware, equipment, and resources; and to prevent actual and/or potential loss of physical resources under its protection.

ICSD Production Services Branch (PSB) is responsible to develop, define, recommend, establish, implement, review, maintain, and enforce policies and procedures relating to physical access to computer hardware, servers, PCs, workstations, terminals, printers, and other equipment physically located at the central computer center site.

Each of the other ICSD branches is responsible to implement, review, recommend, maintain, and enforce policies and procedures relating to physical access to computer hardware, servers, PCs, workstations, terminals, printers, network equipment and other equipment physically located in its areas or under its jurisdiction.

Each individual who has the ability to access equipment or facilities is responsible to actively support and comply with the physical security policies and procedures that are established for the protection of the State's computer assets and resources.

4 SECURITY ENFORCEMENT

Access to mainframe computers, mini-computers, servers, networks and information assets is contingent upon compliance with security policies, guidelines, procedures, and standards. Users who do not comply are subject to protective measures taken to ensure the security of the State's IT resources.

Intrusions, unauthorized access, or misuse of the State's computer or Network resources may be pursued with legal action.

Violation(s) of information security, physical security, or network security policies may be grounds for suspension or revocation of access and use privileges.

Violation(s) of information security, physical security, or network security policies may cause DAGS to recommend that further disciplinary actions be made to the appropriate appointing authority. Such recommendations may include dismissal.

5 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/icsd/

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

http://www.ehawaiigov.org/government/html/

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