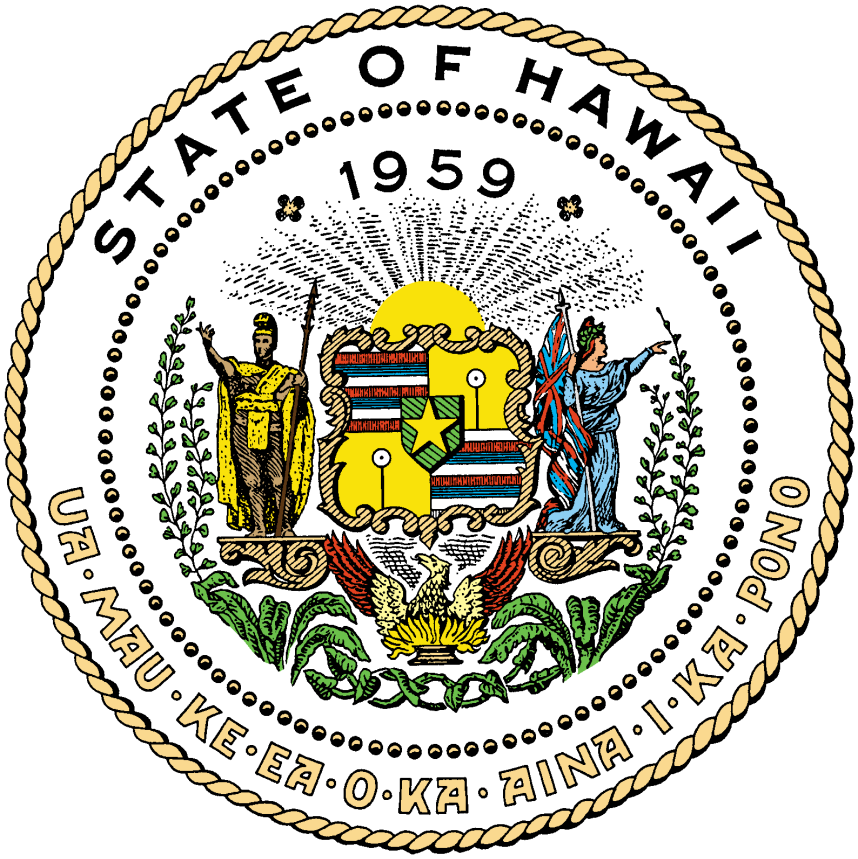
Number: 08.02



INFORMATION SECURITY

NOVEMBER 2009

TABLE OF CONTENTS

Department of Accounting and General Services
Information and Communication Services Division

Information Technology Standards

1 INTRODUCTION

This document addresses the basic issues related to data security for information assets stored in mainframe computers, mini-computers, networks, and PCs.

1.1 Information Security Overview

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

1.2 Exclusions

This document is limited to standards concerned with data housed on mainframe computers, mini-computers, networks, and PCs under the operational control of Department of Accounting and General Services (DAGS), Information and Communication Services Division (ICSD). For standards relating to other areas concerning PCs or Networks, refer to IT Standards 08.03, Personal Computer Security, or 08.04, Network Security.

1.3 Comments and Suggestions

Any comments, recommendations, proposals, or suggestions regarding this document should be in writing and sent to:

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

2 INFORMATION SECURITY RESPONSIBILITIES

To ensure that security responsibilities for electronically based information assets are effective and maintained, the following standards are established for computer systems under the operational control of ICSD.

a. State agencies shall be designated as Owners of information stored in mainframe computers, mini-computers, servers, PCs, and removable information storage media. The Owner is responsible for ensuring the integrity and accuracy of information.

b. Individual managers or employees of the State may be designated as

custodians who are responsible for information asset control.

c. Specific individuals or groups of individuals may further be assigned ownership or custodial responsibilities for certain systems to ensure accuracy, integrity, security, and adequate control of information assets.

d. When proprietary software or property has been provided to the State under a confidentiality agreement, the custodian of the proprietary software or property has the responsibility to assure that all parties are aware of and comply with the terms of such agreements. Such confidentiality agreements are enforceable only to the extent that they do not conflict with Hawaii Revised Statutes, Chapter 92-E, Fair Information Practice, (Confidentiality of Personal Record).

3 INFORMATION SECURITY AREAS

The areas of responsibility and accountability for ensuring the security of the State's information assets residing on mainframe, mini-computer, server, PC, or removable storage media are:

3.1 Owner
3.2 Computer Security Liaison
3.3 Custodian
3.4 User
3.5 Security Administrator

3.1 Owner

The Owner is the State agency that is charged with the responsibility to specify the content of a system and to authorize user access to information assets that are under the agency's jurisdiction. The senior manager of the agency is the individual responsible for performing the tasks and duties relating to ownership.

The Owner may delegate duties and/or responsibilities of ownership to the agency's Computer Security Liaison (CSL) or other selected individuals within the agency, however, final accountability for the information assets rests with the Owner.

The Owner may delegate custodial duties to another agency to enter, store, process, and produce reports using the Owner's data and information systems.

Owner responsibilities include:

a. Knowing the assets and services for which they are responsible.

b. Determining the sensitivity of information, judging the value and importance of the information, and classifying or placing restrictions on the information accordingly.

c. Knowing the specific control requirements that apply to information assets.

d. Establishing the security controls that need to be placed on information assets and communicating the control provisions to the Security Administrator (see section 3.5).

e. Ensuring that established controls are appropriate and effective.

f. Determining, authorizing, and approving who will have access to information and to what extent.

g. Delegating the authority and responsibility for the activation, maintenance, and removal of Logon-IDs and associated access rights to the Security Administrator.

h. Assigning custodial authority and responsibility.

i. Identifying business control and information asset security exposures.

j. Acting upon any loss or misuse of information assets.

k. Ensuring that information assets under the jurisdiction of Federal, State, County, and/or municipal governments are released in compliance with applicable laws and requirements.

l. Conducting self-assessments for compliance with confidentiality agreements.

m. Ensuring employee education and awareness regarding the use and sensitivity of the information assets.

n. Formulating recommendations to improve information security

policies, standards, procedures, and guidelines. Communicating recommendations for such improvements to the Security Administrator.

3.2 Computer Security Liaison

The Computer Security Liaison (CSL) is the individual assigned by the senior manager of the agency to represent the agency's interests in information security matters. The CSL is the information security point of contact for ICSD and performs the computer and network information security tasks for the agency.

CSL security responsibilities include:

a. Formulating recommendations to improve information security policies, standards, procedures, and guidelines. Communicating recommendations for such improvements to the Security Administrator.

b. Notifying the Security Administrator and providing detailed information regarding the following:

   1. Actual access violations to restricted information;

   2. Actual attacks or hacking incidents;

   3. Any virus or computer infestations.

c. Performing liaison duties to coordinate security requirements with CSLs from other agencies.

d. Coordinating security requirements for information to be housed on the State's computer systems and Networks with the Owner and the Custodian.

3.3 Custodian

The Custodian is the agency that enters, stores, processes and/or produces information for the Owner.

The Custodian is the agency that has physical control of the computer equipment on which the information is stored. In most cases, this agency is ICSD.

The manager of the agency entrusted as the Custodian is responsible for taking actions required to protect and safeguard the information.

The areas of responsibility dealing with security that involve the Custodian are: general security requirements; software and programs; and applications.

3.3.1 General Custodial Responsibilities

General security responsibilities of the Custodian include:

a. Establishing the physical safeguards for securing the equipment so that the software, programs and information are protected.

b. Designating an individual to serve as the Security Administrator for equipment under the agency's jurisdiction.

c. Ensuring that security software and programs are available in order to scan diskettes to detect and remove viruses and other infestations prior to installation of the software or program.

d. Informing the CSL, and the Owner when any actual or attempted access violations to classified or restricted information have occurred.

e. Informing the CSL if any virus or other infestation is detected.

f. Formulating recommendations to improve information security policies, standards, procedure, and guidelines. Making recommendations for such improvements to the CSL, and to the Owner.

g. Complying with all security controls designated by either the Owner or CSL.

3.3.2 Software and Program Custodial Responsibilities

Software and program security responsibilities of the Custodian include:

a. Determining the security software and programs that are necessary and appropriate for processing information housed

on the computer system.

b. Authorizing and acquiring security software and programs to be used on the computer system.

c. Installing or delegating the installation of software and programs.

d. Preparing and maintaining an inventory list of all software and programs that reside on each computer system that is under the physical control of the Custodian as a means of ensuring, controlling and validating that only licensed or legal copies of software and programs are installed on the computer system.

e. Ensuring compliance with the licenses and agreements that are issued with issued with software and programs that are installed on a computer system.

f. Ensuring that copies of software and programs which are to be installed on a computer system are free from viruses and other infestations prior to installation on a computer system.

g. Ensuring that only authorized backup copies of software and programs are made.

h. Ensuring that backup copies of software and programs are stored securely and are used for authorized purposes only.

3.3.3 Application Custodial Responsibilities

Application security responsibilities of the Custodian include:

a. Ensuring that Logon-ID identification and authentication is done prior to granting access to information systems.

b. Ensuring availability of the information systems for processing on a continuing basis to Users with authorized access.

c. Ensuring that timely, recoverable backups are available in the event of the destruction or loss of information, or because of a computer outage related to or caused by a security incident.

d. Implementing adequate logical security safeguards for the entrusted information.

e. Implementing adequate physical security measures for equipment to safeguard the information housed on the computer system.

f. Maintaining the established security for information which has been transferred from other computers and/or networks to the computer system.

g. Maintaining the established security for information which has been copied to removable media, down/up loaded, or transferred directly from PCs to the computer system.

h. Using electronic tools to protect sensitive or classified information which passes through the Network. Such tools include but are not necessarily limited to, encryption, digital certificates, and virtual private network (VPN) connections.

i. Ensuring that information systems which are deemed public in nature are available for public inquiry access.

j. Ensuring that information systems which have restricted, confidential, or sensitive information are protected by a firewall.

3.4 User

The User is an individual in an agency who is authorized by and has permission from the Owner, or the Custodian if the Owner has delegated such authority, to access and use information.

The areas of responsibility dealing with security that involve a User are: general security requirements, security of software and programs and security of information housed on the computer system.

3.4.1 User's General Responsibilities

General security responsibilities of the User include:

a. Following the physical safeguards established for securing

equipment so that the software, programs and information are protected.

b. Informing the CSL or the Security Administrator when any actual or attempted access violations to restricted information have occurred.

c. Recommending improvements to security policies, standards, procedure, and guidelines. Communicating recommendations for such improvements to the Security Administrator.

d. Complying with all security controls in force for information to which access is authorized.

3.4.2 User's Software and Program Responsibilities

Security responsibilities of the User for software and programs include:

a. Creating, copying, installing, or allowing the installation of only software and/or programs that are licensed or legally authorized to reside on the computer system.

b. Complying with license agreements by making only authorized copies of software and/or programs installed on the computer system.

c. Reporting the existence of unlicensed, illegal, or pirated copies of software and/or programs to the Security Administrator. And complying with directives to remove such software and/or programs from the computer system.

3.4.3 User's Information Security Responsibilities

Information security responsibilities of the User include:

a. Ensuring responsibility and accountability for all information access made by using assigned Logon-IDs.

b. Ensuring confidentiality of information by not disclosing such information to anyone without the consent of the Owner.

c. Protecting access to information by not disclosing security passwords to anyone and by not leaving an attached terminal or PC unattended while logged on.

3.5 Security Administrator

The Security Administrator is a person within ICSD who is the focal point for information security matters. The Security Administrator is responsible for the security administration functions for DAGS computer systems. The Security Administrator may delegate the security duties and tasks.

Security Administrator responsibilities include:

a. Providing access controls as specified by the Owner.

b. Ensuring that proper logical safeguards are in place to protect the information.

c. Providing adequate procedural controls to protect the information from unauthorized access.

d. Ensuring that ownership and classification information has been established for all information assets used at the State's computing facilities.

e. Reviewing and monitoring computer and network security logs for compliance with security policy.

f. Reviewing access activities to computer systems, networks and firewalls, and communicating violations to the Owner.

g. Restricting or suspending access of user Logon-IDs involved in actual access violations or in potential security breach situations.

h. Developing, modifying, and/or reviewing proposed information security policies, standards, procedures, and guidelines.

i. Providing advice and counsel in matters relating to security to the Owner, CSL, User, Application System developer, Custodian, or other individuals with a need to know.

j. Interfacing with individuals to whom network, firewall, or other

information security tasks and responsibilities have been delegated.

k. Taking security measures to ensure that information which enters the Network is free from nuisance and malicious code.

l. Reviewing and auditing network security logs for compliance with security policy.

m. Recommending improvements to security policies, standards, procedure, and guidelines to the CSL.

4 INFORMATION ACCESS AND USE

As part of information security control, the Owner shall authorize all access to information that falls under the Owner's jurisdiction and for which the Owner is responsible.

Actual access to information is made possible by the Security Administrator through the use of security software which creates the necessary Logon-ID, associated password, access rights, and menus. These permit a user to access application systems information that is housed on a computer system.

4.1 Information Access Security Policy

To ensure that information security is maintained, the following policies are established and in force for all mainframe computer, mini-computers, and servers under the operational control of ICSD.

a. Access to information shall be granted to individuals after the Security Administrator receives a request that is approved by the Owner.

b. The initial request for access which crosses organizational boundaries shall be made in writing by the senior manager of the requesting agency to the senior manager of the owning agency. For State departments, the senior manager is the head of the department.

c. The routine handling of subsequent requests to an Owner for access by other individuals from an agency may be delegated to an individual within the agency. The Owner may specify that such requests be submitted directly to the Custodian or Security Administrator.

d. Information access requests submitted by the Owner or submitted directly to the ICSD, Systems Security Section (SEC) with the approval of the Owner shall be considered as permission for the SEC to create, modify, or delete Logon-IDs.

e. All requests for access to mainframe computer systems, mini-computer systems, or network servers are reviewed and acted upon by Security Administrator within three working days from the receipt of the request.

4.2 Emergency Request Policy

Access requests of an emergency nature are requests which require immediate action. The following policies are established:

a. Any emergency access request shall be coordinated directly with the SEC Chief.

b. The SEC Chief shall determine the validity of the emergency request and specify how the emergency incident is handled.

4.3 File Classification

The following policies are established:

a. File classification codes that specify and limit the access shall be determined and maintained by ICSD/SEC.

b. The Owner shall determine the type of access that an individual User is allowed.

4.4 Use of Production Data

Production data files shall only be used for production applications and/or systems.

4.4.1 Systems Development Testing

Production data files shall not be used for the testing.

Test files shall not be generated by extracting sensitive information contained in live or production data files.

4.4.2 Acceptance Testing

The Owner must approve use of production files in the acceptance testing processes.

4.5 Download or Installation

a. The loading of any software, programs, data, and information to a Network enabled storage device must have prior approval from the Custodian before being copied to the device or being accessed by a User.

b. All software and program storage media are to be scanned by security software to detect and remove viruses and other harmful or invasive code prior to being used for installation of the software or program on a Network enabled storage device. This includes the scanning of all new or update software and installation media, prior to the actual install.

c. The same security access restrictions for information that was originally housed on the mainframe or a mini-computer shall be maintained for that information when it is down loaded to a Network enabled device unless such access restrictions are specifically rescinded or modified by the Owner.

4.6 Access to Public Information

a. Information systems on the State's Network that are open to public access must be separated by a firewall from systems which are for internal use only by State personnel.

b. Identification and authentication of users is required in order to grant access to systems that are for internal use only by State personnel.

5 COMPUTER LOGON ACCESS

The security of information is controlled through granting, reviewing, and monitoring access to the computer hardware and software where the information is housed or referenced.

Computer access is granted in the form of a Logon-ID with an associated password and access rights.

ICSD/SEC is the agency that is authorized to add, change, or delete the Logon-ID.

5.1 Logon-ID/Password Policy

To ensure that Logon-IDs are not misused, the following policies are established and are in force for all mainframe, mini-computer, and servers under the operational control of ICSD.

a. A Logon-ID is issued to an individual.

b. The individual to whom the Logon-ID is issued is responsible and accountable for the use of the Logon-ID.

c. Use of a Logon-ID by an individual, other than the one to whom the Logon-ID is issued, is considered a security violation.

d. A password protects against the misuse of a Logon-ID. The initial password that is associated with a Logon-ID must be changed by the user when the user logs onto the system for the first time.

e. A password must be kept secret. A password shall not be divulged to another individual. Passwords must not be written down nor placed where they could be easily seen or found.

f. Passwords for Logon-IDs shall be forced to automatically expire by the security software. Logon-ID password expiration shall be at regular intervals that are specified by SEC.

5.2 Logon-ID Activity Policy

A Logon-ID that has had its password expired for more than 90 days will be removed from the appropriate computer system as a valid Logon-ID.

5.3 Terminal Activity Policy

The following policies are established:

a. A User shall log off or invoke software that requires entering a

password before leaving a terminal for any reason. Remaining logged on a computer system while not physically present at a terminal, workstation, or PC is considered a security violation.

b. To minimize the risk of a user inadvertently remaining logged on the system while the user is not physically at a terminal, workstation, or PC, the software controlling the maximum duration of inactivity shall log off any user that exceeds the inactivity time parameter. The time parameter shall be specified by SEC.

5.4 Remote Dial-In Access Policy

To ensure that remote dial-in access capabilities to ICSD computers are not misused, the following policies are established:

a. The ICSD Administrator is the approving authority for granting remote dial-in access to computers under the operational control of ICSD.

b. Approval for remote dial-in access shall be granted to specific individuals on a case-by-case basis.

c. Requests for remote dial-in access must include a written justification that details the reason(s) why remote dial-in access is needed.

d. Requests for remote dial-in access for individuals who are not employees of DAGS must be submitted through, and must have the approval of, the senior manager of the requesting agency.

e. Requests for remote dial-in access must be submitted to the ICSD Administrator. Each request is forwarded to the Security Administrator for review and evaluation, then returned to the ICSD Administrator with a recommendation.

f. The Security Administrator shall regularly review the access rights of individuals who are granted remote dial-in access capability. The purpose of this review is to revalidate the remote access rights, and to remove any user who no longer requires remote dial-in capability.

5.5 Dial-Out Access Policy

Approval of dial-out access from the DAGS Network to the Internet or to networks

and computers that are not under the jurisdiction of DAGS is subject to approval restrictions similar to those that are specified in Network Remote Dial-In Access Policy, above. A recap of these restrictions is as follows:

a. The ICSD Administrator is the approving authority.

b. Approval is on a case-by-case basis.

c. A written justification is needed.

d. Requests are submitted to the ICSD Administrator and handled by the Security Administrator.

e. Modems attached directly to Network PCs require approval prior to installation.

f. Use of dial-out capabilities is restricted to accesses related to business of the State.

g. Each individual is responsible for assuring that there are no security breaches onto the Network backbone because of dial-out capabilities.

h. Violation of policy may result in the loss or restriction of access privileges.

5.6 Deletion of Logon-IDs When an Employee Terminates Policy

On or prior to the last day of employment of an employee, all access to ICSD computer files and resources is to be removed. All files associated with the departing employee's logon-IDs are to be reviewed. All files with application, operation, and system value are to be retained. All other files are to be moved to temporary storage and deleted after a short period of time to free up disk storage space.

a. Designated branch personnel will submit an ICSD IT Request System (ITRS), System Access Request (SAR) to delete employee logon-IDs as of a specific date. The branch secretary will also forward the terminated employee's separation notification to ICSD Administration to begin the termination process with DAGS Personnel Office.

b. The terminated employee's logon-IDs will be deleted on the effective date noted in the request. Files, documents, datasets and other computer files in folders specific to the employee on any ICSD server and/or mainframe that are not normal operational files, such as the Notes ID file or Microman report files, will be copied to a temporary private folder and retained for a period not to exceed 30 calendar days.

c. The terminated employee's supervisor will be provided access to the terminated employee's computer files so that the supervisor may preserve any valuable documentation, records, project artifacts, or other operating information by transferring the files to branch folders.

d. After 30 calendar days, all computer files remaining in the terminated employee's private folder will be deleted and the storage space reclaimed.