Number: 08.03

PERSONAL COMPUTER SECURITY

April 2001

TABLE OF CONTENTS

1 INTRODUCTION

This document is identified as IT Standards Number 08.03 in the State of Hawaii IT Standards publication. It addresses the basic issues related to data security for information assets stored in personal computers.

1.1 PC Information Security Overview

The purpose, scope and summary overview for data security IT Standards documents were presented in IT Standards Number 08.01, Information Systems Security Overview.

1.2 Exclusions

This document is limited to standards concerned with data housed on PCs under the operational control of the Department of Accounting and General Services (DAGS), Information and Communication Services Division (ICSD). For standards relating to other areas concerning mini-computers, servers, the mainframe or Networks, refer to IT Standards 08.02, Information 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 PC INFORMATION SECURITY RESPONSIBILITIES

With the advances in networking technology, personal computers (PCs) are increasingly being used to house information. The responsibilities for securing such information are defined below. They are in accord with the responsibilities specified in State of Hawaii IT Standard 08.02 Section 2, Information Security Responsibilities and include the reference to the Hawaii Revised Statutes, Chapter 92-E. "Fair Information Practice, (Confidentiality of Personal Record)".

The areas of responsibility for insuring the security of the State's information assets residing on a PC are the same as those defined for mainframe and mini-computers. The definitions and responsibilities have been expanded or modified as noted below.

The areas are:

1. PC Data Owner
2. PC Data Custodian
3. PC User

2.1 PC Data Owner

The PC Data Owner is the senior manager of the State agency that is charged with the responsibility to control access by users to information assets that are under the agency's ownership.

The final accountability for the security of PC information assets rests with the PC Data Owner.

The PC Data Owner may delegate duties and/or responsibilities of data ownership to or through the agency's DP Coordinator. The DP Coordinator, in turn, may further delegate duties and responsibilities to individuals within the agency. It is possible that the same individual could be the PC Data Custodian and the PC User as well as be delegated the responsibilities and duties of performing the security administration functions defined in 2.4 PC Security Administration, below.

PC Data Owner responsibilities include:

a. Knowing the PC assets and services for which he/she is responsible.

b. Determining the sensitivity of PC data, judging the data's value and importance, and classifying the data accordingly.

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

d. Establishing the security controls that need to be placed on PC data.

e. Ensuring that controls that are established are appropriate and effective.

f. Determining who will have access to PC data and to what extent.

g. Assigning custodial authority and responsibility for PC data to the PC Data Custodian.

h. Communicating the security control provisions to the PC Data Custodian.

i. Delegating PC security administration functions (see Section 2.4, PC Security Administration), to the PC Data Custodian or the PC User.

j. Identifying business control and PC information asset security exposures.

k. Acting upon loss or misuse of PC information assets.

l. Ensuring that PC information assets under the jurisdiction of Federal, State, or municipal governments are released in compliance with applicable laws.

m. Conducting self-assessment for compliance with confidentiality agreements.

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

o. Formulating recommendations to improve PC security policies, standards, procedures, and guidelines.

p. Communicating recommendations for such improvements to the ICSD, Security Administrator.

2.2 PC Data Custodian

The PC Data Custodian is the organizational entity within the agency that has physical control over the PC in which the information is stored.

The manager of the organizational entity entrusted as the PC Data Custodian is responsible for taking actions required to protect, safeguard, and process the information stored on the PC.

The PC Data Custodian may delegate custodial duties and responsibilities to the PC User. This may include the delegation of PC security administration functions that have been delegated to the PC Data Custodian.

The PC Data Custodian installs PC software and programs; enters, stores, processes, and produces information for the PC Data Owner; performs PC security administration functions that have been delegated by the PC Data Owner.

The areas of responsibility for a PC Data Custodian are: General PC security requirements; PC software and programs; and PC application data.

2.2.1 PC Data Custodian General Security Responsibilities

The general security responsibilities of the PC Data Custodian include:

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

b. Designating an individual to serve as the PC Security Administrator for equipment under his/her jurisdiction.

c. Informing the ICSD Security Chief, the PC Security Administrator, and the PC Data Owner when any actual or attempted access violations to restricted data have occurred.

d. Formulating recommendations to improve PC security policies, standards, procedure, and guidelines. Communicating recommendations for such improvements to the ICSD Security Chief, the PC Security Administrator, and to the PC Data Owner.

e. Complying with all security controls designated by either the PC Data Owner or PC Security Administrator.

2.2.2 PC Data Custodian Software and Program Responsibilities

PC Data Custodian software and program security responsibilities include:

a. Determining the PC software and programs that are necessary and appropriate for maintaining the security of information that is stored or processed on the PC.

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

c. Ensuring that only licensed or legal copies of software and programs are installed on a PC.

d. Preparing and maintaining an inventory of all PC software and programs that reside on each PC that is under the physical control of the PC Data Custodian.

e. Ensuring that copies of software and programs that are to be installed on a PC are free from viruses and other infestations prior to installation on a PC.

f. Installing or delegating the installation of PC software and programs.

g. Ensuring compliance with the licenses and agreements that are issued with software and programs that are installed on a PC.

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

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

2.2.3 PC Data Custodian Application Data Responsibilities

PC Data Custodian application data responsibilities include:

a. Ensuring availability of the PC data for processing on a continuing basis to users with authorized access.

b. Ensuring that backup data is available in the event of any destruction or PC computer outage.

c. Implementing adequate logical security safeguards for the entrusted data.

d. Implementing adequate physical security measures for equipment to safeguard the data stored on the PC.

e. Implementing adequate physical security measures to safeguard backup copies of PC data.

f. Knowing and maintaining the established security of data, which has been down loaded from computers and/or network servers to the PC?

g. Knowing and maintaining the established security of data which has been copied to any removable media such as a diskette, a tape, or a CD ROM; or which has been transferred directly from one PC to another PC.

2.3 PC User

The PC User is the individual in the department or agency who is authorized by and has permission from the PC Data Owner or the PC Custodian to access and use the data.

The areas of responsibility for a PC User are: General security requirements, security of PC software and programs, and security of information assets stored on the PC or backup copies stored on removable media.

2.3.1 PC User General Security Responsibilities

General security responsibilities of the PC User include:

a. Knowing and following the physical safeguards established for securing PC equipment so that the software, programs and information are protected.

b. Informing the PC Security Administrator, and the PC Data Owner or the PC Data Custodian when any actual or attempted access violations to restricted information have occurred.

c. Informing the PC Security Administrator, and the PC Data Owner or the PC Data Custodian when any virus, trojan, worm, or other type of infestation happens to the PC.

d. Recommending improvements to PC security policies, standards, procedure, and guidelines. Communicating recommendations for such improvements to the PC Security Administrator, PC Data Owner and PC Data Custodian.

e. Knowing and complying with all security controls designated or delegated by the PC Data Owner, or the PC Data Custodian.

2.3.2 PC Software and Program Security Responsibilities

Security responsibilities of the PC User for software and programs include:

a. Ensuring that only PC software and/or programs that are authorized and approved by the PC Data Owner are installed.

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

2.3.3 PC User's Information Security Responsibilities

Information security responsibilities of the PC User include:

a. Ensuring responsibility and accountability for all data access made by using assigned identification access codes.

b. Ensuring confidentiality of data by not disclosing information to anyone without the consent of the PC Data Owner.

c. Protecting access to information by:

- not disclosing security passwords to anyone
- not leaving the PC active and unattended while logged on
- invoking a password protected sleep mode when away from the PC while logged on.

2.4 PC Security Administration

The PC security administration functions are best performed by a person within the organizational entity that has physical control over the PC.

PC security administration functions and responsibilities include:

a. Maintaining an inventory list of PCs and the people who are authorized to use them. This PC/User Inventory List is to include only

PCs that are under the operational control of PC Data Custodian.

b. Providing the ICSD Security Chief with an updated PC/User Inventory List on an annual basis or whenever the list changes.

c. Providing and documenting data access controls as specified by the PC Data Owner.

d. Ensuring that proper logical safeguards are in place to protect information assets.

e. Providing and documenting adequate procedural controls to protect information assets from unauthorized access.

f. Ensuring that ownership and classification information has been established for all data residing on the PC.

g. Verifying that each PC software or program is authorized and approved by the PC Data Owner before it is installed on a PC.

h. Ensuring that PC security software and programs are available in order to scan removable media such as diskettes and CD ROM to detect and remove viruses and other infestations prior to installation of the software or program on a PC.

i. Informing the ICSD Security Chief when any virus, worm, trojan, or other infestation is detected.

j. Informing the ICSD Security Chief, and the PC Data Owner when any actual or attempted access violations to restricted data have occurred.

k. Formulating recommendations to improve PC security policies, standards, procedure, and guidelines. Communicating recommendations for such improvements to the ICSD Security Chief and the PC Data Owner.

3 PERSONAL COMPUTER INFORMATION ACCESS

As part of data security control, the PC Data Owner shall authorize all access to information for which the PC Data Owner is responsible.

The following types of data exist on a PC:

a. Data that has been created or entered directly on the PC.

Security risks involved with this type of data are easier to identify. The PC Data User is within the same organization or agency as the PC Data Owner and the data classification is stipulated by the PC Data Owner. No organizational lines of authority or responsibility are crossed. PC Users are still responsible for knowing what security measures are in force for the data and maintain these restrictions.

Actual access to data stored on a PC is granted by the PC Data Custodian acting on the authority of the PC Data Owner. The PC Data Custodian shall set up and document the necessary PC security software, access identification codes, associated passwords and access rights.

b. Data that has been created elsewhere and that is subsequently copied, transmitted, imported, or down loaded to the PC by the PC User.

This type of data presents a potential for various kinds of security risks. One type of risk involves the security classification associated with the data. The data inherently carries the access restrictions that were established at the point of origin of the information. When a PC User receives this type of data, it is the PC User’s responsibility to find out the security restrictions that are associated with the data. PC Users must be aware of what security classifications are in force for the data and maintain them. Another type of security risk involves the possibility for malicious or disruptive code to be imbedded within the data that is transferred to the PC. This is one method that a virus, worm, trojan, or other potentially harmful code can be brought to the PC.

c. Data that has been created elsewhere and arrives unsolicited at the PC.

This type of data typically arrives at the PC as an email transmission or as a request for information from the PC. It presents a greater potential security risk in that the transmission can cause a denial of service or can contain a virus or other disruptive or harmful code.

3.1 PC Information Access Security Policy

To ensure that data security is maintained, the following policies are in force on all personal computers under the operational control of DAGS, ICSD.

a. All policies stipulated in State of Hawaii IT Standard 08.02 Information Security, Section 4.1 Information Access Security Policy also apply to the security and access of information assets stored on or associated with a PC.

b. The same security access restrictions for data that was originally stored on the mainframe or on a mini-computer will be maintained for that information when it is down loaded to a PC.

c. All PC software, programs, and data that are to be loaded onto a PC must have prior approval from the PC Data Custodian before they are installed on, copied to, or accessed by the PC.

d. All PC software and program on removable media are to be scanned by PC security software to detect and remove viruses and other infestations prior to installation of the software or program on a PC.

   In some instances, programs or software updates have been shipped by a manufacturer along with embedded viruses. It is NOT to be assumed that because software is shrink-wrapped that it is free from infestation. Therefore, as a precaution, it is highly recommended that all new software, installation CD ROMs and diskettes be scanned prior to running the actual install.

3.2 PC Data File Classification

The Data Owner shall determine the type of access that an individual PC User is granted. The Data Owner may delegate the tasks and responsibility of determining and implementing the type of access to the Data Custodian.

Where applicable, file classification codes that specify and limit the access stipulated by the Data Owner shall be determined and maintained by ICSD Security Chief.

3.3 Use of Production Data on a PC

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

3.3.1 Systems Development Testing

Production data files shall not be used for testing.

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

3.3.2 Acceptance Testing

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

4 PERSONAL COMPUTER LOGON ACCESS

Security of information is initially controlled through granting of access to the computer software and the hardware on which the information is stored.

For most PCs, the physical ability to turn on the power and boot the PC is all that is necessary for a user to have access to the programs and data. In such cases, securing the physical access to the PC is mandatory to safeguard the data stored on the PC.

In some cases logon access software is installed on a PC. Access is granted in the form of a user identification code with associated password and access rights. The identification code is more commonly referred to as the User Identification Code (UID) or as the User Logon-Identification (Logon-Id or ID). It is also known as the Login or Login-Id.

When logon access software is installed on a PC, DAGS, ICSD, SEC, is the agency that is authorized to specify the logon-id format and to add, change, or delete Logon-Ids. The authority to maintain logon-ids on a PC may be delegated by the ICSD Security Chief to the PC Data Custodian.

To ensure that Logon-Ids are not misused, the following policies are in force on all PCs under the operational control of DAGS, ICSD.

4.1 PC Logon-ID/Password Policy

The policy for logonids and passwords for a PC are the same as those for mini-computer and mainframe access specified in State of Hawaii IT Standard 08.02 section 5.1, Logon-ID/Password Policy.

Basically, this policy states that the individual is responsible for use of the Logon-Id, for ensuring that passwords are kept secret, and for not divulged to other individuals.

Passwords should not be written down even if a PC User is worried that the password cannot be remembered. In the event that a password is forgotten, the PC User should seek assistance from the PC Data Custodian or other individual responsible for the administration of Logon-Ids and passwords in the PC User's area.

4.2 PC Logon-ID Activity Policy

The following policies have been established:

a. To minimize the risk that someone might inadvertently remaining logged on while not physically at a PC, software controlling the maximum duration of inactivity shall be installed on each PC. When a PC User exceeds the inactivity time parameter, this software will log off a PC User or suspend activity for a PC User by placing the PC in sleep mode that requires reentering of a password. The inactivity time parameter shall be specified by the ICSD Security Chief.

b. When a PC User leaves work for the day or leaves the PC unattended for any period of time, one of the following actions are to be taken:

- The PC User shall activate the software to put a PC into sleep mode.
- The PC User will power off the PC.
- The PC User shall physically secure access to the equipment in accord with the procedures specified by the Data Owner.

4.3 PC Remote Dial-In Access Policy

The policies for dial-in access to computers and PCs under the operational control of DAGS, ICSD are specified in State of Hawaii IT Standard 08.02 Information Security, Section 5.4 Remote Dial-Up Access Policy.

4.4 PC Dial-Out Access Policy

Approval of dial-out access from a DAGS PC 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 08.02 Information Security, 5.3 Remote Dial-In Access Policy. A recap of these restrictions is as follows:

a. The Comptroller of DAGS 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 ICSD Security Chief.

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 restriction or loss of access privileges.