DHHIT Network Security Standards and Procedures

Contents

1 Introduction

The purpose of information security is to ensure business continuity and minimize business damage by preventing and minimizing the impact of security incidents. Information security management provides an enabling mechanism for information sharing which ensures the protection of information and computing assets. There are three basic components of information security management

confidentiality - protecting sensitive information from unauthorized disclosure
integrity - safeguarding the accuracy and completeness of information and computer software
availability - ensuring that information and vital services are available to users when required

2 Scope

The information security policy and its related standards and procedures apply to all employees, contractors and others with access to Department equipment. It applies to all computer equipment, whether connected to the Department's network or not, and the information and software stored on that equipment.

3 Definitions

Confidential information - Information requiring special safeguards due to the private nature. Examples include client personal data, client medical procedure results and/or related data, employees personal data and Department financial/contractual information.

Security incident - Any event that has, or could have, resulted in loss or damage to Department assets, or an incident that is in breach of Department information security procedures or the rules and regulations governing the use of information systems and services.

4 Employment practices

Every employee, contractor and others with access to Department equipment should have access to a copy of the Information Security policy and this document. Contractors will sign an agreement that they accept the Department's policy on information security, confidentiality and the regulations and responsibilities concerning information technology systems and services.

All employees will be issued with the policy and the regulations governing the use of information systems and associated equipment.

All new employees will be briefed on the importance of information systems security and their role in it, during induction.

Network and Information Technologies Management will be notified of every employee transfer, promotion and termination in order to adjust information systems access privileges as appropriate.

The Secretary to the Department is responsible for Information Technologies security practices relating to employment.

5 Employee Responsibility

Information Technologies security is the responsibility of every employee. No employee shall divulge confidential information to outsiders or other employees who are not authorized to obtain that information. Department information systems resources shall only be used for purposes related to Department business. Employees are also responsible for reporting any security incidents of which they become aware.

The following activities may be illegal or put the Department at risk and are construed as industrial misconduct.

Stealing or copying software

Deliberate propagation of computer viruses/worm/spam/Spy-Ware

Copyright infringement including software copyright

Breaches of confidentiality

Offences under the HIPAA regulation

Failure to maintain appropriate records

Defamation, obscenity, incitement to racial hatred

Failure to report security incidents

Pornography and sexual harassment

Failure to adhere to software licensing and other business/contractual agreements

This document is primarily concerned with Information Technology resources and their use.

6 Physical Security

The Director of Information Technology is responsible for the Department's network security. Individuals are responsible for keeping locations from which information can be accessed secure. Heads of Offices Divisions/Facilities/sections or units have a responsibility for physical security within a given entity's site.

All Information technologies resources will be protected against fire, water, electric power fluctuations, physical damage and theft. Appropriate protection methods will be selected from among others, physical barriers, environmental detection and protection, insurance other risk management techniques, and cost.

7 Network and Systems Security

Only authorized persons will be allowed access to Information Technology resources.

The Director of Information Technologies is responsible for controlling access and providing adequate protection to Department's infrastructure, centralized, and regionally located information technologies resources. In the case of other systems, this is the responsibility of the resource/information 'owner'.

8 User identification and passwords

No one can access Department information systems without an authorized user identification (user id) and password. User id's are made available to staff as part of the process of providing users with electronic mail and other network services.

Each user is responsible for all activity which occurs under the auspices of their user id.

On detection of a serious violation of the Department's Information Security Policy, the Director of Information Technologies (or the system owner) is empowered to revoke the user id at any time provided that a report on the incident is also provided to the Office Assistant Secretary and /or the Secretary of the Department, who will confirm or revoke the suspension. Revocation may be the subject of appeal to the approved Secretary.

User id's will be revoked if the user terminates or transfers employment

9 Access to data

All data files on Department's information systems will be protected against unauthorized changes.

Sensitive data files will be protected against unauthorized reading and copying.

Department information systems shall be programmed to control which user id's can read and which ones can write to any given file.

Every file (including individual databases) shall be associated with an owner. Unless otherwise specified, the owner of a data file (database) is the Assistant Secretary/CEO of the Office/Facility who originated the request for the supporting information system.

The owner of each file (database) is responsible for specifying whether the file (database) is sensitive and which user id's should be allowed to read or write to it. Assistant Secretaries/CEOs of Offices/Facilities are responsible for authorizing in writing any individual request for access to sensitive or confidential information by a member of the department/contractor outside of that entity.

It is the responsibility of data owners to provide to the Executive Steering Committee for Information Technologies their proposed access rules for data which they maintain, to be authorized by the Executive Steering Committee for Information Technologies.

The Executive Steering Committee for Information Technologies will periodically review access rules for data with the data owners, with legal staff and with any other appropriate persons to ensure that the rules provide adequate protection for the Department and appropriate access for Department staff in connection with the duties of their employment.

10 Access to on-line systems enabling direct update or deletion of information

Access to on-line systems containing data of a sensitive or confidential nature is only allowed to user id's which have been authorized for that system.

Techniques will be used to control access to on-line systems and terminals including physical barriers, access control software, automatic shutdown of idle terminals, restriction of sensitive transactions to specified terminals or other methods as appropriate.

A review of user access capabilities will be carried out at least once per year in order to verify whether other events, such as a users change of job function, has led to any non-compliance with the information security policy.

11 Network security including remote access

Wide Area Network (WAN) Management is responsible for ensuring that the policy on information security is not compromised by the network access facilities (including remote access) available to users.

12 Contingency planning

Information owners are responsible for developing and coordinating disaster recovery plans in the event of a short term loss or the destruction of the Department's information technologies systems processing functions for which they are responsible.

Review and testing of the disaster recovery plan should take place on an annual basis.

13 Appendix

Annotated Information Technologies Security Policy

The following details explain the aims of the individual policy statements contained in this Standards document .

To take all appropriate precautions against loss of availability, integrity and confidentiality of information systems and their data.

This includes the organization of appropriate procedures for data backup, ensuring information is kept up-to-date and authorization processes exist for the access to and use of information. It also includes ensuring that rooms and buildings are safeguarded from unauthorized access and that individuals do not leave sensitive or confidential information lying around and that such material is kept in a secure location.

A significant amount of legislation exists and staff will be held personally responsible for any failure to comply with this legislation.

For staff and contractor to be aware of and comply with the Department Information Security Policy and the associated Standards and Procedures. To educate staff in matters relating to the implementation of the security policy

Staff are encouraged to take a positive role in the promotion and implementation of the Department's Information Security Policy, Standards and Procedures. Security incidents must be reported through the correct channels as quickly as possible. Any breach or potential breach of security should be reported. If an aspect of information security is ignored or deliberately breached disciplinary proceedings may be invoked. Awareness information will cover issues such as the need for information security, legal responsibilities of individuals and implementation of information security standards and procedures.

To monitor and control systems in a way in which security threats are detected and eliminated

Access to computer services and data will be controlled on the basis of business requirements. Monitoring tools, including computer virus/spy-ware detection software, will be used to implement appropriate information security measures.

To ensure that adequate safeguards are established in order that disruption to the Department is minimized

Appropriate contingency plans will be available for ensuring the continued availability or immediate replacement of critical information technologies resources for use in the event of a serious breakdown of those resources. Such plans will be routinely tested and maintained.

To ensure that information security standards and procedures are updated as often as necessary

Updates will be required whenever deficiencies are detected, new threats are discovered, new or revised systems are introduced and when new counter measures are installed.