**DPW Internet Policy**

Table of Contents

[I. INTRODUCTION 2](#_Toc350503793)

[II. PURPOSE 2](#_Toc350503794)

[III. RESPONSIBILITY 2](#_Toc350503795)

[IV. SCOPE 2](#_Toc350503796)

[V. DEFINITIONS 4](#_Toc350503797)

[VI. POLICIES 6](#_Toc350503798)

[VII. OWNERSHIP 7](#_Toc350503799)

[VIII. SELECTION AND ACQUISITION 7](#_Toc350503800)

[IX. ANTI-VIRUS SOFTWARE 8](#_Toc350503801)

[X. DIAL-UP ACCESS CONTROLS 8](#_Toc350503802)

[XI. REFERENCES 8](#_Toc350503803)

[List of Appendices 9](#_Toc350503804)

# I. INTRODUCTION

The Department of Public Welfare (DPW), in cooperation with the administrative and program offices, is responsible for ensuring the confidentiality, integrity, and availability of all information that it processes and stores on all Information Technology (IT) resources.

The Department of Public Welfare also has a responsibility, to the residents of the Commonwealth, for ensuring that the IT resources of the Department are used in an approved and appropriate manner. Information Technology resources include all electronic devices used for creating, collecting, producing, processing, transmitting, disseminating, storing, protecting information and for disposing of electronic data, text, images, and voice. Employee and contracted staff times are also considered IT resources.

# II. PURPOSE

The purpose of this document is to provide all users of the Department's IT resources with the identification of accepted standard of conduct mandated by the Department and Commonwealth policies.

In addition, it is the purpose of this document to inform all users of the Department's IT resources of the possibility of disciplinary measures that may be imposed related to violations of the established Commonwealth and Department policies, standards, procedures, and practices.

# III. RESPONSIBILITY

The responsibility for the policies related to the use of IT resources, in an approved and appropriate manner, is organizationally with the Deputy Secretary for Administration.

However, every employees or contracted staff persons within the Department of Public Welfare has a responsibility to respect and adhere to all established Commonwealth and Department policies, standards, procedures, and practices.

# IV. SCOPE

This policy applies to all Department employees/individuals/contractors and their use of its terminal devices, communications lines, mainframes, personal computers, agency data and reports derived from agency data.

**Information Security Policies**

All IT resources provided by the Department are restricted to official Departmental business in accordance with the following related polices:

Management Directive M245.3 - "Guidelines for Personal Computers" amended June 1992 (DPW Administrative Manual 7047.4) Updated in 1997 and currently in the approval process for official release.

Management Directive 235.10, "Commonwealth Data Communications," amended February 1986 (DPW Administrative Manual 7047.7)

Management Directive 205.29, "Commonwealth Internet Access" released March 1996 (DPW Administration Manual, 7047.8)

Management Directive 245.11, "Development of Information Technology - Enterprise Continuity/Recovery Plans" released May 1996 (replaced Management Directive 245.8 "Development of Automated Technology Contingency /Disaster Recovery Plans.)

Management Directive 245.5, "Acquisition, Coordination, and Use of Decentralized and Distributed Automated Technology Equipment and Systems" released May 1987 (replaced Management Directive 235.11)

Executive Order 1988-01, Management of Automated Technology (Amended October 1990)

Executive Order 1980-18 (Amended September 1987), Code of Conduct (DPW Administrative Manual 7170.1)

**Department Information Technical Security Processing Policies**

In addition to the IT security policies referred on the previous page, the Department has developed individual security related processing policies for IT resources. The following is a list of these processing policies. These processing policies contain more detailed information for various IT resources. The documents in this listing should be referenced for specific areas. All of these documents are available to management and staff employees of the Department.

Terminal Security Manual - Released April 1990.

Anti-Virus Distribution, Installation, Cleansing and Reporting Procedures - Released in March 1993.

DPW Electronic Mail (E-Mail) Policy - "draft" currently being reviewed.

Internet Access - (DPW Administration Manual, 7047.8), processing policies and procedures. Revised March 1998.

Internet Usage Policy - issued April 28, 1997 by Mr. J. P. Marinari, Deputy Secretary for Administration.

PC Guidelines - "Guidelines for Personal Computers" amended June 1992 (DPW Administrative Manual 7047.4) Updated in 1997 and currently in the approval process for official release.

POSNet - DPW Administration Manual, 7047.X

# V. DEFINITIONS

The following terminology and their corresponding definitions are used within this document.

**Agency IT Security Officer** - The person in this designated position is responsible for identifying and communicating computer security needs and for incorporating PCc/LANs into the developed security program in an efficient and effective manner in accordance with established policies and procedures.

**Agency Security Officer** - The person in this designated position is responsible for developing and monitoring the agency's total security concept with necessary standards, principles, procedures, and methods relative to personal computer hardware and software which have been authorized for use by the agency, as well as providing essential related training.

**Application Program** - A specific task-oriented program.

**Computer** - An electronic, magnetic, optical, hydraulic, organic or other high speed data processing device or system which performs logic, arithmetic or memory functions, and includes all input, output, processing, storage, software or communication facilities which are connected or related to a network.

**Data** - A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing; any representation, such as characters, to which meaning may be assigned.

**Department/Agency** - Department of Public Welfare.

**"Department employee" and/or "employee."** - These terms are used throughout this document and will included any contracted staff or any other person afforded computer access rights similar to those of persons directly employed by the Department.

**Deputy Secretary for Administration** - The person in this position is directly responsible to the Secretary of the Department of Public Welfare to conduct all business affairs relating to support services for the program offices located organizationally within the Department.

**E-Mail** - Any message sent or received by Department employees and contracted staff with the use of the Department's E-mail system.

**End-User** - The person responsible for adhering to established policies and procedures appropriate for the IT resources being used to ensure the integrity and security of data.

**File Server** - A host, which contains confidential information that may be shared only with predesignated persons who, may have access as determined by job functions and by owner approvals.

**Hardware** - The actual physical devices that make up a computer system. The mechanical, magnetic, and electronic design, structure, and devices of a computer.

**HOST** - Mainframes, File Servers, Mail Servers and/or Information Servers.

**INTERNET** - The worldwide network of networks that are connected to each other and provide unique identification of all computing resources connected. The Internet provides file transfers, remote login, electronic mail, news, and other worldwide web multi-media services.

**LAN** - Local Area Network (same as file server).

**Modem** - Modulator-Demodulator. A device that transforms a computer's electronic pulses into audible tones for transmission over a phone line to another computer.

**Network** - A system which links personal computers together for the purpose of providing access to commonly used computer information (data) among individuals who are designated as approved users within a certain environment.

**Office Security Monitor** - The person in this the administrative head of a Department Program Office and is responsible for controlling on-line access information under their jurisdiction; reviewing security violations; establishing extended security policy and procedures within their jurisdiction; approving terminal security parameters for new on-line transactions under their jurisdiction; and approving changes or additions of Area Security Administrators and/or Site Security Administrators.

**Owner** - An individual or administrative or program office designated as responsible for the management and monitoring of the system including approval of access to software, applications, and/or data.

**Password** - A combination of letters and numbers that serves as a unique identification for the user which allows access to specific data information.

**Peripheral** - A piece of equipment that can be used with a computer to increase its functional range or efficiency, such as a printer, scanner, disk, etc.

**Personal Computer** - A microcomputer designed for individual use.

**POSnet** - Pennsylvania Open Systems Network

**Program** - A set of related instructions that, when followed and executed by a computer, perform operations or tasks.

**Program Office Coordinator** - The person in this designated position is responsible for reviewing and evaluating requests and recommendations from respective program office staff in the selection and acquisition of hardware and software, dissemination of IT related information and software to the end-users within their program office, coordination of IT related concerns or problems with either BIS or vendors, and representation to the POC/BIS committee.

**Software** - The programs used to control computer operations.

**System Administrator** - An individual responsible for maintenance of the system as outlined in the policy under the direction of the owner of the file server.

**Unauthorized Software** - Any software acquired other than through the approved Commonwealth procurement system, developed within DPW, or not otherwise approved by the Office Security Monitor.

# VI. POLICIES

Policies have been developed to provide security and control over the Department's IT resources. These policies must be followed unless it is not technologically feasible or unless a waiver is granted by the IT Security Administrator. The policies to be followed are:

**A. HARDWARE**

All Departmental offices are required to maintain an inventory of hardware including PCs, servers, printers, and peripherals.

**B. SOFTWARE**

The Department (or Commonwealth) enters into license agreements from a variety of vendors. However, the Department does not own this software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce the software and/or documentation. The Department is subject to the license agreement and copyright laws. Therefore, only authorized software will be utilized on Department PCs.

**C. HOSTS**

All Department IT resources that are designated as "HOSTS" (Mainframes, File Servers, Mail Servers and/or Information Servers) must have a designated "owner." This "owner" can be an individual or an organization. The" owner" is responsible for authorizing software, applications, and data to be installed on the host. The "owner" will authorize access to the host. Each host must have a person or group designated as the Systems Administrator. The Systems Administrator will be designated by the Program or Administrative Office "owning" the host. The Systems Administrator is responsible for the non-operating system administration of the host.

The Systems Administrator and "owner" must be registered with the Security, Audits, and Quality Control Section. Information conveyed must include name of "HOST" administrated, name of person or group designated as the Systems Administrator, and other identifying information, as requested.

**D. E-MAIL**

The Department's E-Mail policy incorporates access to, review of, and/or disclosure of E-mail messages. It also sets forth policies on the proper use of the E-mail system provided by the Department. These policies do not constitute a contract. The Department reserves the right to change these policies at any time. Prior notice will be given for any proposed or effective changes.

*The Department of Public Welfare, Statement of Acknowledgment regarding the Department's E-Mail policies is attached as ATTACHMENT ######.*

**E. INTERNET**

The Department's Internet policy is contained in the DPW Administrative Bulletin Number 00-97-07, issued on January 6, 1997. All Internet use will follow this policy.

**F. ACCESS CONTROL**

PASSWORD SECURITY REQUIREMENTS.

Access to all hosts will be controlled by individual Identification and passwords. All individuals access any host will have read and signed a Terminal Operators Statement. The original signed copy of the Terminal Operators Statement will be maintained by the appropriate Site Security Administrator or System Administrator.

Passwords will be updated/changed as specified in the Management Directive 245.X, "Policy on Personal Computers/Networks." Where technologically feasible, passwords are to be changed every 30 days.

**G. AUDIT TRAILS & VIOLATION REPORTING**

All hosts will capture information related to the activity on that host. The information captured will be analyzed to produce violation reports. The violation reports will be reviewed and sent to Site Security Administrator or System Administrator or corrective action.

# VII. OWNERSHIP

Any information generated from agency IT resources, as well as those resources obtained from other agencies, is the property of the Commonwealth of Pennsylvania. Use of the aforementioned IT resources, and of information generated from these resources, is limited to authorized Commonwealth purpose only.

# VIII. SELECTION AND ACQUISITION

All policies and procedures for the planning and acquisition of AT resources are contained in the following documents:

Management Directive 235.10, "Commonwealth Data Communications," amended February 1986 (DPW Administrative Manual 7047.7)

Management Directive 245.1, Management of Automated Technology, Executive Order 1988-01, Management of Automated Technology (Amended October 1990)

Management Directive 245.5, "Acquisition, Coordination, and Use of Decentralized and Distributed Automated Technology Equipment and Systems" released May 1987 (replaced Management Directive 235.11)

Management Directive 245.11, "Development of Information Technology - Enterprise Continuity/Recovery Plans" released May 1996 (replaced Management Directive 245.8 "Development of Automated Technology Contingency /Disaster Recovery Plans.)

# IX. ANTI-VIRUS SOFTWARE

The Office of Administration has obtained a statewide license for software to protect all computers throughout the Commonwealth from virus infections. All end-users are responsible for the safety of the hardware and data processed and therefore, are responsible for the installation and maintenance of anti-virus software.

The Department has established a central control point for the maintenance and distribution of the anti-virus software and information. Anti-virus software will be maintained as specified in the Management Directive 245.X, "Policy on Personal Computers/Networks." The anti-virus software distribution system for the Department is included in Anti-Virus Distribution, Installation, Cleansing and Report Procedures released in March 1993. This information is contained in Appendix ####.

# X. DIAL-UP ACCESS CONTROLS

Dial-up Access Controls must be in accordance with established procedures and approved risk analyses are to be filed with the Security, Audits, and Quality Control Section. All dial-in access must comply with the controls established in the Management Directive 235.10, Commonwealth Data Communications.

Remote access not through approved Internet procedures must have an approved risk analysis and waiver from the IT Security Officer on file with the Security, Audits, and Quality Control Section.

# XI. REFERENCES

Reference A Management Directive M245.3 - "Guidelines for Personal Computers" amended June 1992 (DPW Administrative Manual 7047.4) Updated in 1997 and currently in the approval process for official release.

Reference B Management Directive 235.10, "Commonwealth Data Communications," amended February 1986 (DPW Administrative Manual 7047.7)

Reference C Management Directive 205.29, "Commonwealth Internet Access" released March 1996 (DPW Administration Manual, 7047.8)

Reference D Management Directive 245.11, "Development of Information Technology   Enterprise Continuity/Recovery Plans" released May 1996 (replaced Management Directive 245.8 "Development of Automated Technology Contingency /Disaster Recovery Plans.)

Reference E Management Directive 245.5, "Acquisition, Coordination, and Use of Decentralized and Distributed Automated Technology Equipment and Systems" released May 1987 (replaced Management Directive 235.11)

Reference F Executive Order 1988-01, Management of Automated Technology (Amended October 1990)

Reference G Executive Order 1980-18 (Amended September 1987), Code of Conduct (DPW Administrative Manual 7170.1)

Reference H Terminal Security Manual - Released April 1990.

# List of Appendices

Reference I Anti-Virus Distribution, Installation, Cleansing and Reporting Procedures - Released in March 1993.

Reference J DPW Electronic Mail (E-Mail) Policy - "draft" currently being reviewed.

Reference K Internet Access - (DPW Administration Manual, 7047.8), processing policies and procedures. Revised and released March 1998.

Reference L Internet Usage Policy - issued April 28, 1997 by Mr. J. P. Marinari, Deputy Secretary for Administration.

Reference M POSNet - DPW Administration Manual, 7047.X