

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0520	REVISION: Original	PAGE 1 OF 5
SUBJECT: Acceptable Workstation Use		EFFECTIVE DATE 04/15/05	
OFFICE OF MIS:		DATE:	
SECRETARY OF DHHR:		DATE:	

## 1.0 PURPOSE

The purpose of this policy is to outline the uses of Department of Health and Human Resources (DHHR) workstations, as well as define the responsibilities of DHHR network users.

## 2.0 SCOPE

This policy applies to all employees using DHHR-provided workstations and other computing devices connected to the DHHR network.

## 3.0 APPLICABLE DOCUMENTS/MATERIALS

- 3.1 In instances where state and federal laws and regulations are more restrictive than DHHR IT policies, the more restrictive provisions will supersede.
- 3.2 The Health Insurance Portability and Accountability Act ([HIPAA](#)) of 1996.
- 3.3 DHHR [HIPAA Policy 0423](#) – Sanctions for Violating Privacy and Security Policies and Procedures
- 3.4 DHHR [HIPAA Policy 0441](#) – Safeguards to Protect the Privacy of Protected Health Information
- 3.5 DHHR HIPAA Policy 0446 – Policies and Guidelines on Workstation Use and Location
- 3.6 DHHR [HIPAA Policy 0449](#) – General Guidelines to Safeguard Protected Health Information.
- 3.7 DHHR Policy [IT-0501](#), Use of IT Resources  
Appendix A, [Employee Responsibilities](#)  
Appendix B, [Unacceptable Use of IT Resources](#)
- 3.8 DHHR Policy [IT-0503](#), Software Copyright Compliance
- 3.9 DHHR Policy [IT-0510](#), E-Mail Guidelines and Requirements

DOCUMENT: <b>Policy</b>	DOCUMENT NUMBER: <b>IT-0520</b>	REVISION: <b>Original</b>	PAGE <b>2</b> OF <b>5</b>
SUBJECT: <b>Acceptable Workstation Use</b>		EFFECTIVE DATE: <b>04/15/05</b>	

- 3.10 DHHR Policy IT-0515, Security for Portable Computers
- 3.11 DHHR Policy IT-0518, Access Authorization and Modification
- 3.12 Office of Management Information Services (OMIS) Operating Procedure (OP) -14, User Security
- 3.13 OMIS OP-15, Access Controls
- 3.14 OMIS OP-18, Managing Information Security Incidents
- 3.15 DHHR [Policy Memorandum 2104](#) – Progressive Discipline
- 3.16 DHHR [Policy Memorandum 2108](#) – Employee Conduct

#### 4.0 RESPONSIBILITIES/REQUIREMENTS

- 4.1 Computer workstations installed for use within the DHHR are the property of the DHHR, and are provided to assist DHHR employees in performing their duties and responsibilities associated with their positions and in support of business functions.
  - 4.1.1 DHHR employees and authorized network users can log on to the network from any computer in the state-wide DHHR network to gain access to their e-mail, personal and shared network areas, as well as most other applications to which they are authorized to access.
  - 4.1.2 Only minimal personal use of DHHR computing devices is allowed, and should not interfere with the legitimate business of the State.
  - 4.1.3 Transactions resulting from computer usage are the property of the DHHR, and are subject to DHHR policies as well as all applicable state and federal laws and statutes.
- 4.2 Bureaus/Offices may revoke the access rights of any individual at any time in order to protect data or to preserve the functionality of electronic information systems.
- 4.3 OMIS will evaluate, authorize, install, and maintain all software and hardware for use on all DHHR desktop computers, laptops, servers, and other computing devices.
- 4.4 User Responsibilities

DOCUMENT:	Policy	DOCUMENT NUMBER:	IT-0520	REVISION:	Original	PAGE	3	OF	5
SUBJECT:	Acceptable Workstation Use			EFFECTIVE DATE:	04/15/05				

- 4.4.1 Users of the DHHR workstations and authorized network users are responsible for becoming familiar with and abiding by all DHHR IT policies and OPs.
- 4.4.2 Each network user is responsible for logging out of applications and the network when vacating a shared computer, and for locking or logging off their workstation when not in use.
- 4.4.3 Network users are not permitted to share their userid or password(s), or leave workstations unlocked or unattended.
- 4.4.4 DHHR network users are prohibited from downloading, attaching, installing, or changing any software or hardware, including wireless devices.
- 4.4.5 Vendors and/or non-DHHR employees are prohibited from connecting equipment (including laptops) to the DHHR network without specific authorization by OMIS.

#### 4.5 Unauthorized Uses of DHHR Workstations

- 4.5.1 All activities performed on workstations can affect the availability of resources for part of, or the entire DHHR network. Unauthorized uses of DHHR workstations include, but may not be limited to the following:
  - 4.5.1.1 Bypassing or attempting to bypass OMIS security and access control systems;
  - 4.5.1.2 Using workstations to play or download games, or broadcast audio or video for non-business functions;
  - 4.5.1.3 Access non-DHHR provided web e-mail services;
  - 4.5.1.4 Unauthorized use of Instant Messaging or Internet Relay Chat (IRC);
  - 4.5.1.5 Utilizing non-OMIS authorized peer-to-peer networking or peer-to-peer file sharing;
  - 4.5.1.6 Sending or sharing confidential information for unauthorized purposes; or
  - 4.5.1.7 Using the workstation for activities other than its intended purpose including those that violate any federal, state, or local law, or any other state or DHHR policy.

DOCUMENT:	Policy	DOCUMENT NUMBER:	IT-0520	REVISION:	Original	PAGE	4	OF	5
SUBJECT:	Acceptable Workstation Use			EFFECTIVE DATE:	04/15/05				

#### 4.6 Enforcement Authority

- 4.6.1 The ISO is the person designated by the CTO to monitor and provide initial enforcement of DHHR's information security program and IT policies.
- 4.6.2 The Information Security Liaisons (ISL) are employees assigned by the Bureau Commissioners and/or Office Directors to assist the ISO in the protection of information resources.
- 4.6.3 The Office of the Inspector General (OIG) is the primary authority who investigates any reported instances of Departmental employee misconduct.

#### 4.7 Violations and Disciplinary Actions

- 4.7.1 All suspected violations of this policy will be reported to a supervisor in the chain of command above the employee.
- 4.7.2 The supervisor or designee will review the facts and, if it is suspected that a violation may have occurred, the matter will be referred to his/her Office Director or Bureau Commissioner for appropriate action.
- 4.7.3 As determined by Office Directors and the Bureau Commissioners, instances of abuse or misconduct, depending on the circumstances, will be referred to either the ISO or the OIG for further investigation.
- 4.7.4 Employees who willfully or knowingly violate or otherwise abuse the provisions of this policy may be subject to: (1) disciplinary action as outlined in DHHR Policy Memorandum 2104; or (2) criminal prosecution.

### 5.0 DEFINITIONS

- 5.1 Authorized Network Users – Individuals who have been granted access to DHHR network resources through an assigned userid.
- 5.2 Employee - Individuals employed on a temporary or permanent basis by the DHHR; as well as contractors, contractor's employees, volunteers, and individuals who are determined by the Bureau or Office to be subject to this policy. For the purposes of this policy, this also refers to anyone using a computer connected to the DHHR network.

DOCUMENT: <b>Policy</b>	DOCUMENT NUMBER: <b>IT-0520</b>	REVISION: <b>Original</b>	PAGE <b>5</b> OF <b>5</b>
SUBJECT: <b>Acceptable Workstation Use</b>		EFFECTIVE DATE: <b>04/15/05</b>	

- 5.3 Network – A system of computers, and other peripherals, such as printers, linked together. DHHR workstations are connected to a Wide Area Network (WAN), which is a larger network, which uses telephone lines or radio waves to link computers that can be up to thousands of miles apart.
- 5.4 Workstation – An electronic computing device (ex: laptop or desktop computer) or any other device that performs similar functions, and electronic media stored in its immediate environment.