

DOCUMENT: POLICY	DOCUMENT NUMBER: IT-0515	REVISION: Original	PAGE 1 OF 5
SUBJECT: ACCEPTABLE USE FOR PORTABLE COMPUTERS AND MOBILE DEVICES		EFFECTIVE DATE: 03/20/06	
OFFICE OF MIS:		DATE:	
SECRETARY OF DHHR:		DATE:	

1.0 PURPOSE

This policy outlines acceptable use, security requirements, and confidentiality issues related to portable computers and mobile devices within all DHHR connected and supported sites.

The term *portable computer and mobile device* is used in this document to include: laptops, notebooks, PDAs, Smart phones, and tablet PCs.

2.0 SCOPE

This policy applies to all DHHR employees who use portable computers and mobile devices that connect to the DHHR network.

3.0 APPLICABLE DOCUMENTS/MATERIAL

- 3.1 [DHHR IT Policy 0501](#) – Use of IT Resources
[Attachment A](#) – Employee Responsibilities
[Attachment B](#) – Unacceptable Uses of IT Resources
- 3.2 [DHHR IT Policy 0511](#) – IT Network Security
- 3.3 [DHHR IT Policy 0520](#) – Acceptable Workstation Use
- 3.4 [DHHR IT Policy 0521](#) – Jump Drives
- 3.5 Office of Management Information Services (OMIS) Operating Procedure (OP)–19–
DHHR Portable Computer Security
- 3.6 OMIS OP-28 – Jump Drive Installation Instructions
- 3.7 [DHHR Policy Memorandum 2104](#) - Progressive Discipline
- 3.8 [DHHR Policy Memorandum 2108](#) – Employee Conduct

4.0 RESPONSIBILITY/REQUIREMENTS

DOCUMENT: POLICY	DOCUMENT NUMBER: IT-0515	REVISION: Original	PAGE 2 OF 5
SUBJECT: ACCEPTABLE USE FOR PORTABLE COMPUTERS AND MOBILE DEVICES		EFFECTIVE DATE: Draft: 03/20/06	

DHHR employees are provided the use of portable computers and mobile devices on an as-needed basis to access the DHHR network, or to conduct DHHR business from a remote location not always connected to the network.

Portable computers and mobile devices provide mobility, flexibility, and convenience for the employee. They also offer an elevated risk of becoming infected with viruses when connected to less secure networks, and therefore require higher standards than desktop computers.

4.1 Employee Responsibilities

4.1.1 Employees must use portable computers and mobile devices for business purposes only.

4.1.1.1 All rules regarding the acceptable use of IT Resources within the DHHR apply to the utilization of mobile equipment. (See policy IT-0501, *Use of IT Resources*)

4.1.2 Each portable computer and mobile device must receive program updates, security patches, and anti-virus updates at designated intervals. (See OP-19 – *Security for DHHR Portable Computers and Mobile Devices*)

4.1.2.1 In order to receive updates, each portable computer and mobile device must be connected and logged-on to the DHHR network.

4.1.2.2 OMIS reserves the right to disable computer accounts for any device not connected to the network or updated at the time of the designated interval.

4.2 Data Confidentiality

4.2.1 If a portable computer or mobile device currently contains, or will contain, sensitive data and/or electronic Protected Health Information (e-PHI), its data storage must be encrypted.

4.2.2 The method of encryption will be determined, installed, and configured by the appropriate OMIS technician or designated individual.

4.2.3 Precautions must be taken to ensure the privacy of information when accessing the network from a remote location. These may include: hotels, airports,

DOCUMENT: POLICY	DOCUMENT NUMBER: IT-0515	REVISION: Original	PAGE 3 OF 5
SUBJECT: ACCEPTABLE USE FOR PORTABLE COMPUTERS AND MOBILE DEVICES		EFFECTIVE DATE: Draft: 03/20/06	

hospitals, dial-up modem access, Broadband access (wired or wireless, i.e. Hotspots), or other private network access.

4.3 Security Requirements

4.3.1 Upon installation, each portable computer and mobile device must be loaded with anti-virus software.

4.3.2 Each portable computer and mobile device must be configured with a standard Basic Input/Output System (BIOS) power-on password.

4.3.2.1 In the event a BIOS password is unavailable, a hard drive password must be used.

4.3.2.2 This password will be assigned and installed by the appropriate OMIS technician or designated individual.

4.3.3 Upon installation, each portable computer and mobile device is joined to the DHHR domain, or equivalent secure Group Policy Active Directory domain.

4.3.4 Each portable computer and mobile device must be configured with an OMIS-approved personal firewall for all connections.

4.3.4.1 Settings must be the most restrictive firewall connection possible, while also allowing acceptable use of the device.

4.3.4.2 If these firewall settings are not available, a third-party product must be used for all connections.

4.3.4.3 The selection, installation, and configuration will be conducted by the appropriate OMIS technician or designated individual.

4.4 Physical Care

4.4.1 In all cases, manufacturer's guidelines for the care and safety of portable computers and mobile devices must be followed. (For more information, see OP-19.)

4.5 Enforcement Authority

DOCUMENT: POLICY	DOCUMENT NUMBER: IT-0515	REVISION: Original	PAGE 4 OF 5
SUBJECT: ACCEPTABLE USE FOR PORTABLE COMPUTERS AND MOBILE DEVICES		EFFECTIVE DATE: Draft: 03/20/06	

4.5.1 The Information Security Officer (ISO) has been designated by the CTO to monitor and provide initial enforcement of DHHR's information security program and IT policies.

4.5.2 Information Security Liaisons (ISL's) are employees assigned by the commissioner of each Bureau and/or Office to assist the ISO in the protection of information resources.

4.5.3 The Office of the Inspector General (OIG) is the authority who investigates reported instances of Departmental employee misconduct.

4.6 Violations and Disciplinary Action(s)

4.6.1 All suspected violations of this policy will be reported to a supervisor in the chain of command above the employee.

4.6.2 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 the Office Director or Bureau Commissioner for appropriate action.

4.6.3 As determined by the Office Director or the Bureau Commissioner, instances of abuse or misconduct, depending on the circumstances, will be referred to either the ISO or the OIG for further investigation.

4.6.4 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 Basic Input/Output System (BIOS) – A set of instructions and routines that enable the computer to communicate with the various devices in the system, such as memory, disk drives, keyboard, monitor, printer, and communication ports. The BIOS handles the flow of data between the operating system and the hardware.

5.2 Electronic Protected Health Information (e-PHI) - Health information transmitted by or maintained in electronic media used to identify an individual, which is created, used, or disclosed in the course of providing health care services such as diagnosis or treatment. Examples include: names, phone numbers, medical record numbers, photos, etc.

DOCUMENT: POLICY	DOCUMENT NUMBER: IT-0515	REVISION: Original	PAGE 5 OF 5
SUBJECT: ACCEPTABLE USE FOR PORTABLE COMPUTERS AND MOBILE DEVICES		EFFECTIVE DATE: Draft: 03/20/06	

- 5.3 Office of Management Information Services (OMIS) – This office reports directly to the DHHR Deputy Secretary for Administration and provides the leadership, innovation, and services needed to achieve efficient and effective technology solutions to meet the goals of the DHHR.
- 5.4 Personal Firewall – Personal computer software that can be configured to prevent specific network traffic from entering a computer.
- 5.5 Portable Computers and Mobile Devices – Includes laptops, notebooks, PDAs, Smart phones, and tablet PCs.