

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0513	REVISION: Original	PAGE 1 OF 5
SUBJECT: Physical Security for IT Resources		EFFECTIVE DATE: 04/18/05	
OFFICE OF MIS:		DATE:	
SECRETARY OF DHHR:		DATE:	

1.0 PURPOSE

This policy outlines the responsibilities and requirements of the Department of Health and Human Resources (DHHR) and its employees with regard to physical and environmental security for Information Technology (IT) resources.

2.0 SCOPE

This policy applies to all employees who use, service, and/or maintain the DHHR's information processing hardware, equipment, facilities, and/or resources.

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 0449](#) – General Guidelines to Safeguard Protected Health Information
- 3.5 DHHR IT Policy [0511](#), IT Network Security
- 3.6 DHHR IT Policy [0512](#), IT Information Security
- 3.7 DHHR IT Policy 0514, Disaster Recovery
- 3.8 DHHR IT Policy 0517, Media Disposal
- 3.9 DHHR Policy Memorandum [2104](#), Progressive Discipline
- 3.10 DHHR Policy Memorandum [2108](#), Employee Conduct
- 3.11 OMIS Operating Procedure (OP)-01, Computer Room Access
- 3.12 OMIS OP-17, Media Controls

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0513	REVISION: Original	PAGE 2 OF 5
SUBJECT: Physical Security for IT Resources		EFFECTIVE DATE 04/18/05	

3.13 OMIS OP-18, Managing Information Security Incidents

4.0 RESPONSIBILITIES/REQUIREMENTS

4.1 DHHR Responsibility

- 4.1.1 Each Bureau/Office will develop a plan to maintain the physical security of IT Resources.
- 4.1.2 Each Bureau and/or Office will abide by rules governing physical access to stored information and information devices.
- 4.1.3 Each Bureau/Office should ensure that sufficient procedures relating to physical access to buildings are developed and maintained. Access procedures will vary according to the individual office location.
- 4.1.4 Each Bureau/Office must ensure that rooms and/or storage cabinets housing critical DHHR equipment, information assets, or access points must be restricted to only those who need access to fulfill their job responsibilities.
- 4.1.5 All DHHR employees are accountable for their actions relating to physical security, and will comply with policies and procedures protecting DHHR's computer assets and resources.
- 4.1.6 The DHHR will provide on-going awareness education, and train all employees on physical security requirements for IT resources.
- 4.1.7 The Information Security Officer (ISO) or a designee may conduct a physical security assessment of IT resources as needed.
- 4.1.8 The Office of Management Information Services (OMIS) will develop, review, and maintain policies and procedures relating to physical access to computing resources within the DHHR.

4.2 Access Control

- 4.2.1 Physical security controls for IT resources should be proportional to the risks of physical damage or unauthorized access.
- 4.2.2 All physical security provisions used for off-site storage will be equivalent to the standards of primary facilities and/or approved by the manager of the Network and Technical Support (NTS) unit.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0513	REVISION: Original	PAGE 3 OF 5
SUBJECT: Physical Security for IT Resources		EFFECTIVE DATE 04/18/05	

4.2.2.1 Periodic testing and review of physical security for IT resources plans will be conducted by OMIS.

4.2.3 Appropriate controls will be implemented to reduce the risk of sensitive information being transmitted to un-authorized persons. (Ex: confidentiality statements, outside e-mail encryption, etc.)

4.3 Environmental Security/Equipment

4.3.1 Each Bureau/Office should ensure that sufficient plans are developed and measures are put into place and maintained for protection against environmental factors (e.g., dust, fire, power, or excessive heat and humidity).

4.3.1.1 Temperatures in server and switch rooms must stay between the range of 64 and 75 degrees. Humidity should remain between 30 to 55 percent.

4.3.2 Procedures will be established to ensure that computing resources are properly maintained.

4.3.3 Computing resources, including fax machines and printers, will be located in secure areas appropriate to the sensitivity of the output produced.

4.3.3.1 Employees are expected to be aware of equipment located within their immediate areas and to report missing equipment to supervisors.

4.3.4 All IT equipment should be carefully inspected prior to its disposal or release outside of DHHR to ensure that it contains no sensitive information, including any data remnants that might have been retained on the equipment after processing. (See OP-17, Media Controls)

4.4 Disaster Recovery (See IT-0514, Disaster Recovery)

4.4.1 Plans and controls will be in place to enable DHHR systems, on and off-site, to continue to operate in the event of fire, vandalism, natural disaster, or system failure.

4.4.1.1 Each Bureau/Office will maintain a cost effective business recovery plan that will provide for prompt and effective continuation of critical missions in the event of a disaster.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0513	REVISION: Original	PAGE 4 OF 5
SUBJECT: Physical Security for IT Resources		EFFECTIVE DATE 04/18/05	

4.4.1.2 Each Bureau/Office will have procedures in place for reporting incidents, implementing the disaster recovery plan, and escalating the response to a disaster.

4.4.1.3 Each Bureau/Office is responsible for training, testing, and review of their disaster recovery plan(s).

4.5 Enforcement Authority

4.5.1 The ISO is the person designated by the Chief Technology Officer (CTO) to monitor and provide initial enforcement of the DHHR's information security program and IT policies.

4.5.2 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.

4.5.3 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 his/her Office Director or Bureau Commissioner for appropriate action.

4.6.3 As determined by the Office Director or 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 or systems administrators or managers 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 2104; or (2) criminal prosecution.

5.0 DEFINITIONS

5.1 Access – the ability to read, write, modify, or communicate data/information or otherwise use any system resource.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0513	REVISION: Original	PAGE 5 OF 5
SUBJECT: Physical Security for IT Resources		EFFECTIVE DATE 04/18/05	

- 5.2 Access Controls – rules for limiting access to safeguard systems and data at all times and under all conditions.
- 5.3 Chief Technology Officer (CTO) – the director of OMIS and the person responsible for all information resources within the DHHR.
- 5.4 Computing Resources – computer hardware, servers, PC's, workstations, terminals, printers, and other equipment physically located within the DHHR.
- 5.5 Disaster – Any event that makes an organization unable to provide critical business functions for a pre-determined period of time. This may include: any occurrence or imminent threat of widespread or severe damage, injury, or loss of life or property resulting from a natural, technological, and/or national security incident, (ex: fire, vandalism, natural disaster, or system failure).
- 5.6 Employee – Individuals employed on a temporary or permanent basis by the DHHR; as well as contractors, contractors' 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.
- 5.7 Incident – An adverse event associated with an information system that: (1) fails to comply with security regulations or directives; (2) results in attempted or actual loss of data; (3) involves the waste, fraud, abuse, loss, or damage of property or information; and (4) reveals and/or exploits hardware or software vulnerabilities.
- 5.8 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.
- 5.9 Physical Security – refers to the protection of building sites and equipment (and all other information and software contained within) from theft, vandalism, natural disaster, man-made catastrophes, and accidental damage.
- 5.10 Sensitive Information – Information/data that would be disadvantageous should it become known to others (ex: political/religious beliefs, health information, or criminal record).
- 5.11 Workstation – an electronic computing device (i.e., laptop or desktop computer), or any other device that performs similar functions, and the electronic media stored in its immediate environment.