

DOCUMENT: POLICY	DOCUMENT NUMBER: 0501	REVISION:02/03/03	Page 1 of 4
SUBJECT: USE OF INFORMATION TECHNOLOGY RESOURCES			EFFECTIVE DATE: March 14, 2000
OFFICE OF MIS:		DATE:	
SECRETARY OF DHHR:		DATE:	

1.0 PURPOSE

The DHHR (Department of Health and Human Resources) provides its employees with access to IT (Information Technology) resources as required for the performance and fulfillment of job duties. This policy defines the responsibilities of both the DHHR and the employee in regard to these resources.

2.0 SCOPE

This policy applies to all employees who use DHHR systems.

3.0 APPLICABLE DOCUMENTS/MATERIALS

- 3.1 DHHR IT Policy 0502 - Virus Prevention, Detection, and Removal
- 3.2 DHHR IT Policy 0510 - E-mail Guidelines and Requirements
- 3.3 DHHR IT Policy 0511 - IT Network Security
- 3.4 DHHR IT Policy 0512 - IT Information Security
- 3.5 DHHR Policy Memorandum 2104 - Progressive Discipline
- 3.6 DHHR Policy Memorandum 2108 - Employee Conduct
- 3.7 West Virginia Freedom of Information Act - WV Code, Chapter 29B

4.0 RESPONSIBILITY/REQUIREMENTS

- 4.1 Overview of Technologies
 - 4.1.1 DHHR defines two types of IT resources; technologies that create records, and those that do not.

DOCUMENT: Policy	DOCUMENT NUMBER: 0501	REVISION: 02/03/03	PAGE 2 OF 4
SUBJECT: Use of Information Technology Authority		EFFECTIVE DATE: March 14, 2000	

4.1.1.1 Those that create records include, but may not be limited to Internet/Intranet, e-mail, fax, voice mail, and any emerging technologies.

4.1.1.2 Those that do not create records include, but may not be limited to various types of computer hardware and software, telephones, cell phones, pagers, two-way radios, and other communication devices.

4.2 DHHR Responsibilities

4.2.1 The DHHR has the right to monitor and review employee use as required for legal, audit, or legitimate authorized state operational or management purposes.

4.3 Employee Responsibilities

4.3.1 Only minimal personal use of DHHR IT resources is allowed, and should not interfere with the legitimate business of the State.

4.3.2 Access to any state-provided IT resource may be denied or revoked at any time for any reason without notice.

4.3.3 Access and privileges on DHHR applications systems are assigned and managed by the administrators of specific systems. Eligible individuals may become authorized users of a resource or system and be granted appropriate access and privileges by following the approval steps for that resource or system.

4.3.4 Inappropriate use of state provided IT resources that pose the risk of disruptions to DHHR activities is prohibited. (see appendix B)

4.3.5 Employees will be informed about confidentiality, privacy, and acceptable use of state-provided IT resources as defined in this policy. Detailed information is available in the following appendices:

Appendix A - Responsibilities

DOCUMENT: Policy	DOCUMENT NUMBER: 0501	REVISION: 02/03/03	PAGE 3 OF 4
SUBJECT: Use of Information Technology Authority		EFFECTIVE DATE: March 14, 2000	

Appendix B - Unacceptable Use of IT Resources

4.4 Privacy Issues and Legal Implications

- 4.4.1 Employees should have no expectation of privacy while using state-provided equipment.
- 4.4.2 E-mail and other electronic files create a record and may be accessible through the discovery process in the event of litigation.

4.6 Retention/Disposition of IT Records

- 4.6.1 IT records are retained or disposed of in accordance with the policies and regulations associated with those records.

4.7 Enforcement Authority

- 4.7.1 The ISO (Information Security Officer) is the person designated by the CIO to monitor and provide initial enforcement of DHHR's information security program and IT policies.
- 4.7.2 The ISL's (Information Security Liaisons) are employees assigned by the Commissioner with each Bureau and/or Office to assist the ISO in the protection of information resources.
- 4.7.2 The OIG (Office of the Inspector General) has been designated by the Secretary of the DHHR as the primary authority to investigate any reported instances of Departmental employee misconduct.

4.8 Violations and Disciplinary Action(s)

- 4.8.1 All suspected violations of this policy shall be reported to a supervisor in the chain of command above the employee.
- 4.8.2 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.

DOCUMENT: Policy	DOCUMENT NUMBER: 0501	REVISION: 02/03/03	PAGE 4 OF 4
SUBJECT: Use of Information Technology Authority		EFFECTIVE DATE: March 14, 2000	

4.8.3 After reviewing all allegations, the Bureau Commissioners may refer the alleged abuse or misconduct to the ISO and/or the OIG as warranted for further investigation.

4.8.4 Employees or systems administrators or managers who willfully or knowingly violate or otherwise abuse the provisions of this policy may be subject to: (1) progressive disciplinary action as outlined in DHHR Policy 2104; or (2) criminal prosecution. Levels of discipline include:

- Verbal reprimand
- Written reprimand
- Suspension
- Demotion
- Dismissal

5.0 DEFINITIONS

- 5.1 Chief Information Officer (CIO)- is the Director of MIS and the person responsible for all information resources within the DHHR.
- 5.2 Emerging Technology- Technologies that are yet to be invented or implemented within the DHHR.
- 5.3 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.
- 5.4 MIS (Management Information Services) - Office that reports directly to the Secretary and provides leadership, innovation, and services needed to achieve efficient and effective technology solutions to meet the goals of the DHHR.
- 5.3 Office of the Inspector General (OIG) - is designated by the Secretary to investigate or assist in investigating allegations of employee abuses or misconduct.