

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0512	REVISION: Original	PAGE 1 OF 6
SUBJECT: IT Information Security		EFFECTIVE DATE: 04/07/03	
OFFICE OF MIS:		DATE:	
SECRETARY OF DHHR:		DATE:	

1.0 PURPOSE

This policy establishes guidelines to protect information resources within the Department of Health and Human Resources (DHHR).

2.0 SCOPE

This policy applies to all DHHR employees who have access to, store data in, retrieve data from view, or otherwise make use of DHHR information resources.

3.0 APPLICABLE DOCUMENTS/MATERIAL

- 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 DHHR IT [Policy 0501](#) – Use of IT Resources
[Appendix A](#) – Employee Responsibilities
- 3.3 DHHR IT [Policy 0510](#) – E-mail Guidelines and Requirements
- 3.4 DHHR IT [Policy 0513](#) – Physical Security for IT Resources
- 3.5 DHHR IT [Policy 0514](#) – Disaster Recovery
- 3.6 DHHR IT [Policy 0518](#) – Access Authorization and Modification
- 3.7 OMIS Operating Procedure (OP) – 12 – E-mail
- 3.8 OMIS OP – 22 – Information Security Awareness Training
- 3.9 DHHR [Employee](#) and [Vendor](#) Confidentiality Statements
- 3.10 West Virginia Code – [Section 49-7-1](#), Confidentiality of Records
- 3.11 West Virginia Computer Crime and Abuse Act – [Section 61-3C-21](#)

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0512	REVISION: Original	PAGE 2 OF 6
SUBJECT: IT Information Security		EFFECTIVE DATE: 04/07/03	

- 3.12 West Virginia Governors Office of Technology (WVGOT) Directive [State of West Virginia ITC Information Security Policy](#)
- 3.13 DHHR Common Chapters Manual – [Chapter 200](#), Confidentiality
- 3.14 DHHR Policy Memorandum [2104](#) – Progressive Discipline
- 3.15 DHHR Policy Memorandum [2108](#) – Employee Conduct
- 3.16 West Virginia Freedom of Information Act – [WV Code, Chapter 29B](#)
- 3.17 Federal Computer Fraud and Abuse Act of 1996
[US Code, Title 18, Chapter 47, Section 1030](#)
- 3.18 Electronic Communications Privacy Act of 2000
[US Code, Title 18, Chapter 119, Section 2511](#)
- 3.19 West Virginia Records Management and Preservation of Essential Records Act,
[WV Code, Chapter 5A, Article 8](#)
- 3.20 Health Insurance Portability and Accountability Act ([HIPAA](#)) of 1996
- 3.21 West Virginia Records Retention and Disposal Schedule for Department of Health

4.0 RESPONSIBILITY/REQUIREMENTS

4.1 Information Resources

- 4.1.1 Bureau Commissioners and their organizational equivalent(s) are responsible for the protection of information resources under their jurisdiction and control.
- 4.1.2 Information resources will be used only for intended purposes as defined by the Bureaus/Offices, will be consistent with applicable state and federal laws, and will satisfy all mandated federal compliance requirements.
- 4.1.3 All DHHR employees are accountable for their actions relating to information resources.

4.1.3.1 Passwords must never be shared under any circumstances.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0512	REVISION: Original	PAGE 3 OF 6
SUBJECT: IT Information Security		EFFECTIVE DATE: 04/07/03	

- 4.1.4 The integrity of the data must be ensured (this includes its source, its destination, and the processes applied to it). Changes to data must only be made in authorized and acceptable ways.
- 4.1.5 Continuity of information resources supporting critical governmental services must be ensured in the event of a disaster or business disruption.
- 4.1.6 Security requirements must be identified, documented, and addressed in all phases of development or acquisition of information resources and satisfy all mandated federal compliance requirements.
- 4.2 Owner, Custodian, and User Responsibilities
 - 4.2.1 Owners, custodians, and users of information resources must be identified and their responsibilities defined and documented (see Appendix A).
- 4.3 Classification of Information
 - 4.3.1 Each owner or custodian of information will determine classification based on the circumstances and the nature of the information.
 - 4.3.2 The owner or custodian will determine the protective guidelines that apply for each level of information. They include the following:
 - ? Access
 - ? Distribution within the DHHR
 - ? Distribution outside the DHHR
 - ? Electronic distribution
 - ? Disposal/Destruction (see 3.15, 3.16, and 3.17)
- 4.4 Resource Sharing
 - 4.4.1 Information resources will be shared by all Bureaus/Offices within the DHHR in accordance with applicable state and federal confidentiality laws.
 - 4.4.2 The DHHR will enable and promote interoperability within the DHHR through standardization, training, and the use of IT.
- 4.5 Managing Risks

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0512	REVISION: Original	PAGE 4 OF 6
SUBJECT: IT Information Security		EFFECTIVE DATE: 04/07/03	

- 4.5.1 Under the direction of the Information Security Officer (ISO), periodic risk analysis will be performed and documented.
- 4.5.2 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.
- 4.5.3 A regular review of the DHHR's information security program will be performed at least every two years by an individual(s) independent of the ISO and designated by the Chief Technology Officer (CTO).
- 4.6 Employee/Contractor Practices
 - 4.6.1 Bureaus/Offices will use confidentiality agreements to document the acceptance of agency information security requirements.
- 4.7 Security Awareness and Training
 - 4.7.1 The DHHR will provide ongoing information resources security awareness education for all users.
 - 4.7.2 All employees accessing a mission critical application must receive appropriate training for using that application.
- 4.8 Enforcement Authority
 - 4.8.1 The ISO is the person designated by the CTO to monitor and provide initial enforcement of DHHR's information security program and IT policies.
 - 4.8.2 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.
 - 4.8.3 The OIG (Office of the Inspector General) is the authority who investigates reported instances of departmental employee misconduct.
- 4.9 Violations and Disciplinary Action(s)
 - 4.9.1 All suspected violations of this policy will be reported to a supervisor in the chain of command above the employee.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0512	REVISION: Original	PAGE 5 OF 6
SUBJECT: IT Information Security		EFFECTIVE DATE: 04/07/03	

- 4.9.2 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, Bureau Commissioner, or Community Services Manager (CSM) for appropriate action.
- 4.9.3 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.
- 4.9.4 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 Access – The ability to read, write, modify, or communicate data/information or otherwise use any system resource.
- 5.2 Chief Technology Officer (CTO) – The director of OMIS and the person responsible for all information resources within the DHHR.
- 5.3 Confidential Information – All information not in the public domain.
- 5.4 Control – A protective action, device, policy, procedure, technique or other measure that reduces exposure.
- 5.5 Custodian of an Information Resource – The unit or individual assigned to supply services associated with particular data. (see Appendix A)
- 5.6 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 /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 Information Resources – A collection of manual and automated components, each managing a specific data set or information resource.
- 5.8 Interoperability – The ability of a system to use the parts or equipment of another system.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0512	REVISION: Original	PAGE 6 OF 6
SUBJECT: IT Information Security		EFFECTIVE DATE: 04/07/03	

- 5.9 Mission Critical Information – Information defined by the DHHR to be critical to the DHHR’s function(s).
- 5.10 Owner of an Information Resource – The individual(s) having primary responsibility for the creation and maintenance of the data content. (See Appendix A)
- 5.11 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.
- 5.12 Security Breach – An event resulting in unauthorized access, loss, disclosure, modification, or destruction of information resources, whether accidental or deliberate. (See Appendix A)
- 5.13 User of an Information Resource – The individual(s) who has been granted explicit authorization to access the data by the owners. (See Appendix A)