

DOCUMENT: POLICY	DOCUMENT NUMBER: IT-0511	REVISION: Original	Page 1 of 9
SUBJECT: IT (Information Technology) Network Security		EFFECTIVE DATE: Revised: 02/03/03	
OFFICE OF MIS:		DATE:	
SECRETARY OF DHHR:		DATE:	

1.0 PURPOSE

This policy defines and protects the integrity of the DHHR (Department of Health and Human Resources) network(s).

2.0 SCOPE

This policy applies to all DHHR employees accessing DHHR supported applications and computer systems. It also applies to personnel from other departments, agencies, contractors, and vendors using DHHR's data communications system(s) or networks which may be composed of any combination of LANs (Local Area Networks), or WANs (Wide Area Networks).

3.0 APPLICABLE DOCUMENTS/MATERIAL

Several DHHR regulations and state and federal laws affect the security of information processing resources, computer systems, computer software, and data files. They include the following:

- 3.1 DHHR IT Policy 0501 - Use of IT Resources
Section 4.0 and Appendices A & B
- 3.2 DHHR Policy 0502 - Virus Prevention, Detection, and Removal
- 3.3 MIS (Management Information Services) Operating Procedure-01
Computer Room Security/Access
- 3.4 All DHHR Employee and Vendor Confidentiality Statements
- 3.5 West Virginia Code
§9-7-1, Confidentiality of Records
- 3.6 WV Computer Crime and Abuse Act
§61-3C-4 through 61-3C-21

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0511	REVISION: Original	PAGE 2 OF 9
SUBJECT: IT (Information Technology) Network Security		EFFECTIVE DATE: Revised 02/03/03	

- 3.7 WV GOT (Governor's Office of Technology) Directive
State of WV ITC Information Security Policy
- 3.8 DHHR Common Chapters Manual
Chapter 200 - Confidentiality
Sections 1100 through 1150 - Computer Crimes
- 3.9 DHHR Policy Memorandum 2104 - Progressive Discipline
- 3.10 DHHR Policy Memorandum 2108 - Employee Conduct
- 3.11 Federal Computer Fraud and Abuse Act of 1996
US Code, Title 18, Chapter 47, Section 1030
- 3.12 Electronic Communications Privacy Act of 2000
US Code, Title 18, Chapter 119, Section 2511

4.0 RESPONSIBILITY/REQUIREMENTS

- 4.1 IT Asset Protection
 - 4.1.1 The DHHR CIO (Chief Information Officer) will ensure that IT (Information Technology) assets are protected.
- 4.2 IT Network Security Management
 - 4.2.1 A management committee will provide leadership on IT network security matters in the DHHR.
 - 4.2.2 The ISO (Information Security Officer) will coordinate IT security matters in the DHHR.
 - 4.2.3 Periodic reviews will be conducted to verify compliance to the DHHR's network design, set-up, and configurations; as well as IT security policies and procedures.
 - 4.2.4 Documentation of the IT security controls and procedures in the DHHR must be maintained.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0511	REVISION: Original	PAGE 3 OF 9
SUBJECT: IT (Information Technology) Network Security		EFFECTIVE DATE: Revised 02/03/03	

4.3 User Security

- 4.3.1 All employees are required to comply with all applicable IT security policies and procedures.
- 4.3.2 IT security responsibilities must be defined for relevant employees as part of their job scope.
- 4.3.3 An on-going awareness program must be established to educate and train all employees on DHHR IT security requirements.
- 4.3.4 All software and computing devices used to store, process, and access information related to the DHHR's functions and services must be identified and assessed for legitimacy.
- 4.3.5 Software applications must be updated promptly when security necessitated patches become available.
- 4.3.6 All employees must be educated on procedures regarding security.
- 4.3.7 Employees must be accountable for their computers and for any actions that can be identified to have originated from them.
 - 4.3.7.1 PC's must always be locked or logged off when left unattended.
 - 4.3.7.2 Passwords must never be shared under any circumstances.
- 4.3.8 All programmable computing devices must contain virus protection software.
- 4.3.9 All network connections from computing devices must be identified and verified.
- 4.3.10 When connecting to the DHHR's internal network via remote access, the computing devices will be subject to all DHHR security controls.

4.4 Vendor, Contractor Management

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0511	REVISION: Original	PAGE 4 OF 9
SUBJECT: IT (Information Technology) Network Security		EFFECTIVE DATE: Revised 02/03/03	

- 4.4.1 Vendors/contractors will be subject to the same rules and regulations outlined in this policy.
- 4.4.2 A risk assessment must be conducted to determine the security risks associated with giving a vendor and/or contractor access to a DHHR resource.
- 4.4.3 Security requirements for vendors/contractors must be defined by DHHR and accepted by the vendor/contractor.
- 4.5 Resource Management
 - 4.5.1 An owner must be defined for each IT resource.
 - 4.5.2 The role-based access requirements of employees utilizing the IT resource must be defined.
 - 4.5.3 All access to computing resources will be granted on a need-to-use basis.
 - 4.5.4 Critical system software and files must be routinely backed-up.
- 4.6 Incident Management
 - 4.6.1 Incident response plans supporting the DHHR's security objectives must be established.
 - 4.6.2 Procedures, guidelines, and mechanisms that must be utilized during a security incident will be reviewed as needed.
 - 4.6.3 Roles and responsibilities of the incident management teams must be established and clearly defined.
- 4.7 Authentication
 - 4.7.1 All employees must be authenticated before they are given access to a resource intended for a restricted group.
 - 4.7.2 Appropriate controls must be established and maintained to protect the

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0511	REVISION: Original	PAGE 5 OF 9
SUBJECT: IT (Information Technology) Network Security		EFFECTIVE DATE: Revised 02/03/03	

confidentiality of passwords used for authentication.

4.8 Access Control

4.8.1 Access to the DHHR's assets will be granted on a need-to-use basis.

4.8.2 Access to assets must be approved by the resource owner or a designee.

4.8.3 All access to any DHHR asset must be immediately disabled when access is no longer required.

4.9 Encryption Control

4.9.1 Confidential or sensitive data (i.e., credit card numbers, calling card numbers, log on passwords, etc.) must be encrypted before being transmitted through the Internet.

4.9.2 All sensitive information that requires encryption protection must use a public key or asymmetric cryptography system.

4.10 Database Security

4.10.1 Controls must be established and maintained in the management and administration of the databases. Appropriate authorization must be obtained for access and modification of databases.

4.11 Network Security

4.11.1 Access to network resources must be controlled and limited to authorized employees only.

4.11.2 Networks spanning across the DHHR's boundaries will have defined multiple points, each protected by the appropriate security perimeter and access control mechanisms.

4.11.3 Applications accessible by the public must be placed in the DMZ (demilitarized zone).

4.11.4 The network access firewall and/or secure gateway must be configured to

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0511	REVISION: Original	PAGE 6 OF 9
SUBJECT: IT (Information Technology) Network Security		EFFECTIVE DATE: Revised 02/03/03	

deny all incoming services unless explicitly permitted.

4.12 Network Monitoring and Compliance

4.12.1 NTS (Network and Technical Support) will monitor, oversee, and take actions to safeguard DHHR network traffic and network-based systems.

4.13 Security Operations

4.13.1 Only security tools authorized by the CIO or a designee must be used to enforce the IT security policies and procedures.

4.13.2 Security tools and any information derived from their use must be restricted and will be released as authorized by the CIO or a designee.

4.14 Availability, Recovery and Business Continuity

4.14.1 Each Bureau/Office must work with MIS to define the level of availability required to meet their business needs and service standards.

4.14.2 The DHHR must develop business continuity and recovery plans.

4.14.3 Employees involved in the business continuity and recovery plans must be aware of their roles and responsibilities during a disaster or a service disruption.

4.14.4 The business continuity and recovery plans must be tested periodically.

4.14.5 The DHHR must have documentation of its backup strategy.

4.14.6 Backups of critical business data and resources must be stored in an off-site physically secured environment.

4.15 Enforcement Authority

4.15.1 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.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0511	REVISION: Original	PAGE 7 OF 9
SUBJECT: IT (Information Technology) Network Security		EFFECTIVE DATE: Revised 02/03/03	

4.15.2 The ISL's (Information Security Liaisons) are employees assigned by the Bureau Commissioners and/or Office Directors to assist the ISO in the protection of information resources.

4.15.3 The Secretary of the DHHR has delegated the OIG (Office of the Inspector General) as the primary authority to investigate any reported instances of departmental employee misconduct.

4.16 Violations and Disciplinary Action(s)

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

4.16.2 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, Bureau Commissioner, or CSM (Community Service Manager) for appropriate action.

4.16.3 As determined by Office Directors and Bureau Commissioners, all apparent instances of abuse or misconduct will be referred to the ISO or the OIG for further investigation.

4.16.4 Employees 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 Memorandum 2104; or (2) criminal prosecution. Levels of discipline include:

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

5.0 DEFINITIONS

5.1 Access Control - Hardware, software, and administrative tasks that monitor system operation, perform user identification, and record system accesses and changes.

5.2 Chief Information Officer (CIO) - the director of MIS and the person responsible for

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0511	REVISION: Original	PAGE 8 OF 9
SUBJECT: IT (Information Technology) Network Security		EFFECTIVE DATE: Revised 02/03/03	

all information resources within the DHHR.

- 5.3 Demilitarized Zone (DMZ) - A network added between a protected network and an external network in order to provide an additional layer of security. Sometimes called a perimeter network.
- 5.4 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.
- 5.5 Encryption - the process of scrambling information in a pre-determined way so that it is unintelligible to anyone who does not know how to unscramble it.
- 5.6 Incident or Intrusion - An event that has actual or potential adverse effects on computer or network operations resulting in fraud, waste, or abuse; compromise of information; or loss or damage of property or information.
- 5.7 IT Assets - Any of the data, hardware, software, network, documentation, and personnel used to manage and process information.
- 5.8 Local Area Networks (LAN) - A communications network made up of servers, workstations, a network operating system, and a communications link that serves employees within a confined geographical area.
- 5.9 Malicious Code - Any code added, changed, or removed from a software system in order to intentionally cause harm or subvert the intended function of the system. (Examples of malicious code include: viruses, worms, Trojan Horses, Java attack applets, and dangerous ActiveX controls).
- 5.10 Network - Any number of computers (e.g., PCs and servers) and devices (e.g., printers and modems) joined together by a physical communications link. Networks allow information to be passed between computers, irrespective of where those computers are located; provide the roads for information traffic within a certain environment, and allow employees to access databases and share applications residing on servers.
- 5.11 Network Monitoring- Detection of break-ins or break-in attempts by reviewing logs

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0511	REVISION: Original	PAGE 9 OF 9
SUBJECT: IT (Information Technology) Network Security		EFFECTIVE DATE: Revised 02/03/03	

or other information available on a network. Intrusion detection is essential for maintaining network security.

- 5.12 Network Monitoring Tools - Automated software tools that perform real-time analysis of data traffic, and employ advanced logic to detect patterns of activity that indicate that an intrusion attack is underway.
- 5.13 Network Security - Measures taken to protect a communications pathway from unauthorized access to, and accidental or willful interference of, regular operations.
- 5.14 Network Security Database - This will be established and maintained by the CIO. The purpose of the database is to maintain up-to-date contact information that will identify the emergency contact during a computer or network security incident, and for the dissemination of guidelines and procedures for network security.
- 5.15 Network and Technical Support (NTS) - provides both first and second level support to all computer and network employees throughout the DHHR.
- 5.16 Resource owner - The person or persons designated to administer access rights for the security of an application.
- 5.17 Risk Assessment - An evaluation of: (1) the exposure of an asset to the identified threats; (2) the potential impacts of an event; (3) an estimate of the likelihood of an event occurring; and (4) the effectiveness of existing or proposed safeguards to protect an asset.
- 5.18 Wide Area Network (WAN) - A communications network that connects computing devices over geographically distant locations. A WAN covers a much larger area than a LAN, such as a city, state or country. WANs can either use phone lines or dedicated communication lines.