

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0514	REVISION: Original	PAGE 1 OF 6
SUBJECT: Disaster Recovery Plan		EFFECTIVE DATE: 04/15/05	
OFFICE OF MIS:		DATE:	
SECRETARY OF DHHR:		DATE:	

## 1.0 PURPOSE

The purpose of this policy is to specify requirements and responsibilities for the Department of Health and Human Resources (DHHR), in order to maintain essential services and recover critical systems in the event of major failure or disaster.

Immediately following a disaster, the primary objectives of a disaster recovery plan are: (1) to reduce the risk of disruption of operations and loss of information; (2) to communicate responsibilities for the protection of information and continuity of DHHR operations; and (3) to establish a plan for restoration of information and operations.

Plans and controls will be in place to enable DHHR systems, on and off-site, to continue to operate following a disaster.

## 2.0 SCOPE

This policy applies to all DHHR Bureaus/Offices who operate, manage, or use Information Technology (IT) services or equipment to support critical DHHR business functions.

## 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 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 0441](#) – Safeguards to Protect the Privacy of Protected Health Information
- 3.5 [DHHR HIPAA Policy 0449](#) – General Guidelines to Safeguard Protected Health Information
- 3.6 DHHR IT Policy [0511](#), IT Network Security
- 3.7 DHHR IT Policy [0512](#), IT Information Security

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0514	REVISION: Original	PAGE 2 OF 6
SUBJECT: Disaster Recovery		EFFECTIVE DATE: 04/15/05	

- 3.8 Office of Management Information Services (OMIS) Operating Procedure (OP)-07, Disaster Recovery
- 3.9 OMIS OP-16, Data Backup/Storage
- 3.10 OMIS OP-18, Managing Information Security Incidents
- 3.11 West Virginia Code - [§9-7-1](#), Confidentiality of Records
- 3.12 WV Computer Crime and Abuse Act - [§61-3C-4 through 61-3C-21](#)
- 3.13 DHHR Common Chapters Manual  
[Chapter 200](#) – Confidentiality  
[Sections 1100 through 1150](#) – Computer Crimes
- 3.14 [DHHR Policy Memorandum 2104](#) – Progressive Discipline
- 3.15 [DHHR Policy Memorandum 2108](#) – Employee Conduct

#### 4.0 RESPONSIBILITIES/REQUIREMENTS

##### 4.1 Bureau Responsibilities

- 4.1.1 Each Bureau/Office will create and maintain business continuity and disaster recovery plans in order to effectively resume operations during a disaster or a service disruption.
  - 4.1.1.1 Each Bureau/Office will maintain a disaster recovery plan with procedures designed to provide prompt and effective continuation of critical missions in the event of a disaster.
  - 4.1.1.2 Each Bureau/Office will ensure that all relevant personnel can be contacted when needed to assist in the business continuity and recovery operations.
  - 4.1.1.3 Employees involved in the business continuity and disaster recovery plans will be aware of their roles and responsibilities during a disaster or a service disruption.
  - 4.1.1.4 All plans and procedures will undergo annual managerial review of disaster recovery considerations to update technical, environmental, procedural, or administrative changes that may occur.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0514	REVISION: Original	PAGE 3 OF 6
SUBJECT: Disaster Recovery		EFFECTIVE DATE: 04/15/05	

4.1.1.5 Each Bureau/Office is responsible for periodically testing their disaster recovery plan(s).

4.1.2 Each Bureau/Office will designate or appoint a Disaster Recovery Coordinator.

4.1.3 Each Bureau/Office will periodically assure that all critical systems and data are being promptly identified to OMIS in order for proper maintenance.

#### 4.2 OMIS Responsibilities

4.2.1 OMIS will provide management and technical support to agencies during development and/or execution of their disaster recovery plans.

4.2.2 OMIS will designate an agency Disaster Recovery Consultant, who will work with the Disaster Recovery Coordinator to document a feasible disaster recover plan for each Bureau.

4.2.3 OMIS will maintain the ability to process critical information in the event of a disaster.

4.2.4 OMIS will maintain an inventory of all OMIS approved hardware, software, and service contracts, including contact information, for IT systems.

4.2.5 OMIS will provide security services, where feasible, to protect information assets from theft, alteration, and/or loss of confidentiality.

4.2.6 OMIS will provide monitoring of critical network hardware and services during non-business hours, by a combination of monitoring tools and on-call Network and Technical Support (NTS) and Data Center Desktop Support (DCDS) staff.

#### 4.3 Information Resources

4.3.1 Continuity of information resources supporting critical services must be ensured in the event of a business disruption or a disaster.

4.3.2 The expense of security safeguards must be cost effective and equal to the value of the assets being protected, as determined by a risk analysis.

#### 4.4 Backups (see OP-16, *Data Backup/Storage*)

4.4.1 The DHHR will have a documented definition of its backup strategy, which will minimally include periodic backup of critical business information systems.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0514	REVISION: Original	PAGE 4 OF 6
SUBJECT: Disaster Recovery	EFFECTIVE DATE: 04/15/05		

4.4.2 Backups of critical business data and systems will be stored in a physically secured environment, which will be located at a safe distance away from the originating facility to escape a local disaster.

4.4.3 Backups of critical business data and systems that have been archived for a prolonged period of time will be tested regularly to ensure the information is recoverable and usable.

#### 4.5 Enforcement Authority

4.5.1 The Information Security Officer (ISO) is the person designated by the 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 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.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0514	REVISION: Original	PAGE 5 OF 6
SUBJECT: Disaster Recovery		EFFECTIVE DATE: 04/15/05	

## 5.0 DEFINITIONS

- 5.1 Archive – (1) A long-term storage media, often on magnetic tape, for backup copies of files or files that are no longer in active use. (2) To move data to a less accessible or less expensive storage media or method.
- 5.2 Backup – To copy files from one storage area, especially a hard disk, to another to prevent their loss in case of a disk failure.
- 5.3 Chief Technology Officer (CTO) - The director of OMIS and the person responsible for all information resources within the DHHR.
- 5.4 Critical Business Data – Data that must be backed up frequently because of its importance to the IT system.
- 5.5 Data Center Desktop Support (DCDS) – The OMIS organization that is responsible for the DHHR Data Center and the Kanawha County offices.
- 5.6 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).
- 5.7 Disaster Recovery Plan – A plan that applies to major, usually catastrophic, events that deny access to the normal facility for an extended period. This IT focused plan is designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency.
- 5.8 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.
- 5.9 Information Resources – A collection of manual and automated components, each managing a specific data set or information resource.
- 5.10 Network and Technical Support (NTS) - This group provides first and second level support to all computer and network users in the DHHR field offices.

DOCUMENT: <b>Policy</b>	DOCUMENT NUMBER: <b>IT-0514</b>	REVISION: <b>Original</b>	PAGE <b>6</b> OF <b>6</b>
SUBJECT: <b>Disaster Recovery</b>		EFFECTIVE DATE: <b>04/15/05</b>	

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.