

**CENTER FOR NUCLEAR WASTE  
REGULATORY ANALYSES**

Proc. AP-018

Revision 0 Change 0

**ADMINISTRATIVE PROCEDURE**

Page 1 of 6

**Title AP-018 ELECTRONIC FILE ARCHIVAL AND BACKUP PROCEDURES**

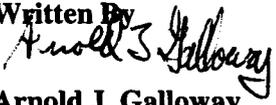
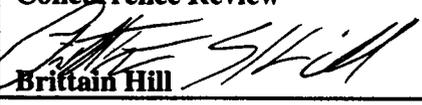
**EFFECTIVITY AND APPROVAL**

Revision 0 of this procedure became effective on October 13, 2000. This procedure consists of the pages and changes listed below.

<u>Page No.</u>	<u>Change</u>	<u>Date Effective</u>
All	0	10/13/2000

**Supersedes Procedure No. None**

**Approvals**

<b>Written By</b>  Arnold J. Galloway	<b>Date</b> 10-13-2000	<b>Concurrence Review</b>  Brittain Hill	<b>Date</b> 10/13/00
<b>Quality Assurance</b>  Bruce Mabrito	<b>Date</b> 10/13/2000	<b>Cognizant Director</b> 	<b>Date</b> 10/13/00

# CENTER FOR NUCLEAR WASTE REGULATORY ANALYSES

Proc. AP-018

Revision 0 Change 0

## ADMINISTRATIVE PROCEDURE

Page 2 of 6

### AP-018 ELECTRONIC FILE ARCHIVAL AND BACKUP PROCEDURES

#### 1. PURPOSE

The purposes of this procedure are to define backup, archives and disaster recovery methods and/or processes, and delineate the responsibilities for copying, storing and retrieving data on various media that reside in the disk drives of CNWRA servers and clients (e.g., workstations).

#### 2. DEFINITIONS

**Administration Tool** – A system administration utility with a graphical interface that enables administrators to maintain system database files, printers, serial ports, user accounts, and hosts.

**Archive** – The storage of a backup outside of the original device that was used to generate the backup, for possible review or recovery at a later date. This may be a local or off-site archive.

**Backup** – The process of copying electronic file system data to alternative media from the hard disk drive on which the data originally resided, (e.g., tape, CD-Rom, Zip disk), and the media that results from that process.

**Client** – Desktop unit that is dependent on a server for some of its processes (e.g., security).

**Disaster Recovery** – Recovery of data in case of a catastrophic event at the local site (e.g., fire, flood, an intentional malicious destruction of original files) using an archive that typically is stored off-site or in an on-site facility that is safe from any disaster and its effects.

**Disk Mirroring** – a feature used to guard against component failure by writing the same data to two or more disk drives at the same time.

**Full backup** – Backup of all selected data on a LAN.

**Incremental Backup** – The process of saving all data created or modified since the previous backup was performed; incremental backups are performed more frequently than full backups.

**Local Area Network (LAN)** – The portions of a network that servers and processes have direct control over.

**Multi-Volume Backup** – A backup where the data to be copied require more than one tape cartridge or diskette.

**File** – A plain file is a file containing data. The data may be text or other content.

**Restore** – The process of copying files and directories from backup to hard disk for review or recovery.

# CENTER FOR NUCLEAR WASTE REGULATORY ANALYSES

## ADMINISTRATIVE PROCEDURE

Proc. AP-018

Revision 0 Change 0

Page 3 of 6

Server – A host process that communicates to a client process. Commonly, the term server is used to refer to a host that provides network processing and storage resources to one or more clients. These resources may include logon security, shared storage devices, e-mail, network printer control and other functions that are performed more efficiently when controlled with a centralized process. A server is connected to the clients it serves through a LAN.

### 3. RESPONSIBILITIES

#### 3.1 Technical and Support Staff

Staff members shall familiarize themselves with the manufacturer's operating instructions for the appropriate media storage device prior to its usage. Staff members shall be familiar with relevant portions of Quality Assurance Records Control Procedures (QAP-012) and must use the desktop backup devices to meet its requirements, as appropriate. If any backup is generated to satisfy the provisions of section 3.2 of QAP-012, it is each staff member's responsibility to provide that backup with their scientific notebook to the Quality Assurance Director at the normal 6 month interval. It is not mandatory that staff members backup any other data on their desktop systems, however they may do so at their discretion.

#### 3.2 NT Administrator

The NT administrator is responsible for ensuring the availability of an adequate supply of the correct tapes to meet the backup requirements stated in section 4.2.1. The NT Administrator shall verify via the Administration Tool that the backups were performed successfully and change out the tapes at the appropriate time. Restoring data from the automated NT backup system will be performed by the NT administrator. The NT Administrator will install any software updates or patches that pertain to the NT servers.

#### 3.3 UNIX Administrator

The UNIX Administrator is responsible for ensuring the availability of an adequate supply of the correct tape cartridge to meet the backup requirements stated in section 4.2.2. The UNIX administrator will verify via the Administration Tool that the backups were performed successfully and change the tapes at the appropriate time. Restoring data from the automated UNIX backup system will be performed by the UNIX administrator. The UNIX Administrator will install any software updates or patches that pertain to the UNIX backup server.

#### 3.4 IMS Project Manager

The IMS Project Manager periodically will verify that the NT and UNIX administrators have performed their tasks correctly & ensure there is an adequate supply of backup media for staff needs. The IMS Project Manager will provide support in the absence of either of the administrators and will contact vendors for hardware failure support if required.

# CENTER FOR NUCLEAR WASTE REGULATORY ANALYSES

## ADMINISTRATIVE PROCEDURE

Proc. AP-018

Revision 0 Change 0

Page 4 of 6

### 4.0 PROCEDURES

#### 4.1 Desktop Backup

CNWRA staff members have multiple methods of data backup available to them at their desktop or through the support staff. Automated backup of hard drives "D:" and above will be accomplished per section 4.2. Data to be part of the automated backup must be moved to one on these hard drives. Data stored on the "C:" drive will not be part of the automated backup and the staff member must back this data up manually to meet the requirements of QAP-012. Blank storage media are available in the IMS Laboratory, room A136 in building 189.

##### Technical Staff Desktop NT units

Desktop NT units (personal computers) have been equipped with read/writeable devices to allow the user to individually create backups of critical data and computer records. These backups will be maintained by the individual users. Those required to meet requirements of QAP-12, 3.2.1 will be stored in QA records.

##### Support Staff Desktop NT units

Support staff desktop NT units (personal computers) are equipped with read/writeable units. This allows the support staff to backup large specific files resident in any computer over the LAN. These backups will be maintained by the individual users. Those required to meet requirements of QAP-12, 3.2.1 will be stored in QA records.

##### Sun Microsystems and Silicon Graphics UNIX based units

All of these units are on the LAN and some have a tape drive (4mm or 8mm) attached directly to them. These drives can be used to back up specific data. These backups will be maintained by the individual users. Those required to meet requirements of QAP-12, 3.2.1 will be stored in QA records.

#### 4.2 Automated Network Backup

The CNWRA IMS group is responsible for automated network backup and archiving as set forth in section 3.

##### 4.2.1 Backup of Windows NT Systems

The backup of the NT portion of the LAN will be accomplished with a read/writeable device connected to the LAN. Full backups will be accomplished automatically once a month after normal business hours. Incremental backups will occur each evening of the normal work week.

# CENTER FOR NUCLEAR WASTE REGULATORY ANALYSES

Proc. AP-018

Revision 0 Change 0

Page 5 of 6

## ADMINISTRATIVE PROCEDURE

The NT Administrator removes the tapes that are to become part of the archive once a month. The most recent backup is then placed in the fireproof safe to become the local archive. The existing archive tapes that are in the fireproof safe are then transferred for disaster recovery purposes to the storage facility at Iron Mountain, an off-site storage facility. The archive tapes already at Iron Mountain then are rotated back to the CNWRA. See figure #1.

Instructions for use of the backup/restore software can be found on the manufacturers CD, or in the user manuals that are kept in the IMS Lab.

### 4.2.2 Backup of UNIX portion of CNWRA LAN

Full backups will be accomplished automatically once a month after normal working hours. Incremental backups will occur each evening of the week. This system backs up all UNIX equipment.

The UNIX Administrator removes the tapes that are to become part of the archive once a month. Those tapes subsequently are labeled and stored in the fireproof safe in the IMS Laboratory. The label includes the dates corresponding to the backup from the UNIX system. The existing archive tapes that are in the fireproof safe will be transferred for disaster recovery purposes to the storage facility at Iron Mountain, an off-site storage facility. The archive tapes already at Iron Mountain then are rotated back to the CNWRA. See figure #1.

The disk mirroring capabilities of the UNIX applications server will be used to provide a redundant file system in case of a hard disk failure in the primary UNIX applications server. In case of disk failure, the UNIX Administrator would be notified via a console pop-up message. At that time the UNIX administrator will contact the appropriate vendor for further corrective action.

A scheduled backup will be run during periods of low network traffic so as to not encumber machine resources during business hours.

For specific instructions on using the backup/restore administration program, refer to the online help or the manufacturer's manuals.

## 5.0 COMMERCIAL APPLICATIONS SOFTWARE

Commercial applications software is loaded on Drive "C:" and will not be backed up. However original copies will be kept in a fireproof safe for purposes of disaster recovery.

## 6.0 DATA RETRIEVAL

Incremental backup will be used to recover any file or set of files lost. Files can be recovered for three months. The backup tapes are reused after that. Full backup will be used to recover from a major disaster in which all data is lost.

**CENTER FOR NUCLEAR WASTE  
REGULATORY ANALYSES**

**ADMINISTRATIVE PROCEDURE**

Proc. AP-018

Revision 0 Change 0

Page 6 of 6

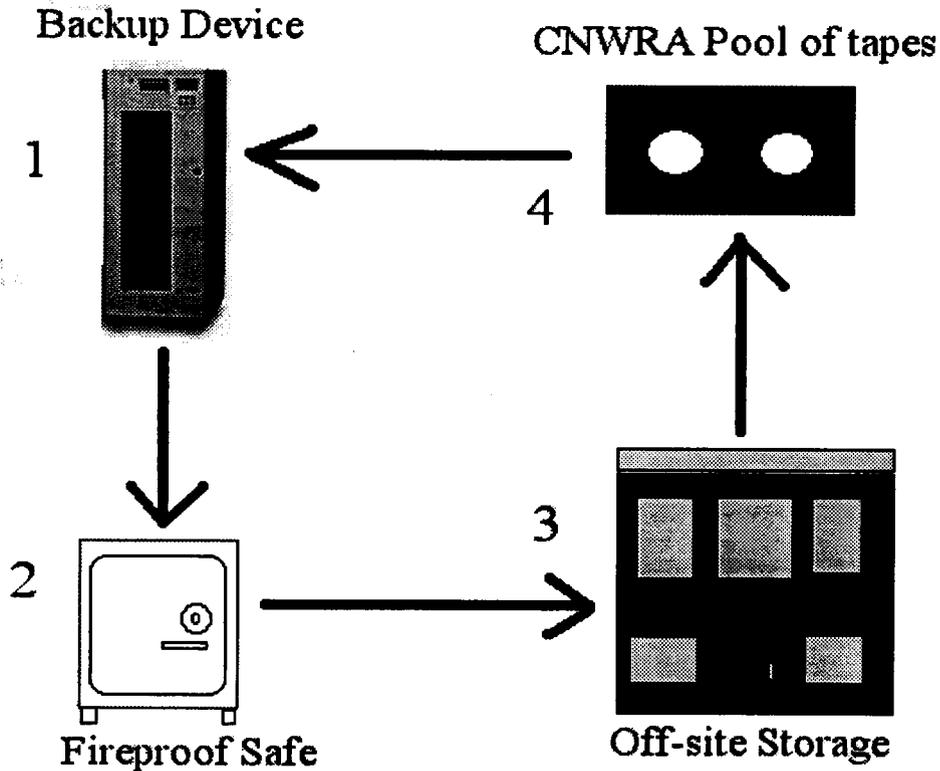


Figure 1: Three consecutive sets of backup are available at any time. Each set contains incremental backups for all days of the month and at least one full backup for the month.

**7.0 Records**

This procedure in itself does not generate any QA records. Therefore no QA record requirements exist for the actual process. However the retention of backups in accordance with QAP-012 section 3.6 applies to this procedure.