Version June 2023

Recommendations for Developing & Managing AIRS Backup Protocols

(Changes made since the last "version July 2021" - Modification to Section 5. A)

Introduction

Maintaining AIRS is critical to both service delivery and your agency's reporting requirements to the AIDS Institute. A lot can happen in day-to-day computer operations that might disrupt this. Hardware can fail. Networks can malfunction. Viruses can render data unusable. Locations can be hacked. Human error can accidentally delete software and/or its associated data. Because any of these unfortunate events might happen, it is essential that an agency maintain Data Backups, such that when adverse events occur, the agency can return to normal AIRS data entry operations as soon as possible.

This document was created to provide recommendations regarding sound backup practices. While these are only recommendations, it is up to AIRS users and system administrators to ensure that an appropriate backup plan is developed and implemented. The AIDS Institute cannot assume responsibility for lost or corrupted AIRS data. Proper procedures must be followed to ensure the security and protection of your AIRS data.

Section 1: Backup Plan Development and Review

A) If your agency has not already developed a plan for backup of AIRS data, please begin the process.

- As part of the development process, it is advisable for program staff, agency IT staff, and/or consultant IT staff to be involved in all phases of development and review.

B) The backup protocol should be tailored to the organization. At a minimum, a backup protocol should address the following.

1) What data is backed up
2) How data is backed up
3) Where and how it is stored
4) Frequency of backup
5) Persons responsible
6) How failed backups are handled

C) Once developed, appropriate staff should review and update it, at least annually.

D) Staff who maintain AIRS, including data entry staff and staff responsible for maintaining overall data quality, should be given copies of the protocol when it is finalized or updated.

Section 2: Backup – Methods, Frequency, and Naming

As noted in the backup survey, there are multiple ways to handle a backup. Most common are the AIRS Backup Utility and third-party backup software running on a network. We recommend utilizing both methods.

A) If your agency is using the AIRS Backup Utility, please review the tutorial and documentation that is available on the *www.AIRSNY.org* web site. For your convenience, the document and video are linked below:

AIRS Backup Steps
AIRS Backup Video

B) The agency AIRS backup protocol should specify how frequently backups of AIRS will be made.

- Backup frequency should relate to the volume of data being entered. Agencies with a high volume of transactions per day, or with a larger data set, should consider backing up more frequently (perhaps daily or twice per weekly).
- Ideally, backups should be done **daily**. However, smaller organizations with fewer clients and lower volume of data entry might consider a less frequent backup but not less than *weekly*.
- We suggest your agency discuss this with IT staff and/or IT consultant and modify your document, if needed.
- Each backup file should be given a *unique* name that includes a date. Please do NOT use the same file name more than once because the most recent backup would overwrite the previous one.

C) If you are using third-party backup software to backup AIRS files and data, it is advisable that someone confirm the AIRS files are successfully included with every backup.

- Since all third-party software works differently, please have the appropriate staff consult the software's backup manual. If you are unclear about this, please ask your IT staff or IT consultant for help. Many types of third-party backup software keep a log of what has been backed up, each time.

Section 3: Backup – Staff Responsibilities

A) Your agency's backup protocol should identify both the designated staff member responsible for initiating backups and an alternate. Both should receive appropriate training.

- Once trained, the designated and alternate staff should demonstrate they can handle and coordinate all aspects of running the backup.

B) Because staff and assignments can change, the backup protocol should be updated, as needed, to reflect current operations.

- All staff involved with AIRS data should know who is currently responsible for the backups.
- The handling of absences and vacation coverage should also be noted in your protocol.
- The backup protocol should be routinely redistributed when there are staffing responsibility changes.

Section 4: Monitoring the Success (or Problem) of a Backup

A) It is important that staff responsible for backups monitor successful completion.

B) Backup Protocols should address what happens when a backup does not complete successfully. The best approach would be to have all staff log out of AIRS and then to retry the backup.

- Repeated backup failures should be addressed with IT staff, consultants, AND Netsmart. The agency will need to decide, in conjunction with AI IT staff/consultants and Netsmart, whether they should continue to enter data in the absence of viable backups.

Section 5: Maintenance and Storing Backups

A) Agency should maintain backup files:
- Save the first or last backup of the month to build a historical backup archive.
- Backup files should be password protected and encrypted.
- Backup files should be copied to encrypted, external media (USB, external hard drive, Cloud, etc.) for storage.

  - DO NOT save backups to:
    - The same network drive (server) where AIRS is located, or
    - The local hard drive if AIRS is located on a stand-alone PC.
    - If the file server for AIRS or local drive fails, then backups may be lost.
- Backup files should be stored in a secure location. Copies should also be stored off-site to ensure access and recovery in the event of a physical disaster.
- DO NOT restore from an older backup unless instructed by Netsmart.

Section 6: Restoring from a Backup

DO NOT attempt to restore from backup until your agency contacts both Netsmart and your AI Technical or Data Unit staff.

- Although the AIRS Backup from AIRS Utilities contains all the data, it does not include all the files needed to restore a working AIRS system. Netsmart/AI will help you select the right backup file and ensure you follow the correct procedures. If you are using a network backup, rather than the AIRS backup utility, please also include your IT Staff and/or consultant in the contact.