

Ash Fall Project

AFP-AP-05, Attachment B – Process Control Examples

Section 1 – Protecting Information from Damage or Destruction

The following examples of process controls are provided for different systems and equipment:

Servers

- Access privileges are set to prevent unauthorized changes.
- Server is periodically backed up and the backups are appropriately labeled and stored.
- When putting files in a different directory or folder:
 - To retain current access privileges, files must be moved (e.g., dragged and dropped), not copied and pasted.
 - To assume the access privileges of the destination directory or folder, files must be copied and pasted, not moved (e.g., dragged and dropped).

Workstations/Personal Computers

- Access to information contained on personal computer is controlled (e.g., password protected and controlled physical access).
- Before changes are made, secured backup copies are created, appropriately labeled and stored, and kept until the changes are confirmed as correct.

Instruments

- Information is copied to a backup medium and the medium is appropriately labeled and stored.
- Any hard copy printouts generated are kept until the backup copy has been verified.

Section 2 – Describing How Information Will Be Stored

- Access controls
- Environmental protection consideration such as humidity, heat, etc
- Location of storage (onsite, offsite)
- Media protection (how different types of media are to be stored)

Section 3 – Identifying Electronic Media

Physical Electronic Media

- Medium type (tape, diskette, compact disk-read-only memory, etc.)
- Appropriately labeled with:
 - Date and time backup or copy was made

- Source of backup (i.e., identify the computer system instrument, or other system that was the source of the information), discovery name, and file name
- System utility used to perform backup
- Format of the backup media
- Method of transport (mail, courier, etc.)
- Method of integrity verification upon receipt delivery (backup listing, file checksums, application/utility for verifications, etc.)
- Method for verifying/confirming delivery of storage or transfer medium

Non-Physical Electronic Media

- Transport mechanism (e-mail, transmission control protocol/internet protocol, etc.)
- Utility and settings (file transfer protocol, copy, mail attachment, etc.)
- Method of receipt verification (visual inspection, transmission verification settings, checksums, application information integrity check, etc.)

Section 4 – Maintaining Information Accuracy and Completeness

- A complete inspection of the information
- Random sampling of the information
- Checksums or cyclic redundancy checks
- Comparison of source hard copy to electronic input
- Other standards and methods, as appropriate

Section 5 – Ensuring Error-Free Data Transfers

- Check sum
- File size
- Visual verification

Section 6 – Ensuring Security and Integrity of Information Maintained

- Maintain documentation for each person with write access to the electronic information management system or electronic media, including the name and signature of the person approving such access, and the date approved.
- Implement system level or internal application controls to give individual users the appropriate level of security access to the electronic information management system or electronic media.
- Perform periodic operational security checks of the electronic information management system or electronic media to detect any unauthorized entry and other breaches in the security system that could compromise the integrity of the information.