Audit Trails

Audit Trail policy:

- The following functions must be recorded:
  - log-in attempts,
  - password changes, and
  - file creations, changes and/or deletions.

- The audit trail event record should specify:
  - type of event,
  - when the event occurred,
  - user ID associated with the event, and
  - program or command used to initiate the event.

- Audit trails must be reviewed weekly by the Large Security Application Security Officer or other authorized agency individuals who are not regular LSA users or who do not administer access to the LSA. The ISSO must review the audit trail monthly.

- Anomalies must be immediately reported to appropriate supervisory and/or ISSO for follow-up action.

- All LSA audit files shall be stored in a locked room and kept for three years.

Compliance

Unauthorized personnel are not allowed to see or obtain sensitive data. The gross negligence or willful disclosure of LSA information can result in prosecution for misdemeanor or felony resulting in fines, imprisonment, civil liability, and/or dismissal.