

Standard Operating Procedures

Subject: Network Data Security

Date: 15Jun2006

Purpose: The purpose of this Standard Operating Procedure (SOP) is to define the minimum standards of data security. Keeping data secure insures that data will not be lost or compromised.

Scope: This procedure applies to all data at the FPG Data Management and Analysis Center (DMAC).

Responsibility: Maintaining data security is the responsibility of the network administrator in IT Services assigned to maintaining the network drives used by the Data Management and Analysis Center. The network administrator is responsible for notifying DMAC of any changes in the security procedures.

Security Review Procedure

- Data Access Security procedures:
 - Passwords for individuals are set to automatically expire every 120 days.
 - Only programmers and statisticians have rights to files and directories that contain sensitive data unless data is currently being entered.
 - Data entry personnel only have access to files and directories where they are entering data.
 - When a programmer, statistician, or data entry person leaves DMAC, their account is immediately disabled and ultimately deleted.
- Software Security Procedures:
 - The administrator must review security alerts distributed on campus by UNC ITS.
 - The administrator must review alerts and or subscribe to mailing lists put out by CERT for major security holes in software (at www.cert.org).
 - The administrator must apply software patches as needed from Novell to keep the server software secure.
 - The administrator must set up logs and review them to monitor possible security breaches.
 - The administrator must maintain backups as needed to recover from deliberate damage.