SOP: SOPCOMSEC - Computer Security
Last date revised: December 26 2009
Date approved: December 26 2009

COMPUTER SECURITY AND DATA SAFETY

PURPOSE:

This document proposes procedures that will prevent unwanted access to documents and data by unauthorized users.

POLICY:

All secure data and documents will be stored on computer disks that are protected by encryted passwords and the data containing computers will not be connected by wired or wireless internet networks to the Word Wide Web.

RESPONSIBILITY:

The X-ray Laboratory personell will be responsible for security issues.

MATERIALS:

- External Hard Disks
- Encrypted Password Protection for all Hard Disks

PROCEDURE:

Approve: JHR 1/8/2009

1. Unprocessed data will be collected on the X-ray instruments. No data processing on data collection instruments will be undertaken.
2. Code names will be used for all data identification. At no time will chemical information or other identification will be included in the data collection material or data.
3. Unprocessed data will be immediately transferred to the encrypted password protected external hard drive and then deleted from the original data collection device.
4. The external hard drive will be removed from a secure location and directly install on a processing computer that is not connected to the Internet.
5. The hard drive will be installed and the appropriate password will be used to access the drive.
6. Data processing will be finished on the processing computer
7. Results will only be released to original user contact. No data will be released to any user without express permission from the originating user.
8. Results and data will not be transferred over unsecured Internet connections without the express permission of the originating user.
9. If results and data must be transferred over the Internet then those files should be archived as zip files and password protected. Passwords for archived files will be sent to the originating user before transfer of the archived files.
10. Once complete the data and results will be archived on password-protected media and the external hard drives will be removed and stored in a secure location.

Approve: JHR 1/8/2009