P601

Computer and Database Security

Created 10/96
Revised 03/02

Approved by Ronald E. Filipy, Director
March 2002

This policy specifies requirements to maintain and ensure the integrity and security of the database in accordance with applicable laws and regulations and bioethical considerations.

Legal and ethical requirements form the basis for protection

Both Washington State law and the Federal Privacy Act as well as bioethical considerations require that information such as is included in the USTUR computerized database be maintained confidential. In addition, the network and individual computer work stations contain unpublished research results and other intelectual property to which access should be limited.

Access to computer network and database is limited to specific individuals

Except as may be otherwise required by law, access to the USTUR computer network and database shall be limited to Registries staff and faculty who have need for such information in their daily activities, and who have on file a valid, signed confidentiality agreement (see F106). Individual access shall be limited to those specific portions of the database that are necessary for the research or other activities of the staff or faculty member.

Network Supervisor is responsible for computer and database security

The overall security and protection of the USTUR computer network and database are the responsibility of the Systems and Programming Professional who shall develop, and, with the concurrence of the Director, incorporate such physical and administrative controls as are necessary to ensure the integrity and security of the network.

Computer network access is password protected

Each Registries faculty and staff member to whom network access has been granted shall be issued a unique password by the Network Supervisor. This password shall be used only by the individual to whom it is assigned to gain access to the Registries network, and shall not be revealed to any other individual. Each Registries staff member is responsible for maintaining and protecting the confidentiality of his/her assigned password. Passwords thus should not be kept in written or electronic format accessible to others. If any password holder has reason to suspect that the confidentiality of his/her password has been breached, he/she shall, in writing, so advise the Director who shall, in conjunction with the Network Supervisor, arrange for issuance of a new password. Passwords shall be changed annually. A list of all passwords shall be maintained by the Director or his designate in a sealed envelope in a secure location. Such envelope shall not be opened except as indicated by contingencies.

Database access has separate password protection

Access to the database is gained through the network and requires a separate specific password. The password shall grant read-only access to the general database. Write access shall be granted to those Registries staff for whom such access is necessary to their job assignments and shall be limited to those portions of the database needed for the job assignment.

Backup of database shall be accomplished weekly

The database system manager shall make a complete and separate backup of the Registries database weekly and shall maintain at least three such historical backups in a secured location.

Shredding material with personal identifiers

All printed or copied database material that includes any Registrant personal identifier; i.e., name, date of birth, address, etc., must be shredded before being discarded.