Guidelines for
Distributed Computing Administration and Security

As the University enters into the era of networked microcomputers and a distributed computing environment, many of the critical tasks originally completed by hand, or centrally on SIU'S mainframe computers, have been or could be transferred to microcomputers at the department level.

University data and information are valuable resources; their safety is imperative. These guidelines provide a University-wide set of standards applicable to microcomputing administration and security. It is the responsibility of individual campus units to develop operating procedures which implement the guidelines.

Local and Central information technology staff

Local (departmental or college) computing professionals play an important yet distinct role from central information technology and academic computing professionals. While central staff are available to serve the entire campus, departmental technical experts serve their designated department(s).

Central information technology staff can play an influential role in local technical support by assisting University departments in training and supporting departmental trainers. As resources allow, central information technology staff may provide consultative services to local computer support personnel regarding new technology acquisitions and problem resolution. Together, local and central staff may assist with institutional planning for technology and developing computer standards.

Roles and Responsibilities: Central Information Technology

Typically, but not always, central information technology professionals will assume responsiblity for all computing infrastructure “behind the wall” which includes routers, hubs, cables, bridges, gateways, wiring, and all other equipment, computer hardware, or computer software which enables a department’s computers to link into the wider campus area network and computing services.

Upon departmental request or by campus decision, campus units may contract with central information technology staff to provide basic LAN management services “from the wall out”. However, within each unit, a local information technology liaison should coordinate all computing resources and support

Central information technology staff are charged with identifying software and hardware needs that cross departmental boundaries. They should monitor the technology environment at large and recommend computer hardware with the longest potential life for the campus community. Campus information technology experts should work with the Purchasing Department in particular and the campus in general to regularly recommend standards for computer hardware configurations and to obtain quotation prices from vendors.

Central information technology staff share the responsibility with local technical personnel to recommend and support application software that facilitates compatibility between all users of SIU’S computing resources.

Roles and Responsibilities: Local Information Technology

Typically, but not always, local information technology staff will assume responsibility for trouble-shooting problems

"from the wall out" to the user. This includes diagnosis of: software problems; basic microcomputer maintenance problems such as changing the battery, adding cards, checking wiring, and all other fairly routine hardware complaints; restoring back–up data when requested; and assisting the end user to employ the University's computing resources in an efficient and effective manner.

Designated Local Technical *Support*

Within each unit, all local computer resources shall be maintained by an employee officially designated as the information technology expert. This individual need not perform computer administration and security tasks exclusively. However, a portion of this employee's appointment must be devoted to departmental computer support. Alternatively, a unit may contract with an outside vendor to provide local technical support; in that case, a designated SIU employee will act as liaison with the computer support service provider.

Training

At a minimum, all local technical professionals must receive basic training in their departmental Operating System and in their Network Operating System if the department maintains a LAN server. This training may be acquired on campus or externally. One or more departments may wish to pool resources to negotiate discounted training for their computer support professionals.

Since computer technology changes daily, local technical professionals must continually update their computing skills. Therefore, the University requires that all local information technology experts annually receive continuing education in the computer technology field. Continuing education may be campus-based (e.g. provided in a user group format) or provided by external vendors. The University also encourages LAN managers to

pursue professional certification or to meet the requirements for computer-support positions as established by the Civil Service System.

Areas of training that are recommended for departmental information technology professionals include, but are not limited to: trouble-shooting microcomputer and network hardware problems, peripheral support, computer security, and training in the application software adopted by their department as standard desktop applications (i.e., word processing, Internet, electronic mail, spreadsheet, etc.).

LAN Management

If computers in the department are networked and the LAN is not maintained centrally, then the department must designate an employee as LAN Manager. LAN managers do not have to perform LAN administration and security procedures exclusively, but a portion of their appointment must be devoted to these tasks. The same employee can serve as local expert and LAN manager.

Departments may contract with other campus units, such as the Office of Information Technology, to obtain LAN management services. Several departments may share a single LAN manager. Also, LAN management tasks may be out-sourced to external vendors, but an SIU employee must assume responsibility for the successful performance of network security guidelines.

LAN Managers, whether at the local or central level, must perform or oversee the performance of routine maintenance tasks on a regular basis. These tasks include, but are not limited to: backing up the server; monitoring usage logs; setting up user groups and directories; scanning for computer viruses; monitoring software usage to ensure compliance with software license agreements; managing associated property and supplies; maintaining key documentation; and establishing and implementing

computer security measures.

Computer Security

Local computing professionals are responsible for implementing physical and logical security measures to safeguard the University's microcomputer equipment and information. Physical security measures must address the safety of: computer hardware and software; local computing peripherals; diskettes; back-up media; and hard copy of computer information.

Logical security measures must be established to guarantee that the University's confidential and critical data and information are protected from access by unauthorized computer users. Procedures must be performed to secure system access points, including modems and hubs from unauthorized intrusion.

Logical security measures include, but are not limited to: unique passwords; expired passwords; system lock-outs after failed log-on attempts; proper disposal of electronic and paper copies of data; virus detection; encryption of openly transmitted data; and all other security measures which guarantee the safety, privacy and integrity of SIU data and information.

Because technology changes rapidly, computer security procedures should be reassessed on a regular basis. The most current security practices should prevail on the campuses. Security software, such as virus protection software, should be updated regularly.

User Education

Part of local technical support's responsibilities include educating all computers users assigned to their area about basic microcomputer controls. Training duties include, but are not limited to, educating the user about: back-up and data

restoration procedures; University computer policies; security procedures; computer virus scanning; and any other information related to compliance with state or federal law and SIU'S computer policies and procedures.

Local technical personnel can establish a forum for information-sharing and training by forming users' groups where appropriate. The University supports and welcomes such users' groups if their primary purpose is to provide education and training to SIU computer users to facilitate the operations of the University.