Code of Responsible Computing

This policy provides guidelines for the administration and use of all computing resources at the University of Scranton. Computing resources include timesharing systems, workstations, personal computers, networks, peripheral equipment, laboratories, and software. They are available for use by authorized individuals including students, faculty, staff, and administrators in compliance with the policy outlined below.

Each user shall act in an ethical manner consistent with the stated goals and mission of the University of Scranton.

Each authorization, including access code, password, file directory and file contents is intended for use by the individual, department, or school receiving the authorization. Each user accepts responsibility for her/his use of computing resources. Users should take adequate precautions against the misuse of computing resources.

The information created, transmitted, or stored on University of Scranton computing resources is presumed to be confidential.

The University has a responsibility to provide appropriate security, to maintain reliability and data integrity, and to enforce this policy. However, privacy and confidentiality cannot be guaranteed because of the nature of the resources involved.

Unauthorized use of a computing resource includes but is not limited to the following or any deliberate attempt to accomplish the following:

- unauthorized copying of software which is licensed or protected by copyright
- any unauthorized commercial use
- use of a resource without authorization
- damaging equipment
- degrading performance
- harassment of other users
- depriving users of their access to computing resources
- preventing the university from fulfilling its responsibilities under this policy.

Unauthorized use or any violation of this policy is subject to investigation and enforcement as outlined in the "ENFORCEMENT GUIDELINES FOR THE 'CODE OF RESPONSIBLE COMPUTING'". Investigation may require the suspension of access to computer resources and inspection of files. Enforcement of this policy with regard to due process may lead to University disciplinary action, and/or prosecution under state and federal law.

It is the responsibility of all users of computing resources to understand and abide by this document and the aforementioned related document. Copies of both documents may be obtained from the Office of [------].

ENFORCEMENT GUIDELINES FOR "CODE OF RESPONSIBLE COMPUTING"

Investigations of suspected computer abuse should be conducted with every effort to assure the proper balance of duties and rights of all parties involved. These guidelines provide certain procedures to follow during an investigation. They also provide for the establishment of a Computer Use Board.

Actions taken under these guidelines are not sanctions but a way of handling an immediate problem. They are taken to assure the quality of computing for the whole university community.

Role and membership composition of the Computer Use Board.

The Computer Use Board (CUB) shall act:

(A) as a clearing house of information on various ways in which system managers have dealt with computer abuse problems;

(B) as a review board to make changes in the investigative guidelines contained below in this document;

(C) and to act as a third party observer/advocate where required or requested in investigations of suspected violations of the University of Scranton Code of Responsible Computing.

The Computer Use Board shall consist of at least one person from the following constituencies (selected by a process yet to be determined):

1. University computing systems
2. Student body
3. Administration or non-UCS Clerical/professional staff
4. Faculty

A delegated member of CUB shall be an independent observer present at inspections of user files in those cases where investigation of abuse requires such action.

I. Denial of access to computing resources

A. In cases where a system administrator may reasonably judge that a computing resource is in jeopardy due to the actions traced to a particular authorization, that authorization may be immediately suspended. This denial of access may continue until the matter is resolved.

B. In cases where a system administrator may reasonably judge that other users are being deprived of their legitimate use

of the computing resource due to actions traced to an particular authorization, that authorization may be immediately suspended. This denial of access may continue until the matter is resolved.

C. In cases not covered by (A) and (B), where a system administrator may reasonably judge that a violation of the code is traced to a particular authorization, the normal procedure shall be to attempt to contact the authorized user to set up a meeting to discuss the problem. If, after one week from the initial attempt to contact the user, the meeting has not taken place, authorization may be suspended. This denial of access may continue until the matter is resolved.

II. Inspection of computer data (e.g. files, logs, archives, programs)

During the course of an investigation of a suspected violation, it may be judged necessary to inspect information created, transmitted, or stored on university computer resources. Since this is a very sensitive issue which deserves careful consideration, files may be inspected only with the expressed consent of the Computer Use Board and with at least one member of CUB present at the inspection. Furthermore, the user whose files are to be inspected must be given ample opportunity to be present at the time the files are inspected.

It should be made clear that the archiving of all files -- suspicious or not, without inspection, is normally done as a routine part of system maintenance and may be done as a routine part of investigation. It is hoped that the actual inspection of files may be avoided except in extreme cases where it may be necessary.