The University of Scranton

Account and Data Policy
Last Revised - 8/20/2004

This policy addresses account creation and termination as well data ownership, integrity and distribution as related to all systems available at the The University of Scranton.

This policy applies to all persons who access University systems, networks or data.

Contents:
I. ACCOUNTS
   A. Account Creation
   B. Account Usage
   C. Account Termination
   D. Disk Space Allocation

II. ACCESS AND DISCLOSURE OF UNIVERSITY DATA
   A. Faculty Access
   B. Staff Access
   C. Student Access
   D. Off-premises Use of University Data and Information
   E. Disclosure of University Information (Information Privacy)

III. DATA OWNERSHIP, INTEGRITY AND DISTRIBUTION
   A. University Data
   B. Library Data
   C. Web Pages

IV ELECTRONIC MAIL AND VOICE MAIL
   A. Permissible Use
   B. Confidentiality
   C. Anti-virus and Anti-spam
   D. Access to e-mail upon separation
   E. Limitation on Disclosure
   F. Violations
   G. Administration of the Policy

I. ACCOUNTS

Account Creation
University employees with an active Human Resources record have the appropriate account(s) automatically created for them providing access to groupware products. Groupware products include but are not limited to e-mail, calendar, campus portal and courseware. Account information is communicated to employees by his/her immediate supervisor or by contacting the IR Help Desk. New employees should allow three days to receive an account.

Employees who need to access the corporate database and the Banner System, will be given a Banner account based on requests made by the divisional Banner User Coordinator or the Department Supervisor via the on-line Project Tracking System. Each individual will receive a unique account. Accounts must not be shared. Exceptions to this policy will be handled through the office of the Vice-President for Planning and Chief Information Officer (CIO).

Student accounts are created once a student record is created indicating that the student is attending or upon registration for classes. The account creation process is automated and begins April 1 for new students attending in fall. After April 1, the account creation process runs daily.

**Account Usage**

Account usage is governed by the Code of Responsible Computing for Faculty and Staff and the Student Computing Policy.

**Account Termination**

Upon employee separation, all accounts are retired within one week of separation. Exceptions to this policy must be addressed by the HR Director or the Vice President for Planning and CIO. If the employee needs to retain the account, the HR department or the employee’s department must submit a request to the Vice President for Planning and CIO. Reference the ‘Access to E-mail Upon Separation’ section for policy on extending access to e-mail accounts. The University reserves the right to revoke all account privileges. Appeals must be made to the Vice President for Planning and CIO.

**Disk Space Allocations**

The disk space allocated to employees is referred to as “disk quota”. There is a limited amount of disk quota provided to each user. Such limitations are enforced. When limits are exceeded, it is the responsibility of the individual to remove unnecessary, out-dated information in order to free up space. Reasonable requests for additional space can be requested via the IR Help Desk. Exceptions to this policy must be approved by the Vice President for Planning and CIO.

**II. ACCESS AND DISCLOSURE OF UNIVERSITY DATA**

Access to data in the corporate database is managed by the divisional Banner User Coordinator, the office designated in the absence of a Banner User Coordinator, or the Vice President for Planning and CIO.
Faculty Access

As a university employee, a faculty member may collect and generate compilations of data as part of a specific assignment by the faculty member's supervisor. These compilations of data are deemed to be owned by the University.

Faculty members may collect and generate compilations of data as part of the faculty member's general responsibility to engage in scholarship. These compilations of data are deemed to be owned by the faculty.

The handling of specific identifying information must be in accordance with the Family Educational Rights and Privacy Act of 1974, as amended (FERPA), the Health Insurance Portability and Accountability Act (HIPAA) and any other federal or state law regulating the disclosure and use of information.

To encourage scholarship, the University may decide to provide assistance to a faculty member to collect and generate compilations of data -- in those situations where the faculty member would not be acting as a University employee nor engaging in scholarship. For example, the assistance could be a grant or opportunities to engage in faculty development. The question of ownership will be agreed upon in writing between the faculty member and the University prior to the University providing the faculty member the necessary assistance. In situations where a faculty member gains unauthorized access and use of university resources to collect and generate compilations of data, contrary to university rules and regulations regarding such access and use, the University may elect to invoke disciplinary measures against the faculty member as provided for in the Code of Responsible Computing.

Finally, unauthorized access and use of university computing resources, including facilities and services, may expose the faculty member to civil and criminal liability under Pennsylvania and federal statutes.

Staff Access

As a university employee, a staff member may collect and generate compilations of data as part of a specific assignment by the staff member's supervisor. These compilations of data are deemed to be owned by the University.

Staff members may collect and generate compilations of data, not as part of a specific assignment, but make substantial use of university-compensated time, personnel, facilities and services. In these cases, the compilations of data are deemed to be owned by the University.

To encourage professional development, the University may grant a staff member the opportunity to access and use university resources for personal business. In these situations,
the staff member may be collecting and generating compilations of data. These compilations of data are deemed to be owned by the staff member, unless it has been agreed upon otherwise, in writing, by the staff member and the University.

However, access and use of university resources by staff members for personal business must be consistent with university rules and regulations regarding such access and use. Nor can such access and use jeopardize the performance of assigned duties by the staff member or other University employees.

In addition, there may be departmental rules and regulations regarding access and use of departmental resources, including its computing resources, facilities and services.

Violations of university or departmental rules and regulations may subject the staff member to disciplinary measures as provided for in the Employee Handbook and the Code of Responsible Computing.

Finally, unauthorized access and use of university computing resources, including facilities and services, may expose the staff member to civil and criminal liability under Pennsylvania and federal statutes.

**Student Access**

Authorized students are given access to components of University corporate data systems for specific functions. Access by students to the corporate database must be restricted to on-campus office locations under the direct supervision of a staff or faculty member. Students are not authorized to access corporate data from off-campus locations or labs.

The handling of specific identifying information must be in accordance with FERPA, HIPAA and any other federal or state law regulating the disclosure and use of information. Breaches of confidentiality will be handled in accordance with those policies defined by the Student Computing Policy.

Students may be hired or commissioned by the University to collect and generate compilations of data. Students receiving a stipend would fall into this category. These compilations of data are deemed to be owned by the University.

Students may collect and generate compilations of data as an assignment under supervision of a faculty member for a course or as a project meeting the academic requirements for a graduate degree. These compilations of data are deemed to be owned by the student, unless it has been agreed upon otherwise, in writing, by the student and the course director, instructor or faculty advisor.

Faculty may state explicitly, in writing, in a course description or syllabus that data collected and generated by the student as a course assignment would belong to the faculty.
However, in these situations, ethical considerations suggest that such students should be compensated with unfettered and fair access to their specific contributions resulting from their own data collection and compilation efforts.

With respect to thesis or dissertation research, a faculty advisor may decide to grant a graduate student access to his or her research database to generate data. In these cases, the question of ownership will be agreed upon in writing by the student, the student’s director and other concerned parties at the time the thesis or dissertation plan is submitted to the Graduate School for review and approval.

To encourage scholarship, the University may decide to provide assistance to a student to collect and generate compilations of data -- in those situations where the student would not be acting as a University employee nor completing a class assignment. For example, the assistance could be a grant or a scholarship. The question of ownership will be agreed upon in writing between the student and the University prior to the University providing the student the necessary assistance.

Students may collect and generate compilations of data in their spare time, that is, on their own time and not for course credit. These compilations of data are deemed to be owned by the student, except in situations where a student has had unauthorized access and use of university resources contrary to university rules and regulations regarding such access and use. In these situations, the University may elect to invoke disciplinary measures against the student as provided for in the Student Computing Policy.

Unauthorized access and use of university computing resources, including facilities and services, may expose the student to civil and criminal liability under Pennsylvania and federal statutes.

Legal and binding contracts and grants entered into by all persons and entities having a rightful claim to ownership or control of data will take precedence over this policy.

**Off-premises Use of University Data and Information**

Access to the corporate database from off-campus locations is restricted to faculty and staff. Off-campus users are responsible for any data downloaded to their PC. Individuals are responsible to protect and remove any PC data. Breaches of confidentiality will be handled in accordance with those policies defined by the Code of Responsible Computing for Faculty and Staff.

Users storing derivative corporate information on their PCs either at work or at home must keep the information confidential. They must not compromise the integrity of the data and they are not allowed to send information to third parties. Users should make use of a secure data transfer program which allows for data encryption when transferring data over the network.
Disclosure of University Information (Information Privacy)

The University recognizes the privacy rights of individuals in accordance with FERPA and any other applicable laws. No information from records, files or data directly related to a student shall be disclosed to individuals or agencies outside the University without the express written consent of the student.

The only exceptions to this policy of access involve public information, response to a lawful subpoena or court order and government officials as required by FERPA. Information contained in such records may be shared within the University with those who have a legitimate educational need to know the information. Records originating at another institution will be subject to these policies.

Disclosure of University data to students is the responsibility of the faculty or staff member authorizing its use. The University policy related to student information is available in the Office of the Vice President for Student Affairs. The confidentiality policy relating to alumni information is available in the Office of Alumni Relations.

III. DATA OWNERSHIP, INTEGRITY and DISTRIBUTION

University Data

University data is defined as any information relating to the University which resides on any University owned computer. In addition to electronic data, University data also includes any paper documents originating within the normal course of business. Data derived from University data remains the property of the University.

Data identified in the University’s Copyright Policy as belonging to an individual is exempt from these statements and does not belong to the University.

Web pages

While the content of web pages which are part of the University web site generally belong to the faculty, staff or students who create them, the web pages themselves belong to the University. Web page development is governed by the Code of Responsible Computing for Faculty and Staff and the Student Computing Policy.

Library Data

Library data is governed by state privacy laws and may be affected by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (the USA PATRIOT Act). Contact the Dean of the Library for more information.
IV. ELECTRONIC MAIL AND VOICE MAIL

Permissible Use

The University provides electronic and voice mail to its faculty, students, and staff for educational, research, healthcare, and internal business purposes. Members of the University community should limit their use to these purposes.

Persons outside the University community may be given access to University electronic and voice mail on a case-by-case basis by special authorization from the Vice President for Planning and CIO and under certain conditions, including adherence to this and other applicable policies.

The use of electronic mail and voice mail at the University should comply with other University policies regarding computing facilities and disclosure of information. In particular, this includes the Student Computing Policy and the Code of Responsible Computing for Faculty and Staff.

Confidentiality

The University cannot guarantee the confidentiality or privacy of electronic or voice mail messages and makes no promises regarding their security. Decisions as to what information to include in such messages should be made with this in mind.

The following elements guide the administration of electronic and voice mail at the University of Scranton as it relates to confidentiality:

A. Administrative Activities: The University reserves the right to conduct routine maintenance, track problems, and maintain the integrity of its systems. As is the case with all data kept on University's computer systems, the contents of electronic or voice mail messages may be revealed by such activities.

B. Monitoring: The University does not monitor the contents of electronic or voice mail messages as a routine matter. However, such monitoring may be conducted when required to protect the integrity of the systems or to comply with legal obligations.

C. Directed Access: The University reserves the right to inspect the contents of electronic and voice mail messages in the course of an investigation in accordance with the policy defined by the Student Computing Policy and the Code of Responsible Computing for Faculty and Staff. The University will comply with all legal requirements for access to such information.
D. **Imperative Access**: From time to time department heads may have a pressing business requirement to access a current or former employee’s e-mail account, or have mail from that account forwarded to another staff member’s account. Written requests for such access should be sent to the office of the Vice President for Planning and CIO. Every effort will be made to secure the affected employee’s written permission in advance. However, access may be granted without the prior permission of affected employee.
**Anti-Virus and Anti-spam software**

The University runs software which scans all incoming messages for viruses or spam. No user is allowed to opt-out of the virus protection plan. Faculty and Staff may opt-out of the anti-spam protection plan. Students may not opt-out of the anti-spam protection plan. Spam messages are collected in quarantine. However, users have the capability to restore any message to their mail Inbox, which is not considered to be spam by the individual.

Entries consistently flagged inappropriately for quarantine can be placed on the whitelist. Requests for inclusion of a site on the whitelist are to be sent to the IR Help Desk.

**Access to e-mail upon separation**

Upon separation from the University, faculty and staff may request that all mail be forwarded to a new address for a period of time not to exceed 90 days. The request must be made to the Department Supervisor who will in turn contact the Director of Systems and Software Resources. The University reserves the right to deny access to a separated employee’s e-mail account, including the denial of forwarding privileges.

**Limitation on disclosure**

Any third-party disclosure of the contents of electronic or voice mail obtained according to this policy will be limited unless such disclosure is required to protect the integrity of University systems or to comply with a legal obligation.

**Violations**

The use of electronic mail services is a privilege offered to University faculty, staff, and students. The University reserves the right to revoke this privilege for violations of this policy.

**Administration of the Policy**

For compilations of data in which the faculty member, staff or student has full ownership, that person shall be responsible for executing all documents, including copyright applications and assignments to exercise and protect his or her rights under federal copyright statutes. In cases where the University has full ownership, the University shall execute the necessary documents. The Copyright Policy will apply in matters regarding the distribution of royalty income.

This policy may be revised when appropriate. It is to be used in conjunction with other University computing use policies.