



UNIVERSITY of ALASKA SOUTHEAST

University of Alaska Southeast Statement of Responsibility and Rules of Conduct

Name (print): _____
First Name MI Last Name

Banner User ID (if assigned): _____ UA ID (if assigned): _____

All university employees and authorized systems users are responsible for the security and confidentiality of university data, records and reports. Individuals who have access to confidential data are responsible for maintaining the security and confidentiality of such data as a condition of their employment. The unauthorized use of, or access to, confidential data is strictly prohibited and will subject the individual to disciplinary action as specified herein.

The system access rules of conduct and user responsibilities include but are not limited to:

1. System users shall not personally benefit or allow others to benefit by knowledge of any special information gained by virtue of their work assignments or system access privileges.
2. System users shall not exhibit nor divulge the contents of any confidential record or report to any person, except in the execution of assigned duties and responsibilities.
3. System users shall not knowingly include nor cause to be included in any record or report a false, inaccurate, or misleading entry.
4. System users shall not knowingly expunge nor cause to be expunged a data entry from any record or report, except as is a normal part of their duties. Due caution will be exercised in the disposal of documents and reports containing sensitive information.
5. System users shall not publish nor cause to be published any university reports, records or other information which contains confidential information for unauthorized distribution.
6. System users shall comply with information security procedures and rules of conduct as promulgated by the university.
7. System users shall not share passwords with any, nor transcribe them in any manner, such as, but not limited to: written, store, transmitted on computer systems or imbedded within automatic log in procedures.
8. No person shall aid, abet or act in concert with another to violate any part of these rules.

In addition to the above items, the users of SCT applications must comply with the conditions of the license agreement the university has with SCT. The agreement requires you and your organization to not sell, give away, or circulate any part or all of the SCT system to anyone. The SCT applications are the property of SCT and they must be treated as confidential information. Should you have any questions regarding the conditions for use of the system, please contact your campus information Security Coordinator.

Violation of these rules of conduct may subject you to loss of information access privileges, reprimand, suspension or dismissal in such manner as is consistent with Regent's policies and university regulations and to prosecution under federal and state computer and information security laws.

I have READ and fully UNDERSTAND the State of User Responsibility and Rules of Conduct printed on this form and shall comply with such statement and rules.

User Signature _____ Date: _____

UAS Security Manager _____ Date: _____