University of South Carolina Beaufort Office of the Registrar
Security and Confidentiality Self Audit for Offices using Student Records

USCB acknowledges that faculty and staff throughout the University need access to student records in order to perform their jobs. Student records may include:

- Official Academic Records
- Advising Records
- Teaching Records
- Financial Records

Financial Aid Records
Judicial Records
Health Records
Student Activity Records

For this reason, the university must strive to ensure that the security and confidentiality of student records are protected using a combination of technology and education. Given its size and geography, the University of South Carolina relies on all University Officials across the system to protect the security and confidentiality of records in their possession. Overall security of a work area is the responsibility of the user and departmental management. Equipment that accesses the University network is required to be secured when the operator is absent or when the system is connected to a network (IT 1.06). Confidentiality of and responsibility for student records is addressed in ACAF 3.03 and UNIV 150. The check list below is intended to be used by University Officials with confidential student materials in their custody in order to audit the security and confidentiality of records in their possession.

Security of Paper Records	Yes	No
Are your paper and electronic records stored in a secure place? (locked cabinets, offices, buildings, keyboards, networks)		
Are precautions taken to protect them against disaster? (fire and flood protection, back-up copies)		
Are your offices, file cabinets, keyboards locked when not in use? Do you know who has the keys?		
Do you have strict procedures/records for building/office/desk key issuance and return?		
Do you have confidential records in any area where an unauthorized party might accidently see them?		
Do you have strict procedures/records for building/office security system password issuance?		
Do you change security passwords whenever an individual with its knowledge terminates employment in the office?		
Do you destroy your records in accordance with the schedule authorized by the University Archivist? (http://arm.scdah.sc.gov/NR/rdonlyres/3DD56BB6-A1FA-4667-AD7E-C60EBC5C934A/0/genskedSCU.pdf)		
Are your documents destroyed in a safe manner such as shredding?		
Security of Electronic Records	Yes	No
Does your personnel practice safe computing using resources available at the University:		

Security of Paper Records	Yes	No
Are your paper and electronic records stored in a secure place? (locked cabinets, offices, buildings, keyboards, networks)		
Are precautions taken to protect them against disaster? (fire and flood protection, back-up copies)		
Are your offices, file cabinets, keyboards locked when not in use? Do you know who has the keys?		
Do you have strict procedures/records for building/office/desk key issuance and return?		
Do you have confidential records in any area where an unauthorized party might accidently see them?		
Do you have strict procedures/records for building/office security system password issuance?		
Do you change security passwords whenever an individual with its knowledge terminates employment in the office?		
Do you destroy your records in accordance with the schedule authorized by the University Archivist? (http://arm.scdah.sc.gov/NR/rdonlyres/3DD56BB6-A1FA-4667-AD7E-C60EBC5C934A/0/genskedSCU.pdf)		
Are your documents destroyed in a safe manner such as shredding?		
Security of Electronic Records	Yes	No
Does your personnel practice safe computing using resources available at the University: http://www.uts.sc.edu/informationsecurity/resources.shtml		
Is your IT security contact personnel confident that the data downloaded from STARMart, extract files, or other access points to any networked PC, server, or non-enterprise system is secure in accordance with federal and industry standards? http://www.nsa.gov/ia/guidance/security_configuration_guides/current_guides.shtml		
When engaging a private entity offering an official University service requires student information, do you create a contractual agreement between the University Board of Trustees and the vendor specifying how the information will be used and what actions the law prohibits?		
Do you require your staff to adhere to IT 1.06 policy regarding acceptable use and practice?		
Do you require your staff to run updated virus and anti-spyware software on all computers on a regular basis?		
Do you assure that members of your staff are not downloading unauthorized software that might compromise the security of the network?		
Does the staff know that confidential student records data should not be kept on any mobile devices, including laptop computers?		
Does your staff know that Social Security Numbers should not be put on any local device or server?		
Confidentiality of Records	Yes	No
Does your faculty know not to inadvertently release personally-identifiable confidential information by making it available to others on class or group materials, handouts, course management systems, blogs, or verbally in class? http://registrar.sc.edu/html/ferpa/fast_ferpa.pdf		
Do you require signed confidentiality statements from staff, faculty, graduate assistants, and student workers who work with student educational records? http://www.sc.edu/policies/acaf702.pdf		
Does your staff know not to speak or ask a person to speak his/her SSN in a public setting? http://registrar.sc.edu/html/student_rights/confidentiality.stm		
Does your staff know not to send a full SSN or other personally-identifiable confidential		