**Comprehensive Standard 3.9.2**

**The institution protects the security, confidentiality, and integrity of student records and maintains special security measures to protect and back up data.**

**Judgment:** Compliant

**Response:**

**Columbia Campus**

The University of South Carolina is committed to protecting the security, confidentiality, and integrity of the academic record, through the enforcement of federal, state, and institutional policies. The federal Family Educational Rights and Privacy Act (FERPA) guarantees students certain rights of confidentiality when it comes to educational records and students may exercise their FERPA right to withhold directory information from release. Students at the University of South Carolina are notified of their rights in accordance with the law, and access to records for authorized individuals is strictly regulated with institutional policy and procedure. The University's specific academic regulations are published in the Academic Bulletins. Other related policies can be found among the University's Policies and Procedures Manual. Throughout this document, policies governing the security, confidentiality, and integrity of both paper and electronic academic records are discussed.

The University of South Carolina predominantly uses electronic means for the storage of student records. Expeditious imaging and destruction of confidential paper materials is an industry best practice to which the University of South Carolina is committed. Images of confidential paper materials are stored on an enterprise system known as Content Manager which is managed by University Technology Services (UTS). Access to the files within Content Manager is password protected and restricted to those with a legitimate, and appropriately authorized, interest.

Although student record materials originate in various admissions offices throughout the University system, the undergraduate records are retained in the care of the Office of the University Registrar or other authorized data steward as defined in University policy 1.50 (pending version attached). The University follows guidelines for records security established by the American Association of Collegiate Registrars and Admissions Officers (Academic Record and Transcript Guide, 2003). In congruence with these guidelines, the Office of the University Registrar is physically inaccessible after office hours. Keys to the offices and elevator doors are issued only to selected individuals and are collected from individuals leaving our employment. In addition, a motion detection system is set every day at close of business and unarmed every morning. Only selected individuals have the code. If the alarm sounds, the University's Division of Law Enforcement and Safety arrive, and call administrators. The office also has panic buttons for staff members in service areas that can be used if security is breached. All student and staff workers sign a statement of confidentiality (attached).

Prior to reaching the Office of the University Registrar, the Columbia Undergraduate Admissions Office (UG Admissions) receives application materials that arrive predominantly (over 90%) by way of an electronic vendor, College Net, whose application system captures applicant data, collects application fees, and transmits data via secure FTP to USC's application processing system. PDF images of applications are uploaded, indexed, and released daily to Content Manager. Supporting credentials such as transcripts and recommendations, as well as paper applications, also arrive by US mail. As these documents arrive, they are scanned and verified for accuracy, readability, and legibility before being released to Content Manager. Paper documents are retained on site in a secure location in the UG Admissions processing department for a minimum of 60 days in order to be available if a processor must refer to the original paper copy after it has been scanned. Documents reaching 60 days of age are then transported to a secure shredding bin which is periodically removed and securely shredded, on site, by a state-approved shredding service. This procedure is in accordance with state records retention requirements mentioned below.

In addition, other University Campuses (including those being accredited with Columbia) deliver paper admissions files of matriculated students to the Office of the University Registrar, where the confidential paper (including enrollment-related paper documents and applications for degree) is processed, scanned to an electronic image, secured on Content Manager, and destroyed in a secure manner by a state-approved service.

Beyond undergraduate admissions, there are other identified data stewards who protect further types of student records at the University of South Carolina. The Graduate School is the data steward for all graduate student admissions and academic program of study records, and they also store application materials using Content Manager. Similar to the Office of the University Registrar, the Graduate School is physically inaccessible after office hours. Keys to the offices are issued only to selected individuals, and keys are collected from individuals leaving employment. Individual offices temporarily housing paper files which await processing, scanning, and shredding, also are locked and inaccessible after office hours.

The Medical School is the data steward for all medical student admissions and academic program of study records. During the four years of medical school, the academic records are kept in a locked file cabinet in a locked office. After graduation, the academic file is moved to a locked file cabinet in a locked Record Room. Keys to the offices are issued only to selected individuals, and keys are collected from individuals leaving employment. Individual offices temporarily housing paper files which await processing, scanning, and shredding, also are locked and inaccessible after office hours.

The Office of Admissions for the Law schoolis the data steward for law student admissions records. File cabinets are locked each evening upon close of business. Files for past applicants are kept for the required number of years in locked file cabinets in a separate locked office. These files are then purged and shredded on-site using a reputable shredding company. For security purposes, the offices are only accessible with a special key. The key

to the offices are issued only to selected individuals, and the key is collected from individuals leaving employment.

The Office of the Law Registrar/Academic Serviceskeeps all supporting records for matriculating law students. The files for matriculating law students are maintained in paper form until they graduate, at which time they stored on the institutional imaging system, Content Manager. All paper files are kept in a locked storage location. File cabinets are locked each evening upon close of business. Keys to the file cabinets are locked in a drawer. For security purposes, the office is only accessible with a special key. The key to the offices are issued only to selected individuals, and the key is collected from individuals leaving employment.

In the Office of Student Financial Aid and Scholarships, documents that become part of each student's official financial aid file are scanned to an electronic image and stored within Content Manager. Once captured electronically, the paper documents are stored in locked containers for on-site shredding by a reputable shredding company. Documents that must be retained in a paper format are securely stored within the physical structure of the Office of Student Financial Aid and Scholarships. The physical structure is unavailable outside of normal work hours to anyone without a university-issued key.

The Office of International Student Services maintains both paper and electronic records of immigration data for international students and for permanent resident alien students. The office is gradually transitioning to a paperless system. Electronic data is securely maintained on virtual servers with UTS and is backed up daily. Paper files are kept in the office. File cabinets are locked each evening upon close of business, and a motion detecting alarm system is activated that will generate a response from the Division of Law Enforcement and Safety if triggered. Only authorized staff members have the alarm code and keys to the office. Keys are collected once employment has ended. When a student ceases to be under the immigration sponsorship of the University, his or her records are archived in a separate locked room where they are kept for five (5) years.

The Office of Student Judicial Programs and Office of Academic Integrity maintains all disciplinary records related to violations of the Code of Conduct and Honor Code. These records are maintained electronically on the Conduct Manager database system by Maxient (which is a service provider with whom USC contracts for Student Conduct records) and are maintained physically in locked file cabinets in a secure file room. The office is locked and an alarm, which is connected to the Division of Law Enforcement and Safety, is set when the office is closed and unarmed when the office opens. Records are stored in compliance with FERPA regulations and The Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act. The records are maintained for a period of six (6) years from the end of the academic year in which the incident occurred. After that time, the physical records are destroyed and only statistical information is maintained electronically. Records where the sanction was suspension or expulsion are maintained for at least 10 years.

In the Office of the Bursar, all users are required to abide by standards and acceptable use of computing facilities and safeguarding sensitive data. In addition to FERPA, the University of South Carolina provides appropriate protection and rights under The Fair and Accurate Credit Transactions Act of 2003. Both hard copy and electronic records are maintained in a secure system managed by the Bursar's office based upon Generally Accepted Accounting Principles (GAAP). All offices are locked and checked regularly by the University Division of Law Enforcement and Safety. The Depository, Student Loan Accounting, and Student Loan Collections areas are secured with an electronic alarm system. All electronic files are on a secure server, and the University's mainframe and security are maintained by UTS as described later in this document.

The Office of the Bursar endorses the new Identity Theft Prevention Program for Covered Accounts to help protect the University and its students, faculty, staff, and other constituents from damages related to the loss or misuse of sensitive information. Covered accounts are those a creditor offers or maintains primarily for personal purposes which involve multiple payments or transactions. The Office of the Bursar is committed to updating the program periodically by reviewing the accounts that are covered and the identified risks that are part of the program. Access to covered accounts for disbursement is obtained in person, requiring picture identification, and disbursement obtained by US mail can only be mailed to an address on file. The University policy for Identity Theft Prevention Program has been submitted to administration for approval.

All full-time and part-time employees and contractors performing work for the Office of the Bursar are required to sign a statement of confidentiality and follow the subsequent best practices: (1) file cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information must be locked when not in use; (2) desks, workstations, work areas, printers and fax machines, and common shared work areas must be cleared of all documents containing sensitive information when not in use; (3) whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas must be erased, removed, or shredded when not in use; and (4) when documents containing sensitive information are discarded, they must be placed inside a locked shred bin or immediately shredded using a mechanical crosscut or approved shredding device. Employees are also made aware that, although sensitive information may be transmitted internally using approved University e-mail, any sensitive information sent externally must be sent only to approved recipients. Additionally, a statement such as this should be included in the e-mail: *"This message may contain confidential and/or proprietary information and is intended for the person/entity to which it was originally addressed. Any use by others is strictly prohibited."*

Last, the University of South Carolina's Student Health Center securely manages student health data. The Student Health Center places the highest priority on a patient's right to privacy and respects the privacy and confidentiality of each patient's health information. Student Health Services adheres to the requirements outlined by the Health Insurance Portability and Accountability Act (HIPAA), which ensures security and privacy of an individual's medical records (protected health information-PHI) and promotes privacy and trust between patients and the health care providers. As part of HIPAA requirements, all new patients are required to sign an acknowledgement form to indicate that they have received a Notice of Privacy (NOP). The Notice of Privacy describes how Student Health Services, and its providers, use and disclose personal health information. Student Health Services may only use and/or disclose (minimally necessary) protected health information (PHI), with its components for treatment, payment and health care operations.

Beyond specific data stewards of the University, the University of South Carolina maintains an IBM Mainframe with an Information Management System (IMS) hierarchical database. Elements of the University's system are contained in IBM's relational data base structure, DB2. The Student System is created and maintained by the central informational technology group, University Technology Services (UTS). The Student System was designed based on requirements of the University system for administrative use of student records. It provides a secure environment for input and access of student information, with a user based security system utilizing IBM Resource Access Control Facility (RACF). Each user of the system is permitted to the appropriate data and access level based on permissions for the RACF user id. Data access policies are approved by an appropriate data steward as

detailed in USC Policy UNIV 1.50. All UTS employees are required to sign a Memorandum of Understanding/Statement of User Responsibility (attached). This document is filed in the employee's UTS personnel file and addresses confidentiality and release of student data.

University Technology Services employs the following data backup / recovery process for the protection of Student Data. The Student system data is continuously logged to IMS datasets and written to tape as needed through the Fast Dump Restore (FDR) utility. This archiving produces two tapes and are stored for 28 days. One tape is kept internally and the other sent to Iron Mountain for offsite rotation. Complete image copies are created that store all transactions and copied to tape twice a week. These tapes are also kept for 28 days and rotated offsite to Iron Mountain for recovery purposes. Dual copying ensures we have access to the data in multiple locations ensuring we have the ability to restore if needed."

Access to student academic records on the Student System is password-protected, authorized by the University Registrar or authorizing data steward, and limited to individuals or groups defined by FERPA as educational officials. Access requires a quiz to certify FERPA responsibilities and authorization by the official's department chair. The UTS building and data center are inaccessible without an active electronic entry card which is controlled by Carolina Card Access system. Access is limited to staff and individuals that have a defined need to access the facilities for the purpose of performing their work duties.

Registration functions on the Student System are authorized centrally by the University Registrar's office. This allows the various registration sites across the University system to manage many activities locally. Students can register and conduct other business on a secure web interface Visual Information Processing (VIP). VIP is a secure Web portal through which students, faculty, and staff may access their own records as well as perform a number of transactions with the University. All communication with VIP is limited to SSL (https) access. SSL securely encrypts the data being transmitted from the user to the system for authentication and data retrieval. VIP Authentication can be accomplished using one of two methods: the recommended method is MyVIPID authentication.

MyVIPID method requires a user to provide his/her MyVIPID (8 digit static identifier) and a password. The credentials are then passed to identity management to verify the combination. If they are successfully validated, the user connects to his/her USC ID/PIN and subsequently to the confidential record, which is based on the user's unique rights. The alternate method is for the user to provide his/her USC ID along with a student and/or Faculty/Staff PIN number. Once the user has been authenticated, the USC ID and PIN number are encrypted and encoded using a unique VIP algorithm and stored for passing to various IMS transactions. A unique session id is created, and the USC ID and PINs along with some other basic information is stored in a local database. The session id and USC ID and PINs are passed as hidden variables within VIP allowing access to the appropriate data, which is based on the user's unique rights.

Students initially access VIP with a randomly-generated provisional PIN, which when combined with the 9-digit University ID (usually SSN) is valid for sign-on and reset. The PIN must be immediately changed by the student, faculty, or staff to a private PIN. Once the student, faculty, or staff achieves initial access to VIP, he or she is expected to obtain the 8-digit MYVIPID under the Personal Menu and set a new password to accompany the MYVIPID. Students with academic records history are held to a higher threshold when claiming or resetting the PIN than those who are newly admitted. A student who has an academic record but is unable to authenticate, must present positive picture identification to reset the PIN.

With technical assistance from UTS, the official academic records are maintained for all campuses by the Office of the University Registrar and are made available to a number of authorized educational officials throughout the University system in a variety of secure ways. The University requires annual testing and certification for advisors/administrators/staff with access to student data. Each one must participate in a FERPA tutorial and sign and certify an understanding of responsibility for maintaining confidentiality. Department head signature is also required for accountability.

Before retrieving class rolls on VIP, instructors must also take a FERPA quiz. This is required upon first access and every three (3) years thereafter. The subject matter of the faculty quiz is slightly different than that of the staff quiz and addresses classroom and office practices, legal issues, and release of information. The University Registrar also sends an annual welcome letter to faculty and staff apprising them of their responsibilities to keep student records safe and confidential. A warning notice is displayed each time an authorized individual retrieves data from VIP or the Student Information System. Additional resources are provided on a regular basis.

In accordance with the State of South Carolina Privacy Protection Act, the University warns all data users that public information may not be used for commercial solicitation. ACAF 3.03 is the University policy which governs confidentiality and release of student information. To minimize student SSN exposure, efforts have been made to remove it from all printed materials and downloaded data files. Educational efforts have yielded heightened awareness of the need to protect personally identifiable information (SSN Protection). Guidelines are also made available to all offices who handle student information through a confidentiality checklist.

Although the University acknowledges the need for students, faculty, and authorized staff to conduct business in the Student System, only staff in the Office of the University Registrar in Columbia can post academic credit or degrees to the central student records system. Because the University of South Carolina transcript is one comprehensive document signed and sealed by the University Registrar, these restrictions ensure that the information posted to the University of South Carolina student academic record is supported by proper documentation and in accordance with the academic rules in place at the time of the action according to the academic bulletin.

In terms of record dissemination, the University discontinued the practice of maintaining paper permanent record cards (PRs or transcripts) in 1988. Imaged versions of pre-1988 permanent records are now placed on the enterprise system Content Manager. Paper PRs of students from 1900 to 1988 are maintained by University Archives in a secure and safe environment in accordance with the South Carolina Department of Archives and Records retention schedule. The Office of the University Registrar retrieves images to issue transcripts, verify information, or reactivate the records of former students. The University follows guidelines for records security established by the American Association of Collegiate Registrars and Admissions Officers (Academic Record and Transcript Guide, 2003). Access to imaged records is granted only to certain individuals in the Office of the University Registrar or to others by authorization of the University Registrar.

About 90% of the official University of South Carolina transcripts are issued on sealed/signed security paper by the Office of the University Registrar. About 10% are sent to and from SPEEDE partners using Electronic Data Exchange procedures. Very few other materials are issued using paper or sent through campus mail. All class

rosters, grade rolls, and student specific reports are now made available to the academic community via secure electronic media.

In conclusion, the University of South Carolina acknowledges that many faculty and staff throughout the large University system need access to student academic records in order to perform their jobs. Therefore, security, confidentiality, and integrity are protected using a combination of technology and education. Given its size and geography, the University of South Carolina interprets the requirements of FERPA in a moderately conservative manner, requiring individual accountability for protecting the confidentiality of student information. We adhere to federal, state, and industry standards for data protection, and expect our administrators, faculty, and staff to be accountable for the student data they use as individuals.

**Regional Campuses**

*USC Lancaster*

The University of South Carolina Lancaster is firmly committed to protecting the security, confidentiality and integrity of all USC Lancaster student records. The Office of Admissions, Records and Financial Aid maintains records in accordance with the Family Educational Rights and Privacy Act (FERPA) and the South Carolina Family Privacy Protection Act of 2002.

In accordance with requirements of FERPA, the University of South Carolina Lancaster has designated the following items as Directory Information: a student's name, electronic mail address, local and permanent mailing addresses and telephone numbers, semesters of attendance, enrollment status (full-time or part-time), date of admission, date of graduation, school major and minor fields of study, whether or not currently enrolled, classification (freshman, etc.), type of degree pursued, expected graduation date, degrees, honors, and awards received (including scholarships and fellowships), weight and height of members of athletic teams, and whether the student has participated in official recognized activities and sports sponsored by the University. The University may disclose any of these items without prior written consent, unless the student has submitted a written request to the Office of Admissions, Records, and Financial Aid not release directory information pertaining to him or her. The student must submit the written request no later than May 31 in order to prevent disclosure in the printed student directory.

USC Lancaster policies on the security of student records can be found in our University Bulletin. Additional information can be found on the Admissions website Information for Students and in the Student Handbook.

Student records at USC Lancaster are stored electronically and physically. The physical records are located in the Admissions, Records and Financial Aid Office in locked file cabinets in a storage room outside of traffic areas within the offices. Additional storage is located in a room located at the end of the office complex outside of the main traffic areas. An authorized employee is on duty at all times during office hours. After hours the office is locked and only certified personnel have access. Cameras are located outside of the entry door of the office, and the building is secured nightly. Documents containing sensitive information are placed inside a locked shred bin when discarded.

Electronic storage of records is provided by USC Columbia on secure servers and databases. Records in the university database, IMS (Information Management System) are password protected and access to the screens and information is limited to individuals on a need to know basis as described in the FERPA regulations. Access to the system requires a written request and signatures of the person requesting access and their supervisor. Access to information is not approved without a signed acknowledgement that the requestor has read, understands and will comply with University policy ACAF 3.03 concerning handling of student records. The level of authorization to access student records is determined by the requestors' job function. Authorization can range from view only, update or a combination of both. Training is provided to all employees with access along with written information concerning handling of student records. A FERPA presentation is also available as a resource for faculty and staff on USC Lancaster's website. Login procedures adhere to standard protocols such as unique identifiers and passwords. Users are required to change passwords on a monthly basis.

All physical records kept at USC Lancaster are copies of originals. The original copies are sent to USC Columbia where they are filed, electronically saved and securely stored as part of a student's permanent record. The University of South Carolina has a back-up system set up for the electronic student records and information. Information concerning the security, confidentially and integrity of student records is periodically reviewed with all personnel who have access to student information. Instructors are required to take a FERPA quiz before retrieving class rolls on VIP. This is required upon first access and every three (3 years) thereafter. The faculty quiz addresses classroom and office practices, legal issues, and release of information. The FERPA website is also included on the final grade request sent to faculty each semester. USC Lancaster subscribes to *The FERPA Answer Book for Higher Education Professionals* in an effort to stay informed of changes in policies.

*USC Salkehatchie*

The University of South Carolina Salkehatchie recognizes the trust its applicants and students place in the institution when it provides representatives of this campus with personal information for purposes of admissions, financial aid, academic records, and other support functions. The campus is committed to the protection of that data and maintaining its security, confidentiality, and integrity, and has adopted a number of policies and practices that support that commitment.

The Office of Student Services is the main location for student records and maintains those records in accordance with FERPA (Family Educational Rights and Privacy Act). The USC Office of the University Registrar publishes policies on the Confidentiality of Educational Records. Other regulations can be found in the Student Right-To-Know Handbook.

Student records at USC Salkehatchie are stored physically and electronically. The physical records are stored in locked file cabinets in the Office of Student Services on the West campus and in the Main Office on the East Campus. During office hours, there is always an authorized employee on duty in each location. During non-office hours, the offices are locked, and only certified personnel have access to the offices and the filing cabinets. The lockable file cabinets are out of the traffic patterns of other offices.

Electronic storage is done on servers on the main campus in Columbia, which handles student information according to policy ACAF 3.03. Records in IMS (Information Management System) are protected by a password security system, as well as by limited-access screens on a need-to-know basis, as described in the FERPA regulations. Staff or faculty members requesting IMS privileges must apply in writing with authorization from their supervisor. The USC Office of the University Registrar provides User Instructions for IMS Transactions. The login process requires user authentication according to standard protocols such as unique identifiers and passwords.

USC Salkehatchie has a foolproof back-up plan in place to retrieve student records in case of an emergency. All physical student records kept at USC Salkehatchie are copies of the original. The originals are sent to the main campus in Columbia, where they are filed and securely stored. The University of South Carolina also has a back-up system set up for the electronic student records and information. All individuals who have access to student records or information are periodically reminded about the security, confidentially, and integrity of student records. This includes keeping track of current updates to FERPA policies.

*USC Sumter*

The University of South Carolina Sumter recognizes the trust its applicants and students place in the institution when it provides representatives of this campus with personal information for purposes of admissions, financial aid, academic records, and other support functions. The campus is committed to the protection of that data and maintaining its security, confidentiality, and integrity, and has adopted a number of policies and practices that support that commitment.

The Office of Student Records is the main location for student records and maintains those records in accordance with FERPA (Family Educational Rights and Privacy Act).

USC Sumter policies on the security of student records can be found in the USC Sumter Academic Bulletin. Other regulations can be found in the Student Right-To-Know Handbook.

Student records at USC Sumter are stored physically and electronically. The physical records are stored in locked file cabinets in the Office of Student Records on the USC Campus. During office hours, there is always an authorized employee on duty in each location. During non-office hours, the offices are locked, and only certified personnel have access to the offices and the filing cabinets. The lockable file cabinets are out of the traffic patterns of other offices.

Electronic storage is done on servers on the main campus in Columbia, which handles student information according to policy ACAF 3.03. Records in IMS (Information Management System) are protected by a password security system, as well as by limited-access screens on a need-to-know basis, as described in the FERPA regulations. Staff or faculty members requesting IMS privileges must apply in writing with authorization from their supervisor. There is also proper training provided to employees with this access. The login process requires user authentication according to standard protocols such as unique identifiers and passwords.

USC Sumter has a back-up plan in place to retrieve student records in case of an emergency. All physical student records kept at USC Sumter are copies of the original. The originals are sent to the main campus in Columbia, where they are filed and securely stored. The University of South Carolina also has a back-up system set up for the electronic student records and information. All individuals who have access to student records or information are periodically reminded about the security, confidentially, and integrity of student records. This includes keeping track of current updates to FERPA policies.

*USC Union*

The University of South Carolina at Union is committed to protecting the security, confidentiality and integrity of all USC Union student records and other information. A number of prevailing legal acts and regulatory agencies are used when managing student records. The Student Affairs Office is the main location for student records and maintains those records in accordance with FERPA (Family Educational Rights and Privacy Act). This information is available to all faculty members, Associate Dean and Dean. USC Union policies on the security of student records can be found in the Union Bulletin. Other regulations can be found under Student Right-To-Know and Campuses Security Act Policies & Information.

Student records at USC Union are stored physically and electronically. The physical records are stored in locked file cabinets in the back filing and supply closet in the Student Affairs Office. During office hours there is always an authorized employee on duty in the Student Affairs Office and during non-office hours the office is locked and only certified personnel have access to the office as well as the filing cabinets. The lockable file cabinets are out of the traffic patterns of all the other offices.

The electronic information that is available resides on secured databases or servers. Records in IMS (Information Management System) are protected by a password security system, as well as by limiting access to screens and information on a need-to-know basis as described in the FERPA regulations. The University's two IT administrators are charged with the user-authorization process and procedures. Before acquiring access to the IMS system access must be applied for in writing which does require the signature of the person requesting access and their supervisor. There is also proper training provided to employees with this access. The login process requires user authentication according to standard protocols such as unique identifiers and passwords.

USC Union has a foolproof back-up plan in place to retrieve student records in case of an emergency. All physical student records kept at USC Union are copies of the original. The originals are sent to the main USC campus in Columbia where they are filed and securely stored. The University of South Carolina also has a back-up system set up for the electronic student records and information. All personnel that have access to any student records or information are periodically reminded about the security, confidentially, and integrity of student records. This includes keeping track of current updates to FERPA policies.

**Supporting Documentation:**

| Description | Source |
|---|---|
| ***Federal Policies*** | |

| | |
|---|---|
| Family Educational Rights and Privacy Act (FERPA) | http://www.ed.gov/policy/gen/guid/fpco/index.html |
| The Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act | http://www.les.sc.edu/annualsecurityreport/index.asp |
| The Fair and Accurate Credit Transactions Act of 2003 | http://www.treas.gov/offices/domestic-finance/financial-institution/cip/pdf/fact-act.pdf |
| Generally Accepted Accounting Principles (GAAP) | http://www.fasab.gov/accepted.html |
| Identity Theft Prevention Programs | http://www.ftc.gov/opa/2009/04/redflagsrule.shtm |
| Health Insurance Portability and Accountability Act (HIPAA) | http://www.cms.gov/HIPAAGenInfo/ |
| ***State Policies*** | |
| South Carolina Department of Archives and Records Retention Schedule | http://arm.scdah.sc.gov/NR/rdonlyres/3DD56BB6-A1FA-4667-AD7E-C60EBC5C934A/0/genskedSCU.pdf |
| South Carolina Family Privacy Protection Act of 2002 | http://www.scstatehouse.gov/code/t30c002.htm |
| ***Institutional Policies*** | |
| USC Policy on Student Records | http://www.sc.edu/policies/ppm/acaf303.html |
| USC Records Retention Policy | http://registrar.sc.edu/html/fac_staff/RecordsRetention2005.pdf |
| Data Access Policy, UNIV 1.50 | http://www.sc.edu/policies/univ150.pdf |
| USC Handling of Student Records (ACAF 3.03) | http://www.sc.edu/policies/ppm/acaf303.html |
| Procedure for Handling Records | http://ipr.sc.edu/pdf/ProcRetentAdmissionCred.pdf |
| USC SSN Protection | http://registrar.sc.edu/html/student_rights/confidentiality.stm |
| Health Notice of Privacy | http://www.sa.sc.edu/shs/NOP_Brochure_2007.pdf |
| Privacy Request Form | http://registrar.sc.edu/pdf/as-175p.pdf |
| American Association of Collegiate | http://www.aacrao.org/ |
| Academic Record and Transcript Guide, 2003 | http://ipr.sc.edu/pdf/AACRAO.pdf |
| Permit to Access IMS Resources | http://www.uts.sc.edu/forms/IMSPermitAccess.pdf |
| Data Stewards | http://www.sc.edu/policies/univ150.pdf |
| Statement of Confidentiality | http://ipr.sc.edu/pdf/BursarStateConfid.pdf |
| ***USC Training Documentation*** | |
| Notification of Student Rights – FERPA | http://registrar.sc.edu/pdf/notification_of_student_rights_2008.pdf |
| USC-Columbia FERPA Tutorial | http://registrar.sc.edu/html/ferpa/ferpa1.stm |
| Lancaster | http://registrar.sc.edu/html/ferpa/ferpa_files/v3_document.htm |
| FERPA Quiz | https://vip.sc.edu/demo/ferpa.html?TERM=4&YEAR=2003&x=24&y=4 |
| Access after Quiz | http://registrar.sc.edu/html/ferpa/ferpamail.stm |
| Final Grade Request - Lancaster | http://usclancaster.sc.edu/SACS/FinalGradeRequest.pdf |
| FERPA Answer Book | http://aasep.org/professional-resources/specialedlaw0/ferpa/index.html |
| USC Confidentiality Checklist | http://registrar.sc.edu/pdf/Security_Confidentiality_Checklist.pdf |
| Annual Welcome Letter | http://registrar.sc.edu/pdf/2009.pdf |
| IMS User Instructions | http://registrar.sc.edu/html/instruction/ims.stm |
| IMS Training | http://hr.sc.edu/profdevp/classes/studregs.html |
| ***Electronic Data Systems*** | |
| IBM Mainframe | http://www.uts.sc.edu/faq/ |
| Visual Information Processing | https://vip.sc.edu/ |
| MyVIPID | https://vip.sc.edu/login.html |
| Electronic Data Exchange | http://www.aacrao.org/speede/index.cfm |
| Content Manager | http://www.uts.sc.edu/support/instructions.shtml |
| University Technology Services | http://www.uts.sc.edu/ |
| College Net | https://www.applyweb.com/apply/uscc/ |
| Maxient | http://www.maxient.com/ |
| ***Bulletins, Manuals, and Misc*** | |
| Academic Bulletins - Columbia | http://bulletin.sc.edu/ |
| Lancaster | http://bulletin.usclancaster.sc.edu/ |
| Salkehatchie | http://bulletin.uscsalkehatchie.sc.edu/ |

| | |
|---|---|
| Sumter | http://bulletin.uscsumter.edu/ |
| Union | http://bulletin.uscunion.sc.edu/ |
| Academic Regulations | http://bulletin.sc.edu/content.php?catoid=10&navoid=1864 |
| Policies and Procedures Manual | http://www.sc.edu/policies/index.shtml |
| Extended Affairs | http://saeu.sc.edu/rcIndex.html |
| Student Right-to-Know | http://saeu.sc.edu/students/docs/StRK09-10.pdf |
| Student Handbook - Lancaster | http://usclancaster.sc.edu/studentlife/2009-2010StudentHandbook.pdf |
| Information for Students | http://registrar.sc.edu/html/student_rights/stud_rights.stm |
| Regional Campus Web Sites | |
| Salkehatchie – East | http://uscsalkehatchie.sc.edu/map.html |
| Salkehatchie – West | http://uscsalkehatchie.sc.edu/map.html |
| USC Sumter | http://www.uscsumter.edu/ |

RETURN TO TOP USC LINKS: DIRECTORY MAP EVENTS VIP SITE INFORMATION
Columbia, SC 29208 • Phone • Email
© University of South Carolina Board of Trustees