12.5 Student records

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

Compliance Judgment: In Compliance

Rationale

The University of South Carolina Aiken operates in accordance with federal and state laws, and the University of South Carolina system policies as they relate to handling of and access to records. The policies and procedures are designed to secure and protect the confidentiality and integrity of student records. All institutions and campuses within the USC system share an enterprise technological system within which principal student records are maintained and secured. In addition, some departments on the campus maintain separate protocols and records which must adhere to the same security measures and standards established by system policies.

General Data Stewardship and Governance. USC System policy UNIV 1.51 - Data and Information Governance [1] establishes the university's ownership of data and information; defines roles and enumerates high-level responsibilities of Data Trustees, Data Stewards, and Data Custodians; and establishes the university's framework for data and information governance which includes four programs: data stewardship, data standards, data quality and integrity assurance, and business intelligence. The policy also establishes the university's data classification schema, which is consistent with the State of South Carolina Information Security policy [2], as well as National Institute of Standards and Technology (NIST) publication SP 800-60 (Guide for Mapping Types of Information and Information Systems to Security Categories).[3] The policy embraces principles, guidance, and best practices promulgated by the US Department of Education's Privacy Technical Assistance Center.

USC System policy UNIV 1.52 Responsible Use of Data, Technology, and User Credentials [4] establishes high level requirements for compliance with laws, statutes,

regulations, policies, standards, and procedures for accessing data and information, including student records. The policy establishes a direct personal responsibility for appropriate use of data and sets the expectations and templates for data sharing agreements.

USC System policy IT 3.00 Information Security [5] commits the university to securing its information assets and empowers the University Information Security Office (UISO) to establish and maintain the University of South Carolina Information Security Program. The UISO implements a risk-based strategy for maintaining and continuously evolving the university's Information Security Program, which enables the university to focus limited resources towards managing the most urgent threats targeting the higher education community in general, and the University of South Carolina system in particular. The university undertakes a broad, multi-pronged approach to ensure adherence to these policies and procedures. While an exhaustive listing of such efforts is impractical, the following activities demonstrate compliance:

- Data steward responsibilities include the authorization of each user's individual access to data and information (supports UNIV 1.51 and UNIV 1.52).
- The USC System's Division of Information Technology (DoIT) maintains an inventory of information systems in use at the university; this includes a record of the system's data steward and the data classification of the system, through the Office of the Chief Data Officer (per UNIV 1.51).The Program Manager for Data Standards, Data Quality & Integrity Assurance administers Data Cookbook at the university's data governance information system, including a functional systems inventory. However, as DoIT matures its service delivery, we plan to establish a Configuration Management Data Base (CMDB) that will become the official systems inventory utilizing information that is currently compiled in Data Cookbook, leveraging the incredible potential of CMDB to enhance security, system integrations, and strategic IT planning.
- The USC System’s DoIT promulgates a guide for Information System Owners, detailing the responsibilities and providing requirements and best practices for system ownership and administration (supports IT 3.00 and UNIV 1.52).

- UNIV 1.52 establishes templates that can be modified by data stewards to support four distinct use cases under the general auspices of Data Sharing Agreements: 1) end user agreement, primarily to guide individual university employees; 2) internal data sharing agreement, which establishes protocols and memorializes exchange of data between two or more units within the university; 3) external data sharing agreement, which establishes protocols and memorializes exchanges of data between a university unit and an external entity or individual; and 4) contract addendum for external data and systems service providers, which affirms the university's permanent ownership and rights to its data, and places restrictions on providers under contract with the university.
- The university has undertaken a campaign to record Data Sharing Agreements in its data governance information system, Data Cookbook; the university is collaborating with the vendor to add capabilities to schedule such agreements for periodic review, renewal, or termination (supports UNIV 1.52).
- The university utilizes leading industry resources, such as Central Authentication Service (CAS) in tandem with multifactor authentication (MFA) as an enhanced security layer for individual user access, to protect enterprise systems, including the Banner student information system (supports IT 3.00).

Student Record Data Stewards. The Chancellor of USC Aiken is ultimately responsible for access to, security, and integrity of student records; Dr. Sandra Jordan is the institution’s Data Trustee. Data stewardship on the USC Aiken campus generally aligns with the responsibilities delegated to senior administrators. The Provost, Dr. Daren Timmons, serves as the data steward and administrator for the student academic record. The Director of Financial Aid, Tony Carter, serves as the data steward and administrator of financial aid records. The Vice-Chancellor of Administration and Finance, Cam Reagin, is the data steward and administrator for student accounts receivable records. The Associate Vice-Chancellor for Enrollment Management serves as the data steward for admissions and registrar related data. The data steward for advancement and external relations data is the Vice-Chancellor of University Advancement and External Relations, Mary Driscoll. The Director of Athletics, Jim

Herlihy, serves as the data steward for athletic data. The information technology data steward is Ernest Pringle, Vice-Chancellor of Information Technology. Brian Enter, the Senior University Facilities Executive is the data steward for operations, and the Vice-Chancellor for Student Affairs, Ahmed Samaha, serves as the data steward for student life and services.

Enterprise Systems containing Student Records. The University of South Carolina system maintains student records and delivers student record services through multiple enterprise systems. Such systems include:

- ***Banner Student Information System.*** Internet Native Banner is the student information system at the University of South Carolina. It is primarily used by core administrative offices including the offices of admissions, registrar, financial aid, and bursar to view and maintain data and process transactions.
- ***Banner Document Imaging System (BDMS).*** BDMS is a system tied to the Banner Student Information System that stored scanned documents tied to academic, financial aid, and bursar records.
- ***Blackboard.*** Blackboard is a web-based server software which features course management, customizable open architecture, and scalable design that allows integration with student information systems and authentication protocols.
- ***Cognos Datawarehouse.*** Cognos Datawarehouse is a repository of generated reports from student, financial, and human resource systems.
- ***DegreeWorks Degree Audit System.*** DegreeWorks aids both students and advisors in monitoring students' progress toward degree and assist students in choosing the most appropriate courses to fulfill degree requirements.
- ***TutorTrac.*** TutorTrac is an advising software that serves as a resource for advisors containing student information, notes, success markers, progression, and incorporates appointment scheduling.
- ***Maxient Student Judicial System.*** The Maxient system is used to maintain student judicial files.

- ***Peoplesoft.*** Student Employment records are stored in the university's human capital management system, Peoplesoft.

Local Student Records. USC Aiken offices that handle student records in electronic and hard-copy forms adhere to specific procedures designed to ensure the security, confidentiality and integrity of the documentation. USC Aiken's Computer Services Division provides scheduled backups of locally maintained public and secured servers. The frequency of backups depends upon the frequency of use and sensitivity of information on the server. Many heavily used servers such as those dedicated for e-mail are scheduled for daily backups. Other less frequently accessed servers that contain sensitive student information on housing, recruitment, and assessment are scheduled for backups three or four times a week. Departments that handle student records and maintain local data and the security protocols employed include:

- ***Student Health, Counseling Center, and Disability Services.*** Student records in the Counseling Center are primarily in hard copy hand-written format. Each student file is securely locked in file cabinets inside a locked office at the end of each working day. Only therapists, the administrative assistant, and trained graduate assistant(s) are allowed access to the files. The administrative assistant has primary responsibility to ensure that cabinets are locked at appropriate times.

  Within the Student Health Center, there are both hard copy records and a Student Health Center database. All members of the department (nursing professionals, director, and administrative assistant) have access to the records. The database is password protected and can only be accessed with director or administrative assistant log-on. During non-business hours files are kept locked inside the administrative assistant's office which is inside the locked Student Health Center suite.

  All hard copies of files of students who request disability services are maintained in the Counseling Center Office in a locked cabinet. Only authorized personnel (Coordinator of Disability Services, Director of Counseling Services and Disability Services, and administrative assistant) have direct access to these

records. Electronic files are maintained with a password protected system and only the Coordinator of Disability Services, the Director of Counseling and Disability Services, and the administrative assistant have direct access to the system.

For all areas, professional staff members are bound by confidentiality requirements of their profession. All staff members are required to sign a confidentiality agreement as workers in the department. Any requests for copies of student records must be accompanied by a written request from the student for authorization to release records. Photo identification is required when an individual walks in requesting a copy of his or her own records. In all instances when information is released, a record is maintained of what records were released, to whom they were released and the date they were released.

When making written chart notes in student health records, staff members sign their name at the end of the dated note and write initials by any correction or update they make. Charts must be completed within 24 hours of contact with a client/patient.

To ensure student health records will not be lost, there is paper documentation of everything in the database, as well as a back-up of the database itself that would be recoverable as long as any failure/loss was noted in a 30-day period. The Disability Services server is also backed-up on a regular basis.

- ***International Student Records.*** Paper copies of international student files are stored in a file-cabinet which remains locked outside of regular work hours. Electronic student records are all password protected and stored on a password protected server and in the Federal Immigration Database (SEVIS). Only authorized users are allowed to access the database and make changes to student records such as the Vice Chancellor for Enrollment Services, the Director of Admissions, and the Director of International Programs. The time and date of access by all authorized users of SEVIS is itself recorded in the database. Immigration requires that a copy of international student files is kept for one year

after students graduate or separate from the University. After that time, paper copies of the files are shredded. SEVIS electronic records remain available for access/viewing in the SEVIS Database.

- ***Student Involvement Records.*** Student records pertaining to student activities and membership in organizations are password protected and maintained on a secure server. Only professional staff members such as the Director, Assistant Directors, or Office Manager of Student Life can access these records. Some organizations such as Greek organizations require the institution to submit academic records of student members to national offices. Before such information is submitted, student members must sign an authorization to release the records. Under no circumstances are social security numbers or other personally sensitive information released through the Office of Student Life.
- ***NCAA Compliance and Athletic Records.*** To ensure the security of athletes' records, hard copies are kept in locked file cabinets. Electronic copies of student information are maintained in a scholarship database and a prospect database on a secured server; on the NCAA Compliance Assistant, a secure Internet based NCAA database; and within other NCAA or Peach Belt Conference reports completed on secure sites. Access to these databases and sites is controlled. To ensure the integrity of student records is maintained, coaches have "read only" access to any areas other than the recruiting section of Compliance Assistant. Access to the scholarship database is limited to athletic administrators and select administrators in Financial Aid, Business Services, and International Programs.
- ***Career Services Records.*** Career Services maintains files that contain hiring forms related to student employment, databases with student and alumni contact information, student resumes, student personality assessment results, and experiential education application forms with contact information. Information is also entered into a secure database on a server. Only Career Services personnel have access to the database. Some Career assessments are located on password-protected sites run by other organizations such as the DISCOVER

assessment by ACT or the Strong Interest Inventory by CPP, Inc. Student employment forms are the only documents with social security numbers. Hard copies of the forms are kept behind the administrative assistant's desk in a locked file cabinet and can only be accessed by a Career Services staff member. The forms are kept secure for two years and are then shredded.

- ***Housing.*** Hard copies of student housing records are secured in a locked file room in a locked office. Only selected members of the Housing Department have direct access to the locked file room. Electronic records are kept in secured areas on the network and are backed up daily. The shared drive that houses most of the electronic records is accessible only through VPN or LDAP connections, and the members of the department have varying levels of access to the folders on the drive, as appropriate for their positions. Confidentiality is addressed at several levels in Housing; through the security of records, limited access to records, and confidentiality agreements included in all hire paperwork and during staff training sessions.

The Housing Office has procedures in place to minimize errors and prevent unauthorized access or changes to records. All hard copy documentation is initialed by the staff member handling the record. All transactions are recorded in a secure database including the identity of the user and action performed. Most transactions such as payments, room changes and damages/fee are recorded in multiple places. Payments are rung up on the cash register and/or credit card machine, recorded on the Daily Transaction Log, keyed to the student's record and filed in their hard copy files. Room changes and damages/fees assessments are documented on multi-part forms, which are distributed to the student, various offices and kept in the student's file.

Administrative records are kept in the office for one fiscal year, and then moved to secure storage for five years before being shredded. Student Housing records are kept in active files as long as the student is housed and then retained for five years after termination of contract.

- ***Judicial Affairs.*** Judicial Affairs records of academic misconduct are maintained in the Office of the Executive Vice Chancellor for Academic Affairs. Non-academic judicial records are maintained by the Vice Chancellor of Student Life and Services. Copies are stored in locked filing cabinets. Persons who are not directly involved with a discipline case, an appellate review of a decision, or the enforcement of a sanction do not have access to the record or results of a hearing or sanctioning meeting without a legitimate educational need to know or the authorization of the charged party. Records of major violation cases which have been resolved with a sanction less than suspension are maintained for a period of 7 years from the date of the last offense. Students graduating before that time may petition in writing to request that their records be destroyed upon graduation. Records may be retained by the University beyond the normal 7-year period in special circumstances, including, but not limited to, situations when legal action is taken by any party involved. When a date for purging records has been reached, records in all formats are destroyed. Records where the discipline sanction was suspension are maintained for a period of at least ten (10) years from the date of the last incident. Notices of minor violations are kept for a period of 7 years from the date of the last offense; however, they are not classified as official University disciplinary records or provided for authorized inquiry (i.e. background checks for employment, military service or graduate school).
- ***Police.*** University Police records are public records, unless a case involves a sexual assault victim and / or juvenile, and then personal information is blocked. Records are kept in the Incident Report Log book throughout the year and then transferred to a locked cabinet at year's end. An electronic record of the report is kept through SCIBRS (South Carolina Incident Based Reporting System) for UCR (Uniform Crime Report) purposes, and managed by SLED (South Carolina Law Enforcement Division). Records that require confidentiality are maintained in a secure locked filing cabinet. Confidentiality Agreements are signed by all those hired to work for University Police. To ensure that the integrity of any student records is maintained, a supervisor reviews and signs all reports.

Once a report is signed by a supervisor, it can only be changed with a supervisor's approval. No official record is ever destroyed except in the case of an incident classified by the state of South Carolina as a misdemeanor that is eligible for expunction.

Integrity. The University of South Carolina system ensures the integrity of its data through robust practices of data stewardship and governance. In addition to above measures established and administered by functional units, the system's Division of Information Technology (DoIT) offers numerous capabilities that support the objectives of confidentiality and security of student academic records. University Policy UNIV 1.52 Responsible Use of Data, Technology, and User Credentials [4] promulgates many provisions that ensure employees uphold their commitments, including but not limited to:

- Appendix 1, User Agreement, which requires individuals to acknowledge they have received, read, and agree to follow this policy, related confidentiality and privacy provisions, standards, procedures, rules, and regulations pertinent to assets they are authorized to use;
- Requiring employees use their university-provided email account to conduct university business;
- Specifying that individuals using personal technology assets (e.g. their own computing devices) are bound by the policy;
- User authentication services for university personnel (CAS and MFA); and
- Virtual Private Network (VPN) is required for off-campus access.

Additional university policies and procedures assist in ensuring that employees carry out their responsibility for confidentiality, integrity, and security of the student academic record. For example, USC System policy HR 1.22 Telecommuting [6] creates the framework for employees to work remotely, including a Telecommuting Agreement that addresses IT Security requirements, including the use of Virtual Private Network (VPN). The University maintains a robust web presence with information for both end users and organizational units, addressing how to get started with security, training and awareness

resources, incident response protocols, policies and standards, and numerous tools available to assist with the prevention, detection and response of unauthorized access to information assets.

Integrity of student data is upheld primarily by functional units with Computer Services supporting these efforts in two primary ways:

- ***System Integrations and Data Feeds.*** When a data feed or data integration is requested from/with Banner Student Information System, Computer Service personnel processes the request through detailed service delivery protocols. This includes initial screening, a security review, and governance approval by the Student Systems Council. As system integrations and data feeds are developed, personnel validate and iteratively improve the accuracy of the request and delivery with the customer.
- ***Data Quality and Integrity Assurance.*** The USC System DoIT has initiated use of Data Cookbook for functional units to write data definitions and data quality rules. Data definitions ensure correct and consistent selection, use, understanding, and interpretation of data. Data quality rules specify what content a given data element can or cannot contain. Definitions and quality rules in Data Cookbook are complemented by use of Data Cookbook's iDataHub functionality, which will analyze data records for compliance with established rules. Identified errors are then sent to functional org unit personnel to review and as needed to correct in the source system. These protocols assist functional org units in assuring that their data are correct, complete, and accurate, yielding data that is are of high quality with necessary integrity. Such data are required by the Office of Institutional Effectiveness, Research, and Compliance to produce official reports and surveys, and is essential to produce reliable business intelligence and analytics using Cognos from raw data within the Operational Data Store.

Confidentiality. The federal Family Educational Rights and Privacy Act (FERPA) guarantees student certain rights for privacy when it comes to educational records and students may exercise their FERPA right to withhold directory information from release.

Written procedures are distributed by the Office of the Registrar and are consistent with the Family Educational Rights and Privacy Act (FERPA), a federal privacy law that gives students certain protections with regard to their education records, such as grades, transcripts, disciplinary records, contact and family information, and class schedules. Students at the University of South Carolina are notified of their rights annually in accordance with the law. In addition to inclusion in the university's policy and procedures as USC System policy ACAF 3.03 – Handling of Student Records [7], FERPA regulations are published in each annual Academic Bulletin.[8]

All faculty and staff who access individual student information are required to read a FERPA tutorial and then take and pass an online FERPA quiz before being given access to course rolls or the student database. After passing the quiz, the individual must print out and sign the Banner Account Request Form, a document certifying understanding of the law; this document is then signed by the employee's supervisor and uploaded into the DAPS System for processing. All faculty and appropriate staff must retake the quiz annually to ensure continued understanding of the law.

The university complies with the South Carolina Family Privacy Protection Act of 2002 (SC Code of Laws 30-2 [9]), and the following policies and procedures to ensure student record confidentiality:

- ***ACAF 3.03 Handling of Student Records.*** [7] Describes how the University of South Carolina collects personal student information considered necessary to fulfill its purpose as an institution of higher education. Describes how the information is maintained and made available in accordance with the federal Family Educational Rights and Privacy Act (FERPA), and the South Carolina Family Privacy Protection Act of 2002.
- ***UNIV 1.51 Data and Information Governance.*** [1] The University of South Carolina system acknowledges that its data and information are vital and valuable assets and is committed to establishing governance programs that ensure the appropriate use, availability, and risk mitigation for data and information assets. This policy describes how data and information governance

programs are developed, implemented, and maintained for the benefit of the University of South Carolina system and its constituents

- ***UNIV 1.52 Responsible Use of Data, Technology, and User Credentials.*** [4] Outlines the requirement for all individuals and organizational units that use or access university data, technology, and user credentials to: comply with state and federal laws, statutes, and regulations; comply with all applicable university policies, standards, and procedures; must have prior authorization for related activities based on job duties or other demonstrated need; and not compromise the appropriate availability, integrity, confidentiality, privacy, or security of data, technology, and user credentials. In order to successfully carry out its mission, the University of South Carolina will act to protect the confidentiality, integrity, and availability of data, technology, and user credentials. The University of South Carolina promotes responsible use and prohibits unauthorized use of these university assets, including for personal or other non-university purposes.
- ***IT 3.00 Information Security.*** [5] The University of South Carolina strives to provide a safe computing environment, and is committed to securing its data and information technology (IT} resources per state and federal laws, statutes, and regulations. In order to support risk management and compliance efforts, the University Information Security Office (UISO) is authorized to administer the university-wide Information Security Program. The UISO develops and publicizes the Information Security Program and coordinates all security incident response. Users and managers of university data and IT assets follow the Information Security Program. The University of South Carolina prohibits interference with-or avoidance of-security measures. Such actions may be grounds for investigation and disciplinary action.

The university has three systems that require faculty and staff to submit account request forms documenting their understanding of privacy policies for students:

- ***Banner Student Information System.*** Internet Native Banner is the student information system at the University of South Carolina. It is primarily used by core administrative offices including the offices of admissions, registrar, financial aid, and bursar to view and maintain data and process transactions. Faculty and Staff that need access to Banner are required to complete the Banner Account Request Form.
- ***Cognos Datawarehouse.*** Cognos Datawarehouse is a repository of generated reports from student, financial, and human resource systems. Authorized student support staff can view, access, and print reports for administrative purposes. Faculty and Staff that need access to Cognos are required to complete the Cognos Access Request Form.
- ***Degree Works.*** DegreeWorks aids both students and advisors in monitoring students' progress toward degree and assist students in choosing the most appropriate courses to fulfill degree requirements. Faculty and Staff that need access to DegreeWorks are required to complete the DegreeWorks Access Request Form.

Security. Access to physical student records for authorized individuals is strictly regulated by institutional policy and procedure. The Office of the University Registrar houses archived physical records on microfilm. These records are accessible only to individuals with authorized key card access. The Student Academic record is primarily stored in secure electronic systems including Ellucians Banner Student Information System and Ellucian Banner Document Imaging System. The security of student record systems is enforced according to USC System Policy UNIV 1.52 Responsible Use of Data, Technology, and User Credentials. [4] All employees authorized by their hiring units to gain access to student records and agree to abide by university policy related to security of student academic records. Employees who have not logged into student record systems for more than six months are deprovisioned from those systems. Employees are inactivated from authenticating into student records systems when terminated from the institution.

When we are notified or observe a potential information security or data breach incident, we follow the SANS Institute Incident Response Process: preparation, identification, containment, eradication, recovery, and lessons learned. Depending on the severity of the incident, steps may involve the USC University Information Security Office or law enforcement during the response. In the event of a data breach, we work with the University's legal team and conform to all requirements under United States Federal and South Carolina State laws regarding breach notifications. We would also use the NIST Data Breach Response Guide [10] and the SANS Institute Breach Incident Notification Handling [11] paper as guides for this process.

Data Protection Backup and Resiliency. The current USC System enterprise database backup retention policy is 30 days on-site with prior 30 days stored off-site. A multilayered approach to data protection has been implemented for data and services residing on campus. The initial layer of protection occurs whenever a block of data is written to disk. All data that exists on our VNX 5200 array is journaled, giving us the ability to perform real-time reversions up to 24 hours. This provides a quick, readily accessible safeguard against data corruption.

The next layer is also provided by the VNX 5200. All data that exists on this array, except in LUNs excluded for security and privacy reasons, is replicated at the block level to an identical array in our disaster recovery cabinet in Columbia. The USC Aiken Division of Computer Service is in the process of upgrading equipment hosted at USC Columbia. The auxiliary array provides additional space for journaling and snapshots, enabling USC Aiken Computer Service Division to perform real-time reversions beyond 24 hours. Additionally, since this array receives real-time block changes from the primary array, the current state of the University's data is continuously available on this array whenever it is needed. This enables Computer Service personnel to provide data recovery services up to the last block change, restore servers to a current state, and provide service continuity during disaster recovery.

The final layer is provided by a pair of Barracuda Backup 800 appliances. The primary appliance resides on campus and performs scheduled point-in-time archival of file systems, system states, and databases. This enables personnel in Computer

Services to perform file, database, and system restoration for up to 60 days. The primary appliance replicates all data it receives to the auxiliary appliance, which resides in our disaster recovery cabinet in Columbia.

For hosts which reside in Azure, Computer Services uses Azure Backup Services for data protection. Each virtual disk has at least one snapshot taken daily, which are kept for 60 days.

Disaster Recovery. The USC Aiken disaster recovery plan separately addresses internal and public technology assets. In the event of a data center outage or loss, hosts providing internal services would be brought online in a vSphere cluster residing in the disaster recovery cabinet in Columbia. Those services would then be accessible from the campus when network connectivity is restored. Hosts providing public services would be imported to Azure and brought online in that environment.

Supporting Documentation

1. USC System policy UNIV 1.51 - Data and Information Governance
2. State of South Carolina Information Security Policy
3. National Institute of Standards and Technology (NIST) publication SP 800-60 (Guide for Mapping Types of Information and Information Systems to Security Categories)
4. USC System policy UNIV 1.52 Responsible Use of Data, Technology, and User Credentials
5. USC System policy IT 3.00 Information Security
6. USC System policy HR 1.22 Telecommuting
7. USC System policy ACAF 3.03 – Handling of Student Records
8. USC Aiken Academic Bulletin: FERPA
9. SC Code of Laws 30-2: South Carolina Family Privacy Protection Act of 2002
10. NIST Data Breach Response Guide
11. SANS Institute Breach Incident Notification Handling