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.

Judgment

☑ Compliant ☐ Non-Compliant ☐ Not Applicable

Narrative

The University of South Carolina and regional Palmetto College campuses has established multiple system-wide policies that collectively address security, confidentiality, and integrity of student records.

Data Stewardship and Governance

UNIV 1.51 *Data & Information Governance* 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 & integrity assurance, and business intelligence. The policy also establishes the university's data classification schema, which is consistent with State of South Carolina policy, 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). The policy embraces principles, guidance, and best practices promulgated by the US Department of Education's Privacy Technical Assistance Center.

UNIV 1.52 *Responsible Use of Data, Technology, and User Credentials* 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.

IT 3.00 *Information Security* 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 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 university'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, but leveraging the incredible potential of CMDB to enhance security, system integrations, and strategic IT planning.
- The 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 University Registrar serves as the data steward and administrator for the student academic record.

The Directors of Financial Aid for the Columbia campus and regional Palmetto College campuses serve as data stewards and

administrators over their respective financial aid records.

The University Bursar is the data steward and administrators for student accounts receivable records.

The Assistant Vice President for Planning, Assessment and Innovation serves as the data steward and administrators for co-curricular records.

The Assistant Vice President for Student Success services as the data steward and administrators for undergraduate advising data.

Disciplinary records on the Columbia Campus fall under the stewardship of the Executive Director of Student Conduct and Academic Integrity.

Stewardship of student employment records is handled by the Director for HR Operations and Services.

Systems with Student Records

The University of South Carolina maintains student records and delivers student record services through multiple 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.

Beyond the Classroom Matters Student Information System

Beyond the Classroom Matters is a supplemental student information system for documenting student engagement and learning in experiential courses and the co-curriculum.

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.

EAB Navigate

EAB Navigate 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.

Integrity

The University of South Carolina Columbia 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 university'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* 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)
- 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.

- HR 1.22 *Telecommuting* 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 Division of IT's Information Security program 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 (including State of South Carolina), and numerous tools available to assist with the prevention, detection and response of unauthorized access to University of South Carolina information assets.

Integrity of student data is upheld primarily by functional organization units in the Division of Student Affairs and Academic Support. DoIT supports 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, DoIT processes the request through detailed service delivery protocols.This includes initial screening, a security review, governance approval by the Student Systems Council, and approved efforts undergo development by Application Services, which validates and iteractively improves the accuracy of the request and delivery with the customer.

Data quality & integrity assurance

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 is correct, complete, and accurate, yielding data that is of high quality with necessary integrity. Such data is required by the Office of Institutional Research, Assessment, and Compliance, to produce official reports and surveys, and is essential to produce reliable business intelligence and analytics from raw data.

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 manual, FERPA regulations are published in each annual academic bulletin of the Columbia and regional Palmetto College campuses.

Columbia

Undergraduate Studies Bulletin | FERPA Notice

Graduate Studies Bulletin | FERPA Notice

School of Law Bulletin | FERPA Notice

School of Medicine Bulletin | FERPA Notice

Regional Palmetto College Campuses

Lancaster Bulletin | FERPA Notice

Salkehatchie Bulletin | FERPA Notice

Sumter Bulletin | FERPA Notice

Union Bulletin | FERPA Notice

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 (Banner®). After passing the quiz, the individual must print out and sign the Banner Account Request Form (see below), 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 FERPA, the South Carolina Family Privacy Protection Act of 2002 (SC Code of Laws 30-2), and the following policies and procedures to ensure student record confidentiality:

ACAF 3.03 Handling of Student Records
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
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
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, confidentiality, integrity, 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
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.

DegreeWorks

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 to institutional policy and procedure.

Physical Records

The Office of the University Registrar houses archived records on microfilm. These records are accessible only to individuals with authorized key card access. Both motion detection alarm and camera surveillance systems are in place in the Office of the University Registrar's Office to monitor the office area during and outside of office hours according to University Policy LESA 3.12 *Access Control, Alarm and Video Security Systems*. Office of the University Registrar employees are required to complete security training which covers both physical and electronic records.

Electronic Records

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 University Policy UNIV 1.52 *Responsible Use of Data, Technology, and User Credentials*. 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 that six months are deprovisioned from those systems. Employees are inactivated from authenticating into student records systems when terminated from the institution.

Data center access is restricted by Carolina Card authorization to Faculty/Staff/Students that require access to the facility. Authorization is requested and must be approved by the supervisor or department head. An annual purging of the data center access list occurs after the Spring semester (less DoIT staff that are required access for their jobs) and access must be renewed and approved each year for continued access. The data center is monitored with cameras and procedures to scan in/out of the data center each time entry is required.

Data Protection and Backup

The current file system and database backup retention policy is 30 days on-site with prior 30 days stored off-site. There is not a current Disaster Recovery Plan that includes off-site resources.

University IT Compliance Auditing

The university's requirements, standards and guidelines for the protection of information assets are rooted in policies UNIV 1.51, UNIV 1.52, and IT 3.00. Organizational units throughout the University of South Carolina system are empowered and accountable for the implementation and maintenance of these requirements and are subject to audits by the university Division of Audit and Advisory Services.

Sources

- ACAF 3.03 Handling of Student Records
- Banner Access and Confidentiality Form
- Cognos Data Access Agreement
- DegreeWorks Access request
- FERPA
- Graduate FERPA Notice
- HR 1.22 Telecommuting
- IT 3.00 Information Security
- LESA 3.12 Access Control, Alarm and Video Security Systems
- Lancaster Bulletin
- Law FERPA Notice
- Policies and Procedures Manual

- Salkehatchie Bulletin
- School of Med FERPA Notice
- Sumter Bulletin
- UNIV 1.51 Data and Information Governance
- UNIV 1.52 Responsible Use of Data, Technology, and User Credentials
- Undergraduate FERPA Notice
- Union Bulletin
- nistspecialpublication800-60v1r1