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

SACSCOC Reviewer Comments

Non-Compliance

The institution's response is in violation of the Southern Association of Colleges and Schools Commission on Colleges (SACSCOC) policy, "Reports Submitted for SACSCOC Review," by including live links in its response and electronic documentation that is not consistently bookmarked, indexed, and searchable.

The institution protects student records guided by State of South Carolina Policy, best practices from the US Department of Education, and the National Institute of Standards and Technology. The Off-Site Reaffirmation Committee reviewed the institution's definitions, policies, manuals, and system-wide data information governance used to protect student records. The institution's Chief Data Officer oversees information security inclusive of institutional data sharing agreements. The institution utilizes multiple student records systems to process and protect the confidentiality of student data. The student records systems they utilize are respected systems in higher education and are sufficient to maintain confidentiality of student records.

In compliance with data integrity expectations, the institution has established a Responsible Use of Data, Technology and User Credentials policy. This policy outlines employee data integrity and confidentiality expectations, along with measures to educate and enforce these institutional standards. Appropriate security measures are in place and were identified for both physical records and electronic records. The institution acknowledged "there is not a current disaster recovery plan that includes off-site resources." The Off-Site Reaffirmation Committee was unable to verify the security of student records; the institution needs to provide information about its disaster plan for records retrieval.

Campus Response

During their review, the Off-Site Reaffirmation Committee noted that they were unable to verify the security of student records. The committee also noted that information about a disaster plan for records retrieval was needed.

In the original submission, the university stated "There is not a current Disaster Recovery Plan that includes off-site resources."

This statement was originally included because of a misunderstanding related to the use of "off-site." There is not a secondary, off-site physical location at which dedicated back-up equipment, running the current version of applications and operating system patches, is used to store backup student-records data. There is, however, a detailed Disaster Recovery Plan and process that includes a Cloud server/storage solution (a virtual off-site location) in lieu of a physical secondary location. In the event of a disaster, critical servers running enterprise business functions, will be recreated in the Cloud from the backups.

The current Disaster Recovery plan (Document 01) was originally drafted in 2016. When the university's mainframe was retired in April, 2020, the Disaster Recovery Plan was updated to remove mainframe references and the Amazon Web Services (AWS) Cloud recovery site information was added.

AWS Cloud
All DoIT managed server configurations, files systems, and databases (including student record systems) are backed up locally and a secondary copy is stored in the AWS Cloud. In the event of a disaster, the AWS Cloud is identified as the virtual recovery site.
This Cloud service provides on-demand IT resources over the Internet in a pay-for-use model. Cloud services allow information to be stored, and backed-up, in a virtual environment. Cloud services eliminate the need for another physical backup location and are considered more secure, as they are not susceptible to natural disasters such as fire or flood. In the event of a disaster, critical servers running enterprise business functions at the University of South Carolina can be recreated in the AWS Cloud from the backups.

Disaster Recovery Plan
The retention policy for on premise backups is 15 days and 30 days for (virtual) offsite back-ups. These are standard practices and retention and can be extended with additional investments. The Disaster Recovery Plan outlines Recovery Time Objectives (RTO) or the estimated time to recover, and Recovery Point Objectives (RPO), age of recovered data (Document 01, pages 13 & 14, respectively). RTO and RPO describe the time to recover and how much data may be lost based on the time that has elapsed between the last backup and the time of the disaster. RTO & RPO are estimates establishing when a service can be restored and with what level of data integrity.

Off-Site Physical Backup of Non-Student Information
Individual departments can also use "share drives" to store unit-level data, reports, and information. These share drives are

not used to store student records. The drives are replicated daily and saved on similar hardware located at the Upstate campus in Spartanburg, SC. This location is covered by the 30-day retention policy.

Sources

- 12.5 Student Records Off-Site Committee Feedback
- Document 01_2020 Disaster Recovery Plan