Southern Arkansas University Student Privacy and Data Protection Policy

Southern Arkansas University (SAU) is committed to ensuring the privacy and accuracy of confidential information. SAU does not actively share personal information gathered from our Web servers. However, because SAU is a public institution, some information collected from the university websites, including information from our server logs, e-mails delivered to the university, and information collected from Web-based forms, may be subject to the Arkansas Freedom of Information Act. SAU does not actively share information, unless compelled by law to release information gathered from our Web servers.

Southern Arkansas University also complies with the Family Educational Rights and Privacy Act (FERPA), which prohibits the release of education records except in limited circumstances (i.e., with the student's permission, to parents of dependent students, and in response to a valid court order). For more information on FERPA at Southern Arkansas University, go to https://web.saumag.edu/registrar/ferpa/

Although FERPA regulations apply only to students, Southern Arkansas University is equally committed to protecting the privacy of all visitors to our websites. SAU also complies with the applicable provisions of the Gramm-Leach-Bliley Act (GLBA) https://web.saumag.edu/glba/ and the Health Insurance Portability and Accountability Act (HIPAA) https://web.saumag.edu/health/policies/. Further information about these follows.

Sharing information

Unless required by the Arkansas Freedom of Information Act, it is against university policy to release information gathered through the Web, such as pages visited or personalized preferences. Southern Arkansas University does, however, share information with other parties at the request of users (persons to whom the information applies). For example, the university receives test scores from testing agencies and will send transcripts to other schools at the student's request.

Consistent with FERPA, SAU does not release personal student information, other than public directory information, to other parties unless we have legal authorization to do so. Student directory information may be released without the student's written consent. Directory information includes: name, address, and telephone number, SAU e-mail address, major field of study, participation in officially recognized sports, weight and height

of athletes, dates of attendance, i.e., an academic year, a spring or fall semester, or summer, degrees and awards received, most recent previous educational agency or institution attended. If a student does not want their directory information released, the student may request in writing that it not be released and file the request with the Office of the Registrar.

SAU complies with all laws that prohibit the release of information. This includes student education records protected by FERPA, financial information, including credit card information protected by GLBA, and personal health information protected by HIPAA. However, other information collected from the SAU websites, including server log information, emails delivered to the university, and information collected from Web-based forms, may be subject to the Arkansas Freedom of Information Act.

Personal Information Protection

SAU's website will only collect personal information that individuals knowingly and voluntarily provide by, for example, sending emails, completing membership forms, registering for classes or other programs, responding to surveys, or ordering merchandise. Individuals that provide contact information will be contacted by the appropriate unit (admissions, financial aid, communications, etc.) and that unit will respond to inquiries and/or requests. The unit will also provide information about college activities, programs, membership and development opportunities, and special events that may be of interest. It is university policy that confidential information submitted is used only for the purposes described in that transaction, unless an additional use is specifically stated on that site.

Southern Arkansas University will only share information with other parties when one or more of the following conditions apply:

- consent to share the information is provided by the individual
- need to share information to provide the service or product requested
- need to send information to companies who work on behalf of Southern Arkansas University to provide a service or product to who operate under the same privacy policy as SAU
- considered directory information consistent with FERPA regulations
- respond to subpoenas, court orders, or any other legal process
- find it necessary to protect and defend the health and safety of an individual

SAU uses encryption to prevent third parties from accessing sensitive data, such as passwords, e-commerce information, etc. Access required to enter an SAU protected web

unit requires username and password when requests for data considered private or to ensure authorized access. For example, students who want to check their grades or staff members who complete time sheets must enter their SAU username and password so the system knows who is requesting the data. This login process uses SSL Certificates so the user name and password are encrypted between the Web browser and our Web server.

Several sites within Southern Arkansas University enable online payment for products or services online with a credit card. These transactions are encrypted. Questions about security concerns involving credit card transactions may be directed to the SAU Vice President for Finance or Director of Information Technology Services (ITS) or Associate Director of ITS for Information Systems.

The SAU website automatically gathers and stores the following information about visits to track the use of our website to make improvements. This information is stored and used in the aggregate only and is not under normal circumstances used to make individual contact:

- The IP used to access the SAU website
- The name of the domain from which access to the Internet (for example, aol.com, if connecting from an America Online account)
- The type of browser and operating system used to access the SAU website
- The date and time of site access
- The pages, files, documents, and links visited

European Union General Data Protection Regulation (ED GDPR) Privacy Notice

The EU GDPR provides broad privacy protections to individuals physically located in the European Economic Area ("data subject(s)"). Under certain circumstances, the EU GDPR may apply to Southern Arkansas University's activities in the European Economic Area, for example, when a student attends a semester-long study abroad program in the European Economic Area. When subject to the EU GDPR, Southern Arkansas University must comply with the regulation's core privacy principles which provide that personal data shall be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Limited to what is necessary in relation to the purposes for which they are processed; Accurate and kept up to date;
- Retained only as long as necessary; and

- Secure.

Personal data is defined very broadly under the EU GDPR and consists of any information relating to an identified or identifiable person and includes a person's name, identification number, location data, online identifier, or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that person.

Lawful Basis for Processing Personal Data

When subject to the EU GDPR, Southern Arkansas University must have a lawful basis to process a data subject's personal data. Although there will be some instances where the processing of personal data will be pursuant to other lawful bases (e.g., processing necessary to protect the vital interests or safety of a data subject, processing related to legal action involving the university, etc.), Southern Arkansas University will likely process personal data relying on one or more of the following lawful bases:

- Processing for the purposes of the legitimate interests pursued by Southern Arkansas University or by a third party;
- Processing for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing for compliance with a legal obligation to which Southern Arkansas University is subject; and
- Processing pursuant to the consent of a data subject for one or more specific purposes.

Types of Personal Data Processed

In order for the university to achieve its core mission, it is essential and necessary for Southern Arkansas University to process personal data of its students, employees, applicants, research subjects, alumni, and others involved in the university's educational, research, and community programs. Southern Arkansas University processes personal information for various lawful reasons, including, without limitation, academic admissions and enrollment; student registration; residence life; delivery of classroom, on-line, and study abroad education programs; administration and oversight of recreation programs, student organizations, and other various student affairs activities; distribution of grades, materials, and other communications by and among students, faculty, and staff; employment; applied research; program development and analysis; job hiring and employment; provision of medical services or health insurance; engagement with the

community at-large; compliance with its internal policies, procedures, and guidelines, as well as all applicable federal, state, and local laws; and records retention. Personal data processed by the university typically includes name, address, email, phone number, transcripts, work history, financial information, information for payroll, research subject information, medical and health information (for admissions, student health services, travel, etc.), and donations. For specific questions regarding the collection and use of personal data, please contact the Vice President for Administration and General Counsel. If a data subject refuses to provide personal data that is required by Southern Arkansas University in connection with one of Southern Arkansas University's lawful bases to collect such personal data, such refusal may make it impossible for Southern Arkansas University to provide education, employment, research, or other requested services.

Where Southern Arkansas University gets Personal Data

Southern Arkansas University receives personal data from multiple sources, most often directly from the data subject or under the direction of the data subject who has provided it to a third party that SAU has a business agreement to acknowledging the security and student privacy requirements.

Individual Rights of the Data Subject under the EU GDPR

Subject to all other applicable laws and regulations, including all laws of the United States of America and the State of Arkansas (USA), data subjects have following rights under the EU GDPR:

- To access the personal data SAU maintains;
- To be provided with information about how personnel data is processed;
- To correct or modify personal data;
- To have individual personal data deleted;
- To object to or restrict how personal data is processed;
- To request personal data to be transferred to a third party; and
- To file a complaint.

To exercise the above rights, data subjects should contact SAU Vice President for Administration and General Counsel who will consider and process a data subject's request within a reasonable period of time. Please be aware that under certain circumstances, the EU GDPR or other applicable law may limit a data subject's exercise of the above rights.

Security of Personal Data subject to the EU GDPR

Southern Arkansas University will comply with all of its published data protection policies in the processing of a data subject's personal data.

Data Retention

Southern Arkansas University keeps the data it collects for the time periods specified in the State of Arkansas Records Retention Guide.
https://dese.ade.arkansas.gov/Files/20201102131206_rec_retention_schedule.pdf

Disclaimer of Liability

The information contained in this policy explains the Internet privacy policy and practices that Southern Arkansas University has adopted for its official Web pages. In legal terms, it shall not be construed as a contractual promise, and the university reserves the right to amend it at any time without notice. Neither Southern Arkansas University nor any of its units, programs, employees, agents, or individual trustees shall be held liable for any improper or incorrect use of the information described and/or contained in the university website and assumes no responsibility for anyone's use of the information. Southern Arkansas University is a large organization with many people sharing responsibility for the content of our website. Comments and inquiries can be sent to individual units at address on the SAU Website, and this will speed response. For questions about this Privacy Statement or SAU Web pages that do not adhere to this statement, please email the Manager of Web Services: joshjenkins@saumag.edu.

Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act (GLBA) enacted by the United States Congress that became effective in 2003 applies to financial institutions and institutions of higher education and established privacy and security provisions that are designed to protect consumer (students treated as a consumer) financial data. GLBA mandates how higher education institutions collect, store, and use student financial records (e.g., records regarding tuition payments and/or financial aid) containing personally identifiable information. GLBA regulations include both a Privacy Rule (16 CFR 313) and a Safeguards Rule (16 CFR 314), both of which are enforced by the Federal Trade Commission (FTC) for higher education institutions. Colleges and universities are deemed to be in compliance with the GLBA Privacy Rule if they are in compliance with the Family Educational Rights and Privacy Act (FERPA). The Safeguards Rule was promulgated in 2002, with compliance documentation required in May 2003.

The objectives of GLBA are to ensure the security and confidentiality of student financial information, protect this information from any anticipated threats or hazards to the security or integrity of such information, and to protect against unauthorized access to or use of such information that could result in substantial harm to any student. While there is overlap with FERPA, GLBA Safeguard Rule still applies. FERPA covers students' *educational records* including their right to access and inspect and what information can be disclosed. GLBA focuses on *nonpublic personal information* which is usually limited to individual's financial information obtained in connection with a financial product or service.

The types of information covered as *nonpublic personal information* that may be required in connection with a financial product or service offered or serviced by or on behalf of SAU can include:

Account Balances, Account Numbers, and Social Security Numbers
Student Financial Aid Information (application through award)
Debit/credit card numbers, payment history, and credit score or rating

Family Educational Rights and Privacy Act

Family Educational Rights and Privacy Act of 1984, also known as the Buckley Amendment, helps protect the privacy of student records. The Act provides for students the right to inspect and review educational records, the right to seek to amend those records and to limit disclosure of information from the records. The Act applies to all institutions that are the recipients of Federal funding. See https://web.saumag.edu/registrar/ferpa/ Institutions may disclose information about a student without violating FERPA through what is known as "directory information." This generally includes but is not limited to the following information:

a.) Name, address, and telephone number.
b.) University e-mail address.
c.) Major field of study.
d.) Participation in officially recognized sports.
e.) Weight and height of athletes.
f.) Dates of attendance, i.e., an academic year, a spring semester, or a first quarter.
g.) Degrees and awards received.
h.) Most recent previous educational agency or institution attended.

FERPA Brochure FERPA Release Form

Southern Arkansas University Information Security Plan

The security plan seeks to:

1. Ensure the security and confidentiality of covered data and information
2. Protect against anticipated threats to the security or integrity of such information
3. Protect against unauthorized access to, or use of, covered data and information th at could result in substantial harm or inconvenience to any student

While the security plan largely affects the University's Information Technology Services (ITS), others that collect covered data in the normal course of business will also be affected. Those areas include but are not limited to the Offices of Admissions, Registrar, Financial Aid, Business Office, Student Life, Human Resources, and various third-party contractors.
Each area is responsible for securing customer information according to University policies.

Information Security Team

The University has established an Information Security Team that consists of five positions. They are:

The Vice President for Finance oversees data security policies for the Business Office and related third party contractors and serves as Coordinator.

The Vice President for Student Affairs overseas data security policies for the Offices of Admissions, Student Life, Student Housing, and Health Services.

The Vice President for Administration and General Counsel ensures periodic training to all staff regarding privacy policies on covered information..

The Director of Financial Aid and the

Director of Information Technology Services.

Risk Identification and Assessment

The Information Security Team will meet annually, or as needed, to identify reasonably foreseeable risks to data security and privacy, along with the sufficiency of safeguards in place to control these risks. Current risks may include, but are not limited to the following:

- Unauthorized access to data through software applications
- Unauthorized use of another user's account and password
- Unauthorized viewing of printed or computer displayed data
- Improper storage or destruction of printed and digital data

Designing and Implementing Safeguards

After such risks are identified, the Information Security Team will ensure that reasonable safeguards and monitoring are implemented. Such safeguards and monitoring will include the following:

•Employee Management and Training – The Office of Human Resources requires annual training through a Blackboard course to all employees regarding privacy and security policies on covered information. Other training resources are available on the University's website to access throughout the year. In addition, supervisors will provide job-specific training on maintaining security and confidentiality of covered data in their respective areas.

• Information Systems – The Director of Information Technology Services (ITS) ensures adequate safeguards within the University's information systems, which include network and software design, information processing, and the storage and transmission and disposal of covered electronic data. Access to covered data through the University's information systems is limited to those employees who have an educational or professional responsibility with such information. User specific passwords are required to grant access to the appropriate level of information. ITS maintains policies on the required strength of passwords and periodic changes to those passwords. In addition, all servers are verified and secured before being permitted through the University's firewall.

Physical Records – Physical records should be stored in a secure area with limited access and reasonable protection against hazards such as fire or water damage. University offices utilizing covered data are locked nightly and when unattended. The main data center is secured via proximity cards or keys. The University has adopted the State of Arkansas Records Retention policy and periodically contracts with certified shredding service providers to dispose of physical records containing covered information.

Management of System Failures – ITS will evaluate its procedures and methods of detecting, preventing and responding to information system attacks or other system failures. ITS has recommended responses which guide the actions users should take when a suspected attack occurs. Immediate response plans will be developed in the event an issue arises.

Overseeing Service Providers

In the normal course of business, the University may appropriately share covered data with third parties. Such activities may include collection activities, transmission of documents,

destruction of documents or equipment, or other similar services. New and renewed contracts and service agreements involving covered data will be selected and approved to those providers that are capable of maintaining appropriate safeguards for the customer information.

Adjustments to Program

The security plan and related policies will be evaluated and adjusted in light of relevant circumstances, or as a result of testing and monitoring the safeguards. The most frequent of these reviews will occur within ITS, where constantly changing technology and evolving risks mandate increased attention.

System Security

Firewalls monitor and control incoming and outgoing network traffic based on predetermined security rules.

The Email Security Gateway inspects incoming and outgoing email for malicious cod e and
prevents transmission. Additionally, content that contains social security, or other similarly formatted numbers, will be prevented from outgoing email delivery.

All campus computers run antivirus software.
SSL certificates are used to provide security for online communications when accessing sensi tive data through web servers. ITS maintains a procedure to update security patches.
Network equipment is located in locked areas with limited access by ITS managers, technicia ns, and engineers.

External network vulnerability scanning is scheduled annually through Division of Legislative Audit or the ARE-ON organization.

An audit log records system changes and can be accessed when necessary.
System Access to
ERP system users are assigned limited role-based access to applications providing secure information.

Employees can directly access the ERP systems data from remote locations through the use of a virtual private network (VPN). The VPN connection encrypts and secur es data transmissions.

All passwords should remain secure to the user and should not be shared or visible t o others.

User passwords on the ERP systems are required to change every 90 days. In addition, password complexity (variety of upper and lower characters and numbers between 1-9 and special characters) is enforced.

With three (3) login failures to the ERP systems, accounts are automatically suspende d and denied access for at least 30 minutes.

Wireless access to ERP systems via SkyLite requires Secure Shell (SSH) protocol.

Computer accounts are disabled as quickly as possible after an employee terminates.
Information Transmission, Retention, and Disposal.

Select information is transferred from ERP to third parties via Secure FTP with public -private key encryption.

To provide for disaster recovery, all ERP data is backed up to disk in a secondary datacenter nightly and stored securely with limited access. In addition, selected critical ERP data is stored at Jenzabar's datacenter located in Tulsa, Oklahoma, nightly.

Backups for data centers servers are done hourly using deduplication. Two copies are

Backups for data centers servers are done hourly using deduplication. Two copies are maintained.

Monitoring of key systems locations are in place to notify ITS staff of datacenter power outages and high room temperatures with gas generators available if needed.

Hard drives are removed and destroyed by drilling holes through them or by comme rcial shredding.

Website and Cloud-Based Data Security Data Collection and Storage

The Southern Arkansas University website collects data from the students and the public through a variety of online forms and applications. All form submissions are received and transmitted over secure SSL-encrypted connections with privately signed security certificates. Routine security audits of cloud-hosted platforms are conducted to ensure best practices.

The vast majority of online forms and applications are managed through the University's WordPress installations. Access to this data is limited to authorized staff members through secure online logins with password strength monitoring, as well as a robust firewall to detect and prevent DDOS attacks and other attempts at intrusion. Sensitive data collected online is encrypted in the web server's databases and at no point is private financial data or highly-sensitive personal data (SSNs) programmatically transmitted over email or any less secure method of transmission.

Online Payment

While SAU does not collect or store private student loan information or account data through the public website, there are a variety of forms that accept online payments from students and the public. These payments are processed exclusively through a PCI-compliant payment method via Authorize.net and at no point is credit card information stored on SAU web servers. Similar to any other web hosted form, non-payment related data may be collected and stored, but access is limited to approved staff members through encrypted and password protected means.

Related Links

- CSF Firewall, used on web server - https://www.configserver.com/cp/csf.html
- Word Fence firewall and security for WordPress - https://www.wordfence.com/
- Rave Alerts - https://www.ravemobilesafety.com/
- Alertus https://www.alertus.com/compliance

- 3rd Millennium Classrooms - https://web.3rdmil.com/s
- Farmers Bank and Trust - https://www.myfarmers.bank/resources/security
- Blackboard - https://help.blackboard.com/Product_Security
- Handshake - https://joinhandshake.com/security/
- Terra Dotta - https://www.terradotta.com/files/Tech-Docs_Information-Security-Policy.pdf
- National Student Clearinghouse - https://www.studentclearinghouse.org/
- SAU ITS Policies and Procedures - https://web.saumag.edu/its/information/policies/