SOUTHERN STATES UNIVERSITY

Student Records, Privacy, and Information Security Program

Main Campus: 1094 Cudahy Place, Suite 120,
San Diego, CA, 92110
Phone: (619) 298-1829

Branch Campus: 2855 Michelle Drive, Suite 380
Irvine, CA 92606
Phone: (949) 833-8868

Branch Campus: 2000 South Jones Boulevard, Suite 120
Las Vegas, NV 89146
Phone: (702) 786-3788

Website: www.ssu.edu
Email: info@ssu.edu

Online Manual Location: https://www.ssu.edu/wp-content/uploads/2015/01/SSU-Records-Privacy-Info-Security-Program-manual.pdf

Student Records, Privacy, and Information Security Program

At Southern States University, nothing is more important to us than the success of our students and website users, including the protection of their personal data. With students and users from all around the world, the University adheres to the following records, privacy, and information security regulations:

- Family Education Rights and Privacy Act (FERPA),
- Gramm-Leach-Bliley Act: Sections 501 and 505 (b) (2),
- FTC regulations: 16 CFR 313.3 (n) and 16 CFR 314.1-5
- US Code: 15 USC 6801 (b), 6805 (b) (2)
- European Union's General Data Protection Regulation (GDPR).

Southern States University has designed the information security program under the direction of the Director of Administration and in collaboration of the Office of the Registrar. The Director of Administration is the officer responsible for oversight, revision, and maintenance of the University's security program. The Office of the Register is responsible for collecting and maintaining official academic records for all applicants and students admitted to Southern States University and promotes student success beginning with the student's application to the University and concluding with graduation from SSU.

All documents submitted to the University become the permanent possession of SSU and cannot be returned to applicants and students under any circumstances. Applicants and students are encouraged to make copies of important documents and maintain said copies for their personal files.

Holds may be placed on student records, transcripts, grades, or registration because of financial or other obligations to the University. Satisfaction of holds is required before a release is granted.

The Office of Admissions and Records for all students is maintained at the University office in San Diego, CA. Requests for information should be sent to SSU Admissions and Records, 1094 Cudahy Place, Suite 120, San Diego, CA, 92110 or registrar@ssu.edu.

FERPA: Confidentiality and Release of Student Records

Southern States University adheres to the regulations and guidelines outlined in the Family Education Rights and Privacy Act (FERPA) of 1974. Under FERPA, school officials may not disclose personally identifiable information, nor permit inspection of student records without written permission from the student (unless such action is covered by exceptions permitted by the Act), and students are permitted to inspect their personal education records.

Education records are any records, with certain exceptions, maintained by University that directly relate to a student's education. This includes any and all information, maintained in any medium, that is directly related to students and from which students can be personally identified. The following are considered part of a student's educational record:

- Letters of recommendation (Note: students do not have the right to inspect these letters unless the author of the recommendation has granted such a waiver.)

- Student enrollment, registration, and course completion data, including course assignments and final grades
- Student applications forms
- Student transcripts from previously attended institutions, including high school and other colleges and universities
- Directory Information

Access to Academic Records and Information:

Under FERPA, students have the right to inspect and review their personal student educational records within 45 days of the day the University receives a request for access. Students also have the right to request an amendment of their educational records that are believed to be inaccurate or misleading, and the right to consent or revoke the disclosure of all or part of their educational records, including Directory Information.

- Students should submit a written request to the Registrar specifying the record(s) they wish to inspect. The Registrar or Registrar's designee will make arrangements for access and notify the student of the time and place where the records may be inspected.
- Students seeking to amend or contest content within their student record. Students may request a determination regarding changes to their records. Such requests must follow the Academic Grievance and Appeal Policies and Procedures. Upon receipt of the request, the Registrar will initiate a review, consulting with any appropriate University official and/or forwarding the request to such officials when necessary. A decision regarding the request will be rendered within 30 days except where a request may require additional pertinent information or verification from an outside agency or party, in which case the decision will be rendered within 30 days after receipt of such information. If a material error in the record is established, or an update is warranted, a change or correction will be made.
- Students wishing to disclose their record to a person or entity other than themselves must provide SSU with a written release to that third party.

Students have the right to consent to the disclosure of personally identifiable information (PII) contained in their educational records, except to the extent FERPA authorizes disclosure without consent, as listed below:

- Disclosure of information to school officials is limited to the needs of the official to execute their official duties and under the existence of a legitimate educational interest. A school official is a person employed or appointed by the University to serve as an administrator, faculty member, or as support staff; a person or company with whom the University has contracted, or a student serving on an official committee (such as a disciplinary or grievance committee) or assisting another school official in performing his or her tasks.
- Law enforcement may access student records under a subpoena.
- Upon request, the University discloses educational records without consent to officials of another school in which a student seeks or intends to enroll. (Note: FERPA requires that the University make a reasonable attempt to notify the student of the records request).

- Accreditors and regulatory organizations that have a right to inspect student records without explicit student consent to the extent that the accrediting and regulatory organizations need the record in order to carry out their official evaluation or function.
- Students wishing to authorize another party (e.g., spouse or financial sponsor) to access personal and specific student data, must submit a written notification to the University with the full name of the person or agency and what information may be disclosed. Named parties must know PII regarding the student before any University official will discuss student records with the named party.

Directory Information:

In accordance with FERPA, schools may disclose what the institution has deemed "Directory Information "to third parties without student consent. Southern States University has designated the following information as "Directory Information" within the provisions of 34 CFR § 99.37 and the applicable regulations as this information is generally not considered harmful or an invasion of privacy if released. Directory information is provided upon request in accordance with state and federal laws and statutes.

- Student name,
- state of residence,
- email address,
- program of study,
- registration status (active, inactive, probation, dismissal, or graduate)
- enrollment status (full-, half-, part-time, or LOA),
- dates of attendance,
- credentials, honors, and awards received, and
- the most recent educational agency or institution attended.

Additional Directory Information of Student Employees:

- Department where employed, and
- Job title. (i.e. Administrative Assistant, Marketing Assistant)

Students have the right to refuse to allow the University to release any or all of this information as directory information. Students wishing to withhold Directory Information must submit a signed written request to the SSU Office of Admissions and Records, Attn: Registrar.

In accordance with the Family Educational Rights and Privacy Act (FERPA), personally identifiable information in education records may not be released without prior written consent from the student. Some examples of information that WILL NOT BE RELEASED without prior written consent of the student are:

- birth date
- citizenship
- disciplinary status
- ethnicity

- gender
- grade point average (GPA)
- marital status
- SSN
- student I.D
- Grades and exam scores
- Test scores

The University will not release personally identifiable information from a student's education records without the student's prior written consent. Notwithstanding this policy, exceptions may be made for authorized officials of State or Federal agencies, if and when such access is necessary for audit or evaluation of educational programs supported by such agencies.

Records Retention:

Student records will be retained according to the following schedule:

- For students who apply to the University but take no further actions with the university (including registration and enrollment), the minimum retention period is one (1) year after the application term.
- For students who enroll, the minimum recommended retention period is seven (7) years after the date of graduation or last date of attendance, whichever is later.
- Data and documents that are FERPA related or relative to final student transcripts are retained permanently, including requests for hearings, requests and disclosures of personally identifiable information, student requests for non-disclosure of directory information, student statements on content of records regarding hearing panel decisions, student's written consent to records disclosure, and waivers for rights of access.

Student Verification

All students and any student designees must verify at least four pieces of PII before any student record information will be discussed or released over the phone, in person, or via email. Should students wish to discuss their student account in person with a University official, the student must produce a government-issued photo ID card and named third parties must verify at least four pieces of personally identifiable information.

Policy for Online Student Verification

According to the U.S. Higher Education Opportunity Act of 2008, Southern States University needs to verify that a student who registers in our online course management system, Moodle, will be the same student who completes all course assessments as given in a course. At Southern States University, students in online and onsite courses are required to use Moodle, a secured online portal requiring a unique username and password, using the assigned Moodle username as given at the time of admissions at the University. Consequently, individual instructors will be able to check the identity of a student by checking a student's activity record on Moodle which contains the IP address, login and access dates, and specific time spent on Moodle under different activities, such as online exams. There are no additional charges for this online verification process.

Student Identity Protection

Upon admission, students will be assigned a Moodle account. Students must provide the University with a full name and email address which will be used for the creation of a student's account on Moodle. A student's name will be made available to other students enrolled in a course on Moodle; however, email addresses will not. A student on Moodle will have the option of making his/her own email address available to the rest of the participants in a class by setting his/her own profile on Moodle. There are no additional charges for this online identity protection setting.

Student Responsibility

A student enrolled in an online or onsite course through Moodle is expected to follow the University's academic honesty policy. Cheating and plagiarism (using someone else's ideas, writings or materials as one's own without acknowledgement or permission) can result in any one of a variety of sanctions. Such penalties may range from an adjusted grade on the particular exam, paper, project, or assignment to a failing grade in the course. The instructor may also summarily suspend the student from the class when the infraction occurs. For further clarification and information on these issues, please consult with your instructor and the Student Handbook.

Gramm-Leach-Bliley Act

In 1999, Congress enacted the Gramm-Leach-Bliley Act (Public Law 106-102). This Act requires that lenders provide certain information to their customers regarding the collection and use of nonpublic personal information. We disclose nonpublic information to third parties only as necessary to process financial information and as permitted by the Family Educational Rights and Privacy Act of 1974 (FERPA). We do not sell or otherwise make available any information about students, staff, faculty, or any other stakeholder of SSU to any third parties for marketing purposes.

SSU protects the security and confidentiality of personal information in accordance with the *Protection of Consumer Information Under the Gramm Leach Bliley Act*. All physical access to any and all University sites and locations where nonpublic personal information (also referred to as Student Directory Information) is maintained, controlled, and monitored by authorized university personnel. Our computer systems offer a high degree of resistance to tampering and circumvention., thus limiting data access to approved staff and contract staff on a "need-to-know" basis, inclusive of individualized user control protocols which limit individual users' ability to access and/or alter records within the university's information systems. All users of these systems are given a unique user ID with personal identifiers.

General Data Protection Regulation

The GDPR expands the privacy rights granted to European individuals and requires certain companies that process the personal data of European individuals to comply with a new set of regulations. In particular, the GDPR may apply to companies that process the personal data of European individuals and have a presence in the EU (e.g. offices or establishments) and to

companies that do not have any presence in the EU but target the European market (e.g. by offering goods or services to the European market) or monitor the behavior of European individuals. SSU is here to help our students in our collective efforts to comply with the GDPR.

What is GDPR?

In 2016, the European Union (EU) approved a new privacy regulation called the General Data Protection Regulation commonly known as the GDPR. It is a mandatory ruling that applies to all companies that collect the data and information of EU individuals and meet certain territorial requirements. The GDPR is designed to strengthen the security and protection of personal data in the EU, as well as provide businesses with a structured framework on how to collect, process, use, and share personal data. Under the GDPR, the concept of "personal data" is very broad, and covers almost any information relating to a specific individual.

This policy affects the legal rights and obligations of individuals, so please read it carefully. For questions regarding GDPR, contact datainquiries@ssu.edu.

Personal data collected by Southern States University

Southern States University collects and uses personal information and data to operate its website(s) and deliver requested services. Individuals for whom data and other personal information is collected may include, but is not limited to, applicants, students, event attendees, customers, and otherwise unaffiliated individuals who access University websites or in-person events, collectively referred to in this section of the document as "users."

Southern States University may also use personally identifiable information to inform users of other products or services available from Southern States University, including surveys to conduct research about one's opinion of current services or of potential new services that may be offered.

The University collects, processes, stores, and uses personal data when users fill out one or more forms for more information including the user's name, email address, physical address, phone number, and educational and/or employment background. SSU may also collect personal data that is given to us about other users who were concurrently registered on the same form to engage in SSU events and activities. It is the official position of the University that any concurrently registered event attendee is informed by the primary event registrant of this privacy notice and, where necessary, obtained their consent so that the University can lawfully process their personal data in accordance with this policy. When registering as a student with Southern States University additional personal data will be kept including, but not limited to, the student's photograph and copy of government issued photo ID, dates of attendance, academic level, registration and enrollment status (e.g., undergraduate or graduate, full-time or part time), degrees earned, honors and awards received, class rosters within the classroom, and the most recent educational agency or institution attended.

All personal data provided to Southern States University must be true, complete and accurate. If the University is provided with inaccurate or false data, and identify fraud is suspected, such information will be recorded and, as necessary, provided to law enforcement.

Personal data is not required to interact with SSU's public website(s) or social media accounts. However, the University may still collect the information set under the Data we automatically collect section of this policy, and marketing communications in accordance with the Marketing Communications section of this policy. Personal data is required for admitted students in order to interact with the University's interactive student learning platform.

When a user contacts SSU by email, post, phone, or in person, a record of the correspondence may be filed as part of the user's record with the University.

Automatically-collected data

When a user visits our website(s), SSU, or third parties on behalf of the University, automatically collect and store information about the device used and activities engaged in. This information may include (a) computer or other device's SSU ID number; (b) technical information about the used device (e.g. type of device, web browser, or operating system); (c) preferences and settings (e.g. time zone and language); and (d) statistical data about browsing actions and patterns. SSU collects this information using cookies in accordance with the Cookie section of this policy and the University uses this specific collected information on an anonymous basis to improve website experiences, tailor events and services provides, as well as for analytical and research purposes.

The University also allows advertisers and advertising networks to collect information about SSU user's computers or mobile devices, activities, and geographic location to enable them to display targeted ads and provide SSU with anonymous information about our users' behavior. Importantly, this takes place through the use of cookies in accordance with the Cookie section of this policy.

Marketing communications

If a user opts in to receive marketing communications from SSU, the user consents to the processing of the user's data to send such communications, which may include newsletters, blog posts, surveys, and information about new events. SSU retains a record of consent.

Users may choose to no longer receive marketing communications from SSU by contacting us at datainquiries@ssu.edu or clicking unsubscribe from a marketing email. It may take up to 5 business days for new preferences to take effect. It should be noted that personal data for marketing purposes is retained indefinitely until the University is in receipt of a request by the user to be removed from future marketing correspondence.

Lawful processing of personal data

Southern States University will use personal data to comply with our contractual obligation to provide users with accurate information about the University and to ensure proper services for our students and graduates, including to contact users with any information relating to any events users may be attending, and to deal with any questions, comments or complaints made in relation to the University.

Southern States University does not sell, rent, or lease its customer (user) lists to third parties.

Southern States University may share data with trusted partners to help perform statistical analysis, send emails or postal mail, provide customer support, or arrange for deliveries to users. All such third parties are prohibited from using user personal information except to provide these services to Southern States University, and such third-parties are required to maintain the confidentiality of user information.

Southern States University will disclose user personal information, without notice, only if required to do so by law or in the good faith belief that such action is necessary to: (a) conform to the edicts of the law or comply with legal process served on Southern States University or the site; (b) protect and defend the rights or property of Southern States University; and, (c) act under exigent circumstances to protect the personal safety of users of Southern States University, or the public.

Data sharing

SSU may share users' personal data with any service providers, sub-contractors, and agents that may be appointed to perform functions on behalf of the University and in accordance with our instructions, including payment providers, email communication providers, IT service providers, accountants, auditors, and lawyers.

Under certain circumstances we may have to disclose user personal data under applicable laws and/or regulations, or protect a third party's rights, property, or safety.

Personal data storage and processing

Some or all of a user's personal data may be stored or reside outside of the European Union (the EU), including, for example, if the SSU email server is located in a country outside the EU or if any of our service providers or their servers are based outside of the EU. We shall only transfer user personal data to organizations that have provided adeSSUate safeguards in respect of user personal data.

Cookies

WHAT ARE COOKIES

As is common practice with almost all professional websites, the Southern States University website uses cookies, which are tiny files that are downloaded to a user's computer, and to improve the user's experience. Described below is information about the data gathered, how information is used by the University, and why such information may be stored, in addition to how users can prevent these cookies from being stored (which may downgrade or 'break' certain elements of SSU's website functionality).

For more general information on cookies, see the Wikipedia article on HTTP Cookies.

HOW COOKIES ARE USED

SSU use cookies for a variety of reasons detailed below. Unfortunately, in most cases, there are no industry standard options for disabling cookies without completely disabling the functionality and features such cookies add to SSU's website. It is recommended that all cookies are left on (enabled) if the user is not sure whether the cookies are needed (in case they are used to provide a necessary service or website functionality).

DISABLING COOKIES

Users can prevent the setting of cookies by adjusting the settings on their browser. Users should be aware that disabling cookies will affect the functionality of the SSU website and many other websites visited. Therefore, it is recommended that cookies are not disabled.

THE COOKIES SET BY SSU

Forms related cookies

Cookies may be set to remember information submitted through a form, such as those found on contact pages or comment forms, for use toward future correspondence.

Third Party Cookies

In some cases, SSU also uses cookies provided by trusted third parties. The following are examples and details of third-party cookies that may be encountered through SSU's website.

Southern States University uses Google Analytics, which is one of the most widespread and trusted analytics solutions on the web for helping us to understand how individuals use the site and ways that we can improve user experiences. These cookies may track things such as how long users spend on the site and the pages visited so we can continue to produce engaging content.

For more information on Google Analytics cookies, see the official Google Analytics page.

From time to time SSU tests new features and makes subtle changes to the way that the site is delivered. When new features are still being tested, these cookies may be used to ensure that users receive a consistent experience whilst on the site and ensuring that we understand which optimizations our users appreciate the most.

As the University provides courses and degree programs, it is important for us to understand statistics about how many of the visitors to our website follow through to applying to the University as a student; it is this type of data that the cookies we set track. This is important to users as it means that SSU can accurately make business predictions that allow us to monitor our advertising and product costs to ensure the best possible user experience, tuition rates, and event fees.

SSU also uses social media buttons and/or plugins on our website that allow users to connect with their social network in various ways. For these to work, the following social media sites will set cookies through our site, which may be used to enhance user profiles on their sites or contribute to the data they hold for various purposes outlined in their respective privacy policies: Facebook, Instagram, and YouTube.

Security

The University shall process user personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

All information users provide to us is stored on our secure servers. Any payment transactions are encrypted using SSL technology.

Where a password has been provided by the University or chosen by the user, the user is responsible for keeping this password confidential.

However, it should be acknowledged that no system can be completely secure. Therefore, although Southern States University takes these steps to secure personal data, SSU does not promise that user personal data will always remain completely secure.

User rights

Users have the right to obtain a copy of the personal data that we store on the user, and to require SSU to correct errors in the personal data if it is inaccurate or incomplete. Users also have the right to require that we delete your personal data at any time. To exercise these rights, or any other rights the user may have under applicable laws, please contact us at datainquiries@ssu.edu

Please note, SSU reserves the right to charge an administrative fee if a user's request is manifestly unfounded or excessive.

Retention

If a user fills out a form on our website(s), SSU shall retain the user's personal data until said user closes their account or asks to be removed from our system. Registered students are encouraged to review the FERPA data retention policy regarding official academic records.

If users receive marketing communications from us, SSU shall retain user personal data until a request to opt out of receiving such communications has been received from the user.

More information on GDPR

If any provision of this policy is held by a court of competent jurisdiction to be invalid or unenforceable, then such provision shall be construed, as nearly as possible, to reflect the intentions of the parties and all other provisions shall remain in full force and effect.

Southern States University reserves the right to change the terms of this policy as deemed necessary. Users are responsible for regularly reviewing this policy to remain aware of any changes herein. If any user continues to use our website(s) after the time we state the changes will take effect, it is assumed that users will accept the policy changes.

Policies and Procedures for Safeguarding Information

As mandated by the Federal Trade Commission's Safeguards Rule and the Gramm-Leach-Bliley Act (GLBA) SSU intends to ensure the security and confidentiality of covered records~~,~~ protect against any anticipated threats or hazards to the security of records with PII, and protect against the unauthorized access or use of records or information in ways that could result in substantial harm or inconvenience to students and other University systems users, including prospective students, current students, former students, alumni, staff, faculty, and contractors. These

practices impact departments including but not limited to the financial aid, financial services, registrar, students' services, and the library.

To protect SSU information and personally identifiable information (PII), the following policies and procedures have been established that relate to access, storage, protection, carriage, and destruction of records, computer system safeguards, and training.

- Only SSU employees, or authorized agents, are granted access to any physical or electronic files.
- Computer access passwords are to be kept confidential and disabled prior to termination of employment.
- Upon termination of employment, the employee's access to their computer workstation, student records, and school documents are immediately barred.
- The student information system, student learning platform, and all computers are backup safely.
- Electronic records containing PII are stored on secure, encrypted servers, and, when stored on authorized desktop computers, are to be password protected.
- Paper records containing PII are kept in fireproof locked cabinets in a secure area when not in use. The University Registrar is the custodian of records and is responsible for all official student files.
- SSU employees cannot touch, access, or remove any record from the premises without consent. When it is necessary to remove records containing PII to an off-campus location, employees must safeguard the information. Under no circumstances are documents, electronic devices, or digital media containing PII to be left unattended in any unsecure location.
- When there is a legitimate need to provide records containing PII to a third party, electronic records are password-protected, and paper records are securely sealed.
- Destruction of paper and electronic records must be approved in accordance with the SSU's records procedures, or other applicable federal, state and local regulations.
- The Director of Administration monitors the information safeguards on an ongoing basis to control when improvements are required. In order to avoid external risk and secure the network and the data that contain PII, SSU has implemented the following:
    - Secure user authentication protocols
        - Unique strong passwords are required for all user accounts; each employee receives an individual user account
        - Computer workstation passwords are required
        - Server accounts are locked after 3 successive failed password attempts
        - User passwords are stored in an encrypted format; root passwords are only accessible by system administrators.
    - Secure access control measures
        - Access to specific files or databases containing PII is limited to those employees who require such access in the normal course of their duties.
        - Each employee has been assigned a unique password, different from the employee's password to the computer network, to obtain access to any file or database that contains PII needed by the employee in the course of his or her duties.
        - Files containing PII transmitted outside of the SSU network are encrypted.

- The Director of Information Technology performs regular internal network security audits, and reviews SSU's computer systems to prevent possible electronic security breaks.
- Operating system receive regular security updates.
- Antivirus software is installed and kept updated on all servers and workstations. Virus updates are installed on a regular basis, and the entire system is tested periodically.

All SSU employees receive an initial training for guidance, access, and managing the student information system, students record management, and confidentially. All SSU employees are required to pass a FERPA training and adhere to FERPA policies.

Policy and Procedural Review

Southern States University will review the Program at least annually and will change, modify, or otherwise alter this program deemed necessary. This review will be conducted by the Director of Administration, the Registrar, Compliance Officer, and Information Technology Manager.