Information Security Plan

December 2022

Table of Contents

Information Security Plan

The following Information Security Plan describes Sullivan University's safeguards to protect data, information, and resources. These safeguards:

- Make reasonable efforts to ensure the security and confidentiality of covered data, information, and resources
- Protect against anticipated threats to the security or integrity of covered data, information, and resources
- Protect against unauthorized access or use of covered data, information, and resources that could result in substantial harm or inconvenience to any customer

This Information Security Plan also provides mechanisms to:

- Identify and assess the risks that may threaten the covered data, information, and resources maintained by the University
- Manage and control risks
- Implement and review the plan
- Modify the plan to reflect changes in technology, the sensitivity of covered data, information and resources, and internal or external threats to information security

Identification and Assessment of Risks to Customer Information

The University recognizes that it has both internal and external risks. These risks include, but are not limited to:

- Unauthorized access of institutional data, information, and resources by someone other than the owner of the institutional data, information, and resources
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access or distribution of institutional data, information, and resources by employees, students, affiliates, or other constituencies
- Unauthorized requests for institutional data, information, and resources
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of institutional data, information, and resources through third parties

The University continuously monitors industry trends and attempts to take reasonable measures to identify and mitigate new and emerging threats. Due to the constantly evolving threat landscape, the University cannot guarantee that all risks will be identified and that the security of the institutional data is without flaw.

Data Classification

Class	Description
Institutional	Data that is classified as either restricted or private (described below)
Restricted	Data protected by state and federal privacy regulations and confidentiality agreements (requires most restrictive security controls)
Private	Any institutional data that is not considered restricted or public (e.g. business secrets, business intellectual property)
Public	Data which unauthorized disclosure, alteration, or destruction would pose little to no risk to the institution or its affiliates

Information Security Plan Coordinators

The Senior Director for IT is the coordinator of this plan with significant input from the Information Security Steering Committee comprising of several leaders and experts in their respective areas. This committee is responsible for assessing the risks associated with unauthorized transfers of covered data, information, and resources. They are also responsible for implementing procedures to minimize those risks to the University and/or conducting audits of this plan on a periodic basis.

Design and Implementation of Safeguards

Employee Management and Training

References of new employees working in areas that regularly work with covered data, information, and resources (e.g., Information Technology Services, Office of Bursar, and Admissions) are checked by the hiring supervisor prior to extending an offer of employment. Additionally, criminal background checks are conducted on all employees of the University hired after April 1, 2012. Other checks could include identity verification, education verification, moving violation record, NSLDS status, and professional licenses.

Upon hire, each new employee will receive proper training on the importance of confidentiality of student records, student financial information, and other types of covered data, information, and resources as covered under the Family Educational Rights and Privacy Act (FERPA). Each new employee is also trained in the proper use of computer information and passwords, network security, inherent risks of online activity, protecting personal devices, and safe online behavior.

All training is administered by the human resources department through the institution's online learning platform for employees. Employees are required to repeat the training every two years. All employees are required to review and sign the Statement of Understanding for the Faculty/Staff Manual, which contains the institution's policies concerning private student information and use of computing technology and networks. All employees are also required to sign and adhere to the Code of Conduct in support of their intent to maintain ethical behavior and best practices concerning, among other things, the handling of confidential information.

Each department responsible for maintaining covered data, information, and resources is instructed to take steps to protect the information from destruction, loss, or damage due to environmental hazards, such as fire and water damage or technical failures.

Physical Security

The University has addressed physical security by placing access restrictions to buildings, offices, and records storage facilities containing covered data, information, and resources to permit access only to authorized individuals. These locations are to be locked, and only authorized employees are permitted to possess keys or combinations to them. Paper documents that contain sensitive data are to be shredded at the time of disposal.

Information Systems

Access to institutional data, information, and resources via the University's IT Infrastructure is limited to those employees who have a business reason to access such information. Each employee is assigned a set of unique credentials. Databases containing institutional data, information, and resources including, but not limited to, accounts, balances, and transactional information are available only to University employees in appropriate departments and positions.

The University will take reasonable and appropriate steps consistent with current technological standards to make sure that all institutional data, information, and resources are secure and to safeguard the integrity of records in storage and transmission. All University hosted servers and applications are required to be patched and updated on a regular basis that is consistent with the manufacturer's recommendations. All systems are behind a firewall and encryption technology is used when it's reasonable to do so. A managed detection and response (MDR) system provides real time monitoring and threat detection. Automated mitigation steps are taken by the MDR system within 15 minutes if a threat is detected.

Management of System Failures and Compromises

The University has developed written plans and procedures to detect actual or attempted attacks on University systems and has Incidence Response plans in place which outline the procedures for responding to an actual or attempted unauthorized access to covered data, information, and resources. Incidence Response and Reporting procedures are detailed later in this document.

Selection of Appropriate Service Providers

Due to the specialized expertise needed to design, implement, and service new technologies, external resources may be needed to provide services the University determines it will not provide on its own. In the process of choosing a service provider that will maintain or regularly access covered data, information, and resources, the evaluation process shall include the ability of the service provider to safeguard confidential financial information. Contracts with service providers may include the following provisions:

- An explicit acknowledgement that the contract allows the contract partner access to confidential information
- A specific definition or description of the confidential information being provided
- A stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract
- An assurance from the contract partner that the partner will protect the confidential information it receives according to commercially acceptable standards and no less rigorously than it protects its own confidential information

- A provision providing for the return or destruction of all confidential information received by the contract provider upon completion or termination of the contract
- An agreement that any violation of the contract's confidentiality conditions may constitute a material breach of the contract and entitles the University to terminate the contract without penalty
- A provision ensuring that the contract's confidentiality requirements shall survive any termination agreement

Information Technology Services Unit - General Security Considerations

Computer Lab

- Computer labs are provided for use by Sullivan University students, faculty, and staff. All lab computers require authentication for access. The institution has the right to deny access to the labs to anyone without proper identification.
- Guests are allowed to use computer labs on an as needed basis. Guest accounts are requested by the department hosting the guest and are provided by the IT helpdesk staff. Guest accounts are enabled only for the duration of the approved guest visit and are password protected.
- Lab machines are prohibited from engaging in port scanning, traffic spamming/flooding, and other similar activities that negatively impact the University network and/or non-University networks. In the event that these activities are required for course work, these activities may only be leveraged against environments that were explicitly designed with the intention of being targeted by such activities for the purposes of academic learning & instruction, or if arranged otherwise by the instructor and approved by the department Dean.
- Network equipment such as hubs, switches, routers, and wireless access points may not be placed in University labs without written authorization from the Sullivan University IT Department

Anti-Virus

- All University controlled computers must have the institution’s standard anti-virus software installed and kept up to date.
- Computers identified as possibly being compromised will be removed from the network until they can be verified as virus-free by a member of the IT staff.
- Any activities with the intention to create and/or distribute malicious programs into Sullivan University's networks (e.g., viruses, worms, Trojan horses, etc.) are prohibited.

Network Control and Access

1. Anyone who uses the campus computing environment must be properly authorized.

2. Users must not:

- Perform acts that negatively impact the operation of computers, peripherals, or networks or that impede the ability of someone else to do his/her work
- Attempt to circumvent protection schemes for access to data or systems

- Gain or grant unauthorized access to computers, devices, software, or data

3. Users may be held legally and financially responsible for incidents resulting from unauthorized use of University network and system accounts.

4. Sullivan University has installed various network security devices, including account passwords and firewalls, to help ensure the safety and security of University information. Any attempt to disable, defeat, or circumvent any security facility is considered inappropriate activity and is a violation of this network policy.

5. Expansion or manipulation of network hardware and/or software, except by designated individuals within the IT Department, without prior approval from the IT Department, is strictly prohibited.

6. Prior to connecting any server to the University network, approval must be obtained in writing from the Sullivan University IT Department.

7. Attachment of any of the following devices to the campus network, other than those provided or approved by the IT Department, is strictly prohibited:

- DHCP servers
- DNS servers
- NAT routers
- Packet capturing technology
- Any device that disrupts or negatively impacts network operations

8. Static assignment of IP addresses not approved and obtained through the IT Department is not permitted.

9. Only IT Department staff or authorized agents may move University-owned networking and communications equipment.

10. The owners of data stored on network accessible systems are responsible for managing and determining the appropriateness of information stored on these systems. This includes both private storage areas and “shared” folder areas.

11. Only authorized merchants may use University networks, wired or wireless, to accept credit card payments. Merchants must notify and receive approval from the IT Department before using Sullivan University networks to accept payments and must comply with current Payment Card Industry Data Security Standards (PCI DSS).

12. DHCP and DNS Services – the IT Department provides centralized and redundant DHCP and DNS services for the University. Due to the nature of these services, and because of the potential disruption of service and possible security breaches resulting from incorrect setup of additional systems, attachment of unauthorized DHCP or DNS servers is prohibited. The following guidelines must be followed when requesting or using any DHCP or DNS services

DHCP Guidelines

- By default, systems requiring an IP address must support DHCP and be capable of obtaining DHCP address information from one of the centrally administered University DHCP servers.
- Using DHCP, devices requesting an IP address will be assigned a dynamic pool address from the subnet to which the device is attached. Devices with dynamically assigned IP addresses may have their address changed.
- Reserved IP addresses needed for devices functioning as servers must be requested from the IT Department. Once assigned, the IP address must be obtained by the machine via DHCP. The MAC address for any reserved IP address must be provided prior to assignment.
- Static IP addresses to be hard coded for specialized equipment incapable of using DHCP may be requested from the IT Department. The MAC address for any statically assigned IP address must be provided prior to assignment.
- The IT Department must be informed of any changes to equipment utilizing reserved or static IP addresses.

DNS Guidelines

- Any domain that is to be associated with Sullivan University's network must be registered with the IT Department.
- Requests for assignment of DNS names must be for valid University purposes.
- DNS names ending in suscorp.edu or sullivan.edu are made available upon request at no charge for University approved services.
- DNS names for domains other than suscorp.edu or sullivan.edu and which are to be hosted on University systems, must be requested from the IT Department. Any charges for initial or ongoing registration of the requested name are the responsibility of the requestor.
- The IT Department will work with any user requesting a domain name to identify an appropriate and available name; however, the IT Department has final approval for all DNS name assignments.
- DNS names, not in the suscorp.edu or sullivan.edu domain, will not be approved for use without justification. For any other domain name to be approved for use, it must be demonstrated that equivalent functionality cannot be provided under the existing suscorp.edu or sullivan.edu domain.

Vendor/Merchant Access

Only authorized vendors/merchants will have access to University systems. The following rules apply to vendors/merchants requesting access to University IT resources:

- Vendor accounts should have a passphrase with a minimum of 16 characters.
- Vendors must provide technical reasoning for their need to access Sullivan University IT resources.
- If multiple employees of the vendor will be accessing Sullivan University IT resources, each employee should have his/her own vendor account.
- Vendors must provide an estimated duration of time that they need to access Sullivan University IT resources. The account will be configured to expire after this time period has elapsed.

- In the event the duration the vendor needs to access Sullivan University IT resources is indefinite/perpetual, the vendor account should be set to expire at a maximum of every 6 months – at which point the vendor will need to request from IT that the account be reinstated.

End-User Devices (Workstations, Laptops, Tablets, Mobile Devices, etc.)

- Administrative employees who are approved to use personally owned devices for institutional purposes are responsible for the security and integrity of any data stored on their device.
- Storage of sensitive or personal institutional data is prohibited on mobile devices.
- Employees accessing IT services and systems with their own personal device must adhere to all IT policies.
- Anti-virus software and security related operating system patches must be installed on all workstations that connect to the University network.
- For personal devices used for educational purposes see the Bring Your Own Device Acceptable Use Policy.

Security Assessment

- Network and system security audits will be conducted by a third party on an annual basis.
- Reasonable efforts will be made to minimize or eliminate any security related issues.

Software Licenses

- Placing unlicensed or illegally obtained software or media on University computers is strictly prohibited.
- Software must be used in accordance with the terms of the license agreement between the institution and software vendor.
- All software must be approved for use on the institutional network by the IT department.

Servers

- Administrative access to servers must be limited to just those users with a legitimate need for that level of access.
- Servers should be physically located in an access-controlled environment.
- All servers deployed at Sullivan University must be approved by the IT department. Server maintenance plans must be established and approved by the IT department.
- Appropriate efforts should be made to lessen the attack surface by limiting services and applications to just those required. Reasonable effort should be made to keep anti-virus, application, and operating system patches and updates current.
- Privileged access must be performed via an encrypted network protocol.
- Security-related events will be reported to the IT Department, who will review logs and prescribe corrective measures as needed. Security-related events include, but are not limited to:

    - Port-scanning or Distributed Denial of Service attacks
    - Evidence of unauthorized access to privileged accounts
    - Evidence of access to information by an unauthorized viewer
    - Anomalous occurrences that are not related to specific applications on the host

- Audits may be performed on any device utilizing Sullivan University Network resources at the discretion of the IT Department

Passphrases/Passwords

- Passphrases are implemented to control access to information and systems. Users are responsible for protecting their passphrases as well as any other authentication mechanisms such as PIN numbers etc.
- Passphrases should be a minimum of 16 characters in length and include alpha and numeric characters.
- Passphrases will be set to automatically expire every 365 days at a minimum. Users will be required to change any passphrase identified by the IT department as compromised immediately.
- Passphrases should be memorized whenever possible. Any stored passwords must be strongly encrypted.
- Passphrases should only be stored in browser caches or other auto complete types of features on single use corporate owned devices.
- Passwords should only be inserted into emails that are using strong encryption.
- Do not use the same passphrase for Sullivan University accounts as other non-Sullivan University access.
- Sullivan University accounts of passphrases should not be shared with anyone and should be treated as sensitive, confidential information.
- Passphrase "lockout" features should be enabled on any systems where it is available and reasonable to implement. Users will be locked out of systems after 10 unsuccessful attempts in 30 minutes and will auto-unlock after 30 minutes from the 10th login failure.

Physical Access

- Access should only be granted to any person with proper authorization to access the corresponding area.
- Unauthorized access to areas where personally identifiable information is stored is prohibited.
- Supervisors must ensure that staff who (voluntarily) terminate their employment with the department return their physical access keys and cards on their last day of work in that unit.
- Employees who are (involuntarily) dismissed from the institution must return their keys and other access control devices/cards at the time they are notified of their dismissal. Any access granted to access control devices/cards must be removed immediately.
- If an employee does not return his/her keys, areas controlled by the outstanding keys must be rekeyed.
- University information or records may not be removed (or copied) from the office where it is kept except in performance of job responsibilities.
- Access to IT Infrastructure operations areas shall be restricted to those responsible for operation and maintenance. Non-IT personnel are not permitted unless they are escorted by an authorized IT staff member.
- Key access is granted on an individual basis and in no case should be lent or given to others.
- Some units leverage key cabinets to allow the physical keys to be a shared resource but under auditable conditions.

- Computer installations should provide reasonable security measures to protect the computer system against natural disasters, accidents, loss or fluctuation of electrical power, and sabotage.
- Adequate disaster recovery plans and procedures are required for critical systems data.

Physical Assets

- Networking and computing hardware should be placed in a secure environment and space shall be dedicated to the functions whenever possible.
- Employees must know where the fire suppression equipment is located and how to use it.
- Materials should not be stored on top of or directly next to equipment; proper airflow and environmental conditions must be maintained.

Wireless Access

- This policy strictly prohibits access to institutional data or Sullivan University systems via open, unsecured wireless communication mechanisms (an exception is the “Sullivan University-Guest” wireless network which is provided by the University IT Department for the convenience of visiting constituencies). This guest network will have restricted access to non-confidential resources.
- Wireless access points not sanctioned by the Sullivan University IT Department are prohibited.

Destruction and Disposal of Information and Devices

- Confidential information must be disposed of in such manner as to ensure it cannot be retrieved and recovered by unauthorized persons. Physical documents must be shredded.
- When donating, selling, transferring, sending to surplus, or disposing of computers or removable media, care must be taken to ensure that confidential data is rendered unreadable. Any restricted information that is stored must be thoroughly destroyed. In general, it is insufficient to "delete" the information, as it may remain on the medium. The data should be properly removed from the drive either by software that meets U.S. Department of Defense specifications or the drive may be physically or destroyed.
- Standardize utilization of Bluegrass Recycle or other vendor that will pick up storage media or other electronic devices and provide a certificate of secure destruction for any data-holding hardware. Scheduled pickups should be coordinated through campus support and the related parties.

Sensitive Data Protection

Special care and awareness are required with regard to “sensitive data.” Sensitive data are any data that the unwarranted and/or unauthorized disclosure of such would have an adverse effect on the institution or individuals to which it pertains. Unauthorized disclosure or mishandling of sensitive data can be a violation of federal and state law and the institution and its employees can be held personally liable for damages or remediation costs.

Data related to identity theft such as social security number (SSN), credit card numbers, bank account information, driver’s license, name, address, birthdate, passwords, Personal Identification Numbers (PINs), and ID pictures are of particular concern as all or most of this information is collected in the course of University business. Other types of data such as medical information, tax returns, scholarship information, and financial information are examples

of data that could require confidential handling or restricted access. These examples are not exhaustive or all inclusive. It is the responsibility of University employees handling any University data to understand what data are sensitive and confidential and to adhere to the following guidelines and any applicable regulations.

1. Do not collect and/or store SSN/DOB unless it is required by a federal or state agency and there is no other option in terms of unique identifier. Access to SSN/DOB data must be pre-approved by the department supervisor through the submission of a request form with appropriate explanation of needed access. The request will be added to a workflow for review and approval.

2. Use the Sullivan University ID (SUID) assigned to all students as the unique identifier for all entities. If SUID is not available or does not exist for certain populations, such as camps or events, use a non-SSN type of ID.

3. Data should be stored in as few places as possible and duplicated only when necessary. Unless absolutely necessary, data should be stored on central administrative systems only.

4. Avoid storing data on departmental servers or creating databases that duplicate data on central administrative systems.

5. Never upload, post, or otherwise make available any kind of sensitive data on a web server even for short periods of time. Individuals responsible for maintaining web site content must be particularly cognizant and vigilant regarding this matter.

6. Inventory and identify the data under your control that is external to central administrative systems. Know where you have data and in what form (electronic, paper, etc.). Purge or delete data files in a timely manner to minimize risk.

7. Do not store sensitive data on or copy it to mobile, external, and/or removable storage devices. This may include smartphones, tablets, or any other device that could easily be lost, stolen or compromised.

8. Do not store sensitive data on or copy it to local workstations or network drives unless such data is not available on centralized systems. If you must store data on workstations or network drives, it is your responsibility to secure your workstation and/or ensure that only authorized individuals have access.

9. Do not use shared network drives to share or exchange data unless you are certain that access to those shared drive resources is restricted to individuals authorized to handle such data.

10. Know and understand your environment technically. Understand who has access to areas to which you send, receive, store, or transmit data.

11. Transmission of any sensitive data should be encrypted. Websites should use HTTPS (TLS 1.2 or greater) encryption if they collect data. Unencrypted protocols should be abandoned in favor of their encrypted counterparts (i.e. abandon FTP in favor of SFTP). When in doubt, contact the IT Help Desk.

12. Do not release Sullivan University data of any kind to 3rd party, non-Sullivan entities for any reason, unless such entities have agreed in writing to restrict the use of such data to the specific and intended purposes authorized by the University department enlisting the services of the 3rd party entity. Any University department releasing data to a non-Sullivan 3rd party entity is responsible for how the data are used (misused). Release of highly sensitive and confidential data (beyond FERPA allowed "directory information") is prohibited.

13. Do not send, receive, or store any sensitive data using email under any circumstances. Email is not secure.

14. Under no circumstances should credit card numbers be collected and stored on standalone devices, digital media, or paper media. Processing credit card numbers should be done via secure methods that authorize or deny the transaction in real time but do not retain or store the credit card number. Collecting credit card numbers via phone calls, websites, or email and retaining such numbers on paper or in electronic files for periodic processing is bad practice and insecure. All merchants accepting credit card payments on campus must comply with Payment Card Industry Data Security Standards (PCI DSS).

15. Report any breaches, compromises, or unauthorized/unexplained access of sensitive data immediately to the Senior Vice President for IT or directly to your supervisor.

Privacy Policy – Student Records

The confidentiality, use, and release of student records are governed by the Family Educational Rights and Privacy Act (FERPA). University employees' utilization of this information depends on the nature of their duties and responsibilities. In general, all student information must be treated as confidential. Even public or directory information is subject to restriction on an individual basis. Unless an employee's job involves release of information and they have been trained in that function, any requests for disclosure of information, especially outside the University should be referred to the Registrar's Office.

Other than directory information, no other information about a student may be released without the written consent of the student. Items such as grades, test scores, social security numbers, gender, ethnic background, and class schedules may never be released to anyone other than the student. This includes parents or guardians. In no case should a student's information be released by phone.

Faculty are provided specific instructions related to maintaining the privacy of student records. They are instructed to not:

- Use the social security/student ID number of a student in a public posting of grades
- Link the name of a student with his/her social security number in any public manner
- Leave graded tests in a stack for students to pick up by sorting through the papers of all students
- Circulate a printed class list with student name and social security number or grades as an attendance roster
- Discuss the progress of any student with anyone other than that student without the consent of the student
- Provide anyone with lists of students enrolled in your classes for any commercial purpose

- Provide anyone with student schedules or assist anyone other than University employees in finding a student on campus

Students are assigned a unique Sullivan University ID that is used and referenced for all personal, academic, and administrative information.

A student's record may be released in compliance with a court order or subpoena. The University will make a reasonable attempt to notify the student in advance of compliance unless special circumstances exist in which such notification interferes with the purpose of the request.

Student information may be released for health and emergency reasons.

Family Educational Rights and Privacy Act (FERPA)

Sullivan University is committed to the privacy and security of student records. The University complies with the Family Educational Rights and Privacy Act (FERPA), as amended, that protects the privacy of student education records. FERPA is a federal law that provides guidelines for maintaining the confidentiality of education records and monitoring the release of information from those records.

Within the Sullivan University community, only those members, individually or collectively, acting in the student's educational interests are allowed access to student educational records. These members include personnel in the Student Services Department, Accounting, Financial Planning, Admissions, Deans, Directors, Vice-Presidents, and academic personnel within the limitations of their need to know. Faculty members may also have access to records if/when a need-to-know situation arises.

At its discretion, Sullivan University may provide directory information in accordance with the provisions of the Act to include: student name, address, telephone number, date and place of birth, major field of study, dates of attendance, degrees and awards received, the most recent previous educational agency or institution attended by the student, participation in officially recognized activities and sports, and weight and height of members of athletic teams. Students may withhold Directory information by notifying the Academic Services office in writing within two weeks after the first day of class each quarter.

Student Inspection of Records

Requests for nondisclosure and authorization to withhold Directory Information must be filed annually in the Academic Services Office.

The law provides students with the right to inspect and review information contained in their educational records, to challenge the contents of their education records, to have a hearing if the outcome of the challenge is unsatisfactory, and to submit explanatory statements for inclusion in their files if the decisions of the hearing are unacceptable.

The right to inspect or receive information regarding students does not extend to parents or others not specified above unless the student has given written permission.

The Academic Services/Registrar's Office at Sullivan University has been designated by the Institution to coordinate the inspection and review procedures for student education records, which include admissions, personal, academic and financial files, cooperative education and job placement records.

Students wishing to review their education records must make written requests to the Registrar Office listing the item or items of interest. Only records covered by the Act will be made available within five days of the request. Students may have copies made of their records with certain exceptions (e.g., a copy of the academic record for which a financial "hold" exists, or a transcript of an original or source document, which exists elsewhere.) These copies would be made at the student's expense at prevailing rates that are listed in the current catalog. Education records do not include records of instructional, administrative, and education personnel that are in the sole possession of the maker and are not accessible or revealed to any individual except a temporary substitute, records of the law enforcement unit, student health records, job employment records or alumni records. Health records, however, may be reviewed by a physician of the student's choosing.

Accuracy of Records

Students who believe that their education records contain information that is inaccurate or misleading or is otherwise in violation of their privacy or other rights, may discuss their problems informally with the University's Registrar. If the decisions are in agreement with the student's requests, the appropriate records will be amended. If not, the student will be notified within a reasonable period of time that the records will not be amended; they will be informed by the Registrar of their right to a formal hearing.

The educational records will be corrected or amended in accordance with the decisions of the hearing panel, if the decision is in favor of the student. If the decision is unsatisfactory to the student, the student may place with the education records, a statement commenting on the information in the records, or statements setting forth any reasons for disagreeing with the decisions of the hearings panel. The statement will be placed in the education records, maintained as part of the student's records, and released whenever the records in question are disclosed.

Students who believe that the adjudications of their challenges were unfair or not in keeping with the provisions of the Act may request, in writing, assistance from the President of the Institution. Students should know that complaints regarding potential violations may be lodged with the Family Policy Compliance Office, US Department of Education, 400 Maryland Avenue, SW, Washington, DC 20202-5920.

Revisions and clarifications will be published as experience with the law and Institutional policy warrants.

The FERPA policy is available in the University catalog.

Health and Safety Exemption Requirement

The school only discloses personally identifiable information from an education record to appropriate parties in connection with an emergency if knowledge of the information is necessary to protect the health and safety of the student or other individuals.

Incident Reporting

Sullivan University employees must immediately report the following to their managers, unless a conflict exists with the manager, and the IT Department:

- Any actual or suspected security incident that involves unauthorized access to electronic systems owned or operated by Sullivan University
- Malicious alteration or destruction of data, information, or communications
- Unauthorized interception or monitoring of communications
- Any deliberate and unauthorized destruction or damage of IT resources

- Unauthorized disclosure or modification of electronic institutional or personal information

Incidents will be treated as confidential unless there is a need to release specific information

Incident Response

The IT Department is the primary point of contact for responding to and investigating incidents related to misuse or abuse of Sullivan University Information Technology resources. This includes computer and network security breaches and unauthorized disclosure or modification of electronic institutional or personal data.

Upon discovery of a security breach, provide initial notification of the breach to:

1. The IT Department

2. The affected system's owner (administrative responsibility for the system)

3. The System Administrator (technical support responsibility for the system)

4. Other individuals as required by the circumstances

a. This group will comprise the Incident Response Team for a specific incident. After initial notification, they will provide information updates as appropriate throughout the incident response process.

b. Communications with the media and public should be restricted to University Communication Department. University employees involved in the incident or the incident's response and investigation should refer all media and other public inquiries to the University Creative Communications Department.

c. Create a log of all actions taken and maintain this log consistently throughout the response process.

d. Secure the affected area(s). Electronic evidence can be easily destroyed, resulting in the inability to determine if confidential information has been compromised or to provide evidence for future prosecution. Identify potential evidence, both conventional (physical) and electronic, and determine if perishable evidence exists. For example, do not alter the condition of any electronic device by either turning it on, off, or rebooting it until it is determined that it is safe to do so. Inventory and evaluate the scene.

e. Assess the need for forensic information, such as that gathered from packet traces and system monitoring utilities, which can aid in understanding the nature and scope of the incident and provide evidence for any potential criminal investigation. During this process, consider both the potential value of forensic information vs. the immediate need to protect and restore University resources and services. Document the decision process.

f. Collect and save any forensic information identified in the previous two steps. This may include video records, access logs, system logs, network traces, IP addresses, MAC addresses, data backups, system images, or affected computer hardware.

g. Regain control of the compromised system. This may include network disconnection, process termination, system shutdown, or other action as indicated to prevent further compromise of protected information.

h. Analyze the intrusion. Document the nature of the intrusion and its impact on information and process integrity. Determine if unauthorized individuals may have acquired restricted information. Attempt to determine the identity of those whose data may have been acquired. Estimate the potential cost (in time, money, and resources) of the intrusion to the University.

i. Correct any identifiable system or application vulnerabilities that allowed the intrusion to occur.

j. Verify system and data integrity.

k. Restore service once the integrity of the system and/or information has been verified.

l. The incident response team shall create an incident report with all relevant information. The report should include:

- Date and time the incident occurred
- Description of incident
- Detailed list of system(s) and data which were compromised
- Identifiable risks to other systems or information
- Corrective actions taken to prevent future occurrences
- Estimated costs of incident and any corrective actions
- Identity of those responsible for the incident (if available)

The Director of Information Technology and University Counsel, with input from the Incident Response Team and other appropriate individuals, shall determine if disciplinary action should be taken, criminal charges filed against those involved, and which individuals should be notified.

Sullivan University will act in accordance with the Kentucky data breach notification law, KRS 365.732.

University Department Procedures

Academic Services Office

The Academic Services Office maintains files both in paper and electronic format. These files are accessed regularly by staff who are trained in the Family Educational Rights and Privacy Act and by the standards set forth by the Office of the Registrar.

Electronic records are maintained in the CampusNexus Student Information System and Perceptive Content file database. Access to both systems require credential login via the virtual desktop or via a University provided staff ID and password. Permissions to view, access, edit, and maintain documents are specific to each individual staff group. Requests to edit, access, and view are vetted by the Executive Director of Academic Operations & Institutional Effectiveness in collaboration with Application Support or upon hiring. Significant training is provided to new hires who access these databases. Paper records, with the exception of Official transcripts, added to the electronic databases are shredded following validation and upload of applicable documents to student records in secured storage bins located within the Academic Services Office. Official transcripts are routed to the Office of the Registrar for storage.

Academic Services staff access student records via the Blackboard Learning Management System. Access to the system requires a University provided ID and password. Academic Services does not store student related documents within the Learning Management System, but access to grades or work may be required upon request by appropriate parties.

Paper records are maintained by the Office of the Registrar. Requests to view or access these documents are vetted by their office. A small number of staff have access to the previously utilized Student Information System AS400 in order to build student records within the current database. System access requires a University provided ID and password and are applicable to staff level permission groups.

Miscellaneous paperwork such as deferments, unofficial transcripts for planning purposes, degree progress audits, and other like documents are shredded in secured storage bins after use. Outside of normal business hours, offices are locked for security.

Career Services and Alumni Affairs

The Career Services (CS) and Alumni Affairs (AA) departments assist graduates in their employment search, track employment as it relates to a graduate's education and celebrate alumni accomplishments. To do this, the department tracks employment information, including, job title, employer, salary, employment start date, along with other general information. This information is maintained in the Sullivan University student information system, CampusNexus, as well as in files within the departments. Additional personal information may be included in graduate resumes stored within the University's electronic filing system. Hard copy information is maintained in filing cabinets within CS/AA offices which are locked during non-business hours. Access to this personalized employment information is only provided to authorized employees within the departments. Employment information is also supplied to a third-party employment verification entity that maintains the highest standards of privacy and confidentiality.

Office of Admissions

The Office of Admissions obtains and collects a variety of different information for prospective students through a variety of stages and in different formats.

The types of data that are collected include, but are not limited to:

1. Prospect Stage:
   - Purchased information of high school graduates
   - Standardized test results from prospective students

2. Inquiry Stage:
   • General inquiries from prospective students through either inquiry card or web form
3. Applicant Stage:
   • Applications from prospective students
   • Advanced placement examination information
   • Standardized test results for prospective students
   • Immigration documentation of prospective international students
   • High school and college transcripts of prospective students
4. Admission Stage:
   • Applications from re-entry and continuing students

All student records that are stored within the Office of Admissions are covered under the Family Educational Rights and Privacy Act of 1974 (FERPA) and those guidelines establish release of student information. In addition to FERPA regulations, the Office of Admissions has the following policies and procedures in practice to protect information:

1. Electronic data - All electronic data is held in at least one of three places.

   - Velocify, the University's Customer Relationship Management software
   - CampusNexus, the University's Student Information System
   - Perceptive Content, the University's electronic document storage software

   Only certain authorized staff members can view or edit certain personal information such as a social security number or date of birth. All three systems are password protected and secured.

2. Hard copy – Any hard copy documents are immediately scanned into Perceptive Content and then shredded. The only hard copy information that is kept in the Office of Admissions are inquiry cards that are shredded at the end of each year. These are always kept in a locked file cabinet until they are shredded. All personnel are required to read and abide by office procedures on student record information including FERPA regulations. Training agendas include a component on information security. For additional information call the Office of Admissions at 502-456-6504.

Office of the Bursar

The Office of the Bursar maintains financial records for the Cashiers, Billings and Receivables functions of the University. These records include both electronic and paper records. The Bursar's Office is in a secure, locked environment with video surveillance and an intrusion detection system. Electronic records are maintained through the University's student information system. Prior to receiving access to the system, each employee is required to sign an agreement to comply with federal law and University policy regarding the protection of and correct use of information related to students and records privacy. Paper records are maintained in filing cabinets. Third party/company pay records are maintained in filing cabinets within the secure area of the Bursar's Office. The University receives credit card information for payment of tuition and fees and uses Heartland for credit card processing. The hard copy information is maintained in a locked storage room at the Nolan building and regulated by the accounting department. It is then shredded after a specified retention period. When a student pays with a

credit card via our secured website, the credit card number is masked on the secured system maintained by the IT department. Additional safeguards include:

- Records are disposed of after the designated period of retention via shredding.
- Computers are password protected.

For additional information, call the Office of the Bursar at (502) 213-8310.

Office of the Registrar

The Office of the Registrar (OTR) is the custodian of Sullivan University's academic student records. The records are stored in an electronic and paper format. The OTR adheres to the Family Educational Rights and Privacy Act (FERPA) in order to protect the privacy of student records and as guidance regarding the release of student information. All requests for student information, external and internal are reviewed and approved by the University Registrar in accordance with FERPA.

Sullivan University uses CampusNexus as its student information system to store and maintain electronic student records. Sullivan University also utilizes electronic forms through the protected CampusNexus data platform. Additionally, any forms, electronic and paper, related to the enrollment and academic matriculation of a student, are stored and maintained in Perceptive Content. Electronic student record permissions are set in both the CampusNexus and Perceptive Content systems to allow only trained, academic support staff to add and make changes to student records. The electronic permissions are applied according to approved job responsibilities and each employee has a unique login and password which identifies him/her as a specific user. The unique login and password system allows the ability to ascertain the employee who executed a targeted function. Office of the Registrar personnel receive departmental training regarding FERPA, the execution of records review and maintenance, proper records storage and concealment, records request processes and technical training for the use of CampusNexus and Perceptive Content.

Paper files, for records Sullivan University assumed responsibility, in the form of transcript cards for former Bryant and Stratton College, are also maintained in the Office of the Registrar. They are in a secure, segregated areas of the Office of the Registrar. This area is locked and only the University Registrar, Associate Registrar and Records Supervisor have access. Inactive records are housed at Access, a data vault company. There is a secure system for the request and return of any inactive student records from File Management Pros. The Office of the Registrar is locked during non-business hours.

For additional information contact slv-registraroffice@sullivan.edu or call (502) 413-8507.

Department of Housing & Residence Life

The following information regarding student data is retained in the Office of Housing and Residence Life at Gardiner Point Residence Hall. The records retained relate to:

- Forms and waivers which include, medical and emergency contact information, room liability, policy and procedure acknowledgements and building waiver releases
- Room assignment, room condition, room occupancy, and roommate change requests and single room requests
- Lease information and miscellaneous fines or fees

- Disciplinary or informational incidents or actions originating in the residence halls
- Room and mailbox key distribution

Records of student information is retained in physical and electronic form. Specifics concerning the stored data is outlined below:

- Records related to the assignment process are maintained in Outlook, Microsoft Teams, PandaDoc and in hard copy. The hard copies for active students are held in student files and are maintained in a locked office within the housing office. Past student files are stored in a locked archived housing closet and held on record for a minimum of 5 years.
- Records related to financial information, such as leases are maintained in CampusNexus, Perceptive Content, Microsoft Teams and in hard copy. The files for active students are held in student files and are maintained in a locked office within the housing office. Past student files are stored in a locked archived housing closet and held on record for a minimum of 5 years.
- Records related to active housing students, regarding disciplinary affairs are maintained in hard copy form. The files for active students are held in student files and are maintained in a locked office within the housing office. Past student files are stored in a locked archived housing closet and held on record for a minimum of 5 years. An electronic file is also created and maintained on a secure server via ReportExec. Only individuals with authorized access to the Student Conduct System may access the database through login procedures.
- Records related to student key registration is held electronically within the Onity Key Database. Only authorized personnel have access to this information following login procedures.

Staff members should follow FERPA guidelines when handling confidential information.

For additional information contact the Department of Housing and Residence Life at (502) 213-8330.

Financial Planning Office

The Financial Planning office handles confidential and sensitive information, which is any information pertaining to the students' financial aid eligibility and personally identifiable information, by allowing only authorized school officials access to such data. All financial aid related data is contained within Sullivan University's student information system, Campus Nexus. The Senior Director of Financial Planning authorizes access to individuals on an as-needed basis and requests for access are provided by our internal IT department. Staff are assigned exclusive credentials for login to the student information system. Hard copy information is filed by student name, last then first, and is kept in a filing cabinet in the Senior Director's office which is locked during non-office hours.

The Financial Planning office collects, manages, and has access to a vast amount of confidential student and parent data. This data includes information from the Free Application for Federal Student Aid (FAFSA), the Institutional Student Information Record (ISIR), and the National Student Loan Data System (NSLDS), as well as information from other sources, such as tax returns, professional judgment documents, student progress data, and other private and sensitive information. Due to increased regulatory focus on student-data privacy, Financial Planning is aware and adheres to the legal restrictions that govern the sharing of student

financial aid information with other institutional offices and outside entities protecting the release of private student data.

Additionally, Financial Planning follows the guidance from three important laws that control the release of student data: (1) Sections 483(a)(3)(E) and 485B(d)(2) of the Higher Education Act (HEA), as amended; (2) the Family Educational Rights and Privacy Act (FERPA); and (3) the Privacy Act and the statutory and regulatory restrictions on the improper release of student data. Conceptually, Financial Planning understands the distinction between restrictions on uses of FAFSA data under the HEA, general restrictions on the release of all student data under FERPA, and the release of government data under the Privacy Act. The Department of Education requires that safeguard procedures be in place for the institution to be eligible for Federal Financial Aid. Below is more information on how Financial Planning controls the privacy and release of student data.

HEA, FERPA, and the Privacy Act

Scope of the HEA Restriction on Releasing Data from the FAFSA

Section 483(a)(3)(E) of the HEA limits the use of FAFSA application data. Without a student's written consent, SU can only share FAFSA data for the purpose of applying for, awarding, and administering Title IV funds, state aid, and institutional aid programs. PTAC guidance states that ED's interpretation of the "administration of aid" release provision includes audits and program evaluations necessary for the efficient and effective administration of the student aid programs. This includes mandatory federal reporting, such as to the Integrated Postsecondary Education Data System (IPEDS).

With a student's written consent, however, Sullivan University (SU) can share FAFSA data with scholarship granting organizations, tribal organizations, or other organizations assisting the applicant in applying for and receiving federal, state, local, or tribal financial assistance for any component of the applicant's cost of attendance. The Financial Planning Office keeps this data separate from other data collected from the student to ensure that it is only used for the awarding and administration of financial aid.

FAFSA data is easy to identify; it comprises answers to the 100+ questions students and parents are required to answer on the FAFSA. However, SU's Financial Planning Office follows PTAC's guidance which clarifies that the HEA restriction applies broadly to FAFSA data, ISIR data, key processing results, expected family contribution, awards, and the student's financial aid history, as reflected in NSLDS. The PTAC guidance also states that use of the ISIR data to determine award eligibility, and the resulting awards and disbursement data, including information contained in the Common Origination and Disbursement (COD) System, are covered by the same restrictions that apply to the FAFSA data.

Similar or identical data collected by the institution through a source other than the FAFSA, such as the CSS Profile, is not subject to the same HEA restriction. However, data collected through a source other than the FAFSA would be part of the education record and therefore subject to the FERPA regulations.

Scope of the HEA Restriction on Releasing NSLDS Data

The Financial Planning office follows Section 485B(d)(2) of the HEA that contains a provision that specifically prohibits the release of PII from NSLDS to non-governmental researchers and

policy analysts and also prohibits use of NSLDS data for marketing purposes. These restrictions also apply to NSLDS data on the student's ISIR.

Scope of FERPA

FERPA prohibits institutions receiving federal funds from disclosing personally identifiable information contained in education records without the express written consent of the student unless doing so falls into one of several exceptions found in 34 C.F.R. 99.31. Unless student data is requested by an auditor, regulatory agency, or in connection with a court order, it is important to note that Sullivan University is not required to release student data to third parties simply because it may do so under one of the FERPA exceptions.

The term "education records" is defined as those records that contain personally identifiable information directly related to a student and which are maintained by SU or by a party acting on behalf of SU. PII includes items such as the student's name, address, Social Security Number, or student identification number, but it also includes indirect identifiers such as the student's date of birth, place of birth, and mother's maiden name. PII also includes information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.

Records received or created and maintained by the Financial Planning office (regardless of the format of the documents) that directly pertain to a student qualify as education records. This includes most records generated and held by the SU's financial planning office, including but not limited to the following:

- Grades
- Student course schedules
- Disciplinary records
- Financial aid applications (FAFSA application also subject to the HEA restriction)
- Financial aid history information (including transfer students)
- Cost of attendance information, including documentation relating to any adjustments
- Records relating to eligibility and disbursement of federal student aid funds
- Satisfactory Academic Progress (SAP) documentation
- Documents used for verification of FAFSA data
- Loan entrance and exit counseling records
- Student financial records, including student account and loan repayment records

Scope of the Privacy Act

The Privacy Act applies to ED's student records to prevent the improper release of government-held student PII. ED is prohibited from releasing student records from their systems without prior written consent from the individual to whom the record pertains. However, the Privacy Act allows for the release of data to institutions for the "routine use" for which the data was collected.

The Student Aid Internet Gateway (SAIG) agreement between Sullivan University and ED establishes requirements for the electronic exchange of student data for the administration of the Title IV programs. Under the SAIG agreement, access, disclosure, and use of student data is limited to "authorized personnel." Sullivan University's "authorized personnel" includes only

those staff who are permitted access to the information under all applicable statutes and regulations, which would capture, for example, FERPA's school official and studies exceptions.

FAFSA Data

As discussed above, FAFSA data is part of the student's educational record and is protected by the FERPA regulations. Information that is exclusive to the FAFSA is also subject to the more restrictive HEA provisions.

- Under FERPA, disclosure of FAFSA data is permitted without the student's written consent if necessary, to determine financial aid eligibility or the amount of aid, the conditions for the aid, or to enforce the terms and conditions of the aid.
- Under the HEA, however, the FAFSA application data may only be used for the application, award, and administration of Title IV funds, state aid, and institutional aid programs or, with the student's written consent, for the purpose of assisting the applicant in applying for and receiving federal, state, local, or tribal financial assistance for any component of the applicant's cost of attendance.
- Sullivan's Financial Planning office follows the PTAC guidance that, de-identified, aggregate, descriptive statistics about program participants is a permitted use of the FAFSA data and related award information, because it relates to the administration of the financial aid programs. If a data set subject to FERPA is properly de-identified, it may be released without student consent under the FERPA rules.
- Sullivan University does not release a student's FAFSA data and related award information that has not been de-identified for purposes other than those prescribed in the HEA (including the amendments to HEA that were included in the FY18 and FY19 federal appropriations bills), even if the student provides a signed release. The student must provide the data directly to the requesting party.
- Sullivan University is required to disclose student records, including the FAFSA data and the resulting award information, to an independent auditor, ED, accrediting agencies, and other state and local education agencies, without obtaining prior written consent, as required by 34 C.F.R.§ 668.24.

De-identified Data

Sullivan University follows ED's PTAC guidance on how student data can be de-identified for release without student consent under FERPA and the HEA. Data de-identification is defined in 34 C.F.R. § 99.31(b) as the removal of all personally identifiable information provided to the institution and the determination that the student's identity is not personally identifiable.

The PTAC document states that the de-identification requirement goes beyond the removal of the student's name and Social Security Number. The removal of direct and indirect identifiers is required, along with the introduction of one or more statistical disclosure limitation (SDL) techniques like suppression, recoding, or the introduction of "noise" into the data. Determining the methods for de-identifying data and limiting disclosure risk must be made on a case-by-case basis after examining the underlying data sets and determining what information is publicly available.

Educational Records

As outlined above, FERPA generally prohibits disclosure of student education records without the student's prior written consent. There are several exceptions where prior written consent is

not required, including, but not limited to, the following examples that may be relevant in the financial aid context:

- Disclosures to other offices or departments at the institution are generally prohibited unless the institution has determined that the school official requesting the data has a "legitimate educational interest" in the records and uses reasonable methods to ensure that school officials obtain access to only those education records in which they have legitimate educational use for the information as part of their official duties. Additionally, Sullivan University discloses the information under this exception in its annual notification of FERPA rights and states the criteria it uses to determine who constitutes a school official and what constitutes legitimate educational interest. For example, a legitimate educational use of a student's educational record would include such things as the review of a student's grades by an advisor for determining the need for academic counseling, registration activities, or a degree audit.
- Sullivan University may disclose PII from education records to a contractor, consultant, volunteer, or other third party outside the University if the University has outsourced institutional services or functions to that entity. In such cases, the third party must perform an institutional service or function for which the University would otherwise use its own employees and the third party must be under the direct control of the University with respect to the use and maintenance of education records. Sullivan University enters into written agreements with such third parties outlining the purpose, scope, and the information to be disclosed, limiting the use of personally identifiable information to one or more specific purposes, and prohibiting disclosure of records to anyone other than representatives of the entity with third party legitimate educational interest in the data.
- Sullivan University may disclose, and in some cases may be required to disclose, student records to ED, auditors, accrediting agencies, and other state and local education agencies without obtaining prior written consent in connection with an audit or evaluation of federal or state supported education programs, or for the enforcement of or compliance with legal requirements that relate to those programs.
- Sullivan University may disclose information regarding students that it classifies as "directory information." Only information that would not generally be considered harmful or an invasion of privacy if disclosed can be considered directory information, and the institution must provide public notice to students each year informing them of the information it considers to be directory information. Directory information may include information such as the student's name, email address, photograph, major field of study, grade level, and enrollment status. As part of the annual notice, students are given the opportunity to opt out of having their directory information disclosed.
- Sullivan University may disclose student information, if necessary, to determine financial aid eligibility or the amount of aid, determine the conditions for the aid, or to enforce the terms and conditions of aid that the student has received or for which the student has applied.
- Sullivan University may disclose student information to officials of another school where the student intends to enroll, or where the student is already enrolled so long as the disclosure is for purposes related to the student's enrollment or transfer.

Violations

Any violation of the rules, regulations, policies, and procedures in this Information Security Plan may lead to suspension of access to Information Technology resources, with the possibility of revocation of privileges, or other action as provided by disciplinary provisions applicable to faculty, staff, or students. Confirmed or suspected violations of local, state or federal laws will be turned over to the appropriate law enforcement agency.

Continuing Evaluation and Adjustment

This Information Security Plan will be subject to periodic review and adjustment. The most frequent of these reviews will occur within the IT department where constantly changing technology and evolving risks mandate increased vigilance. Continued administration of the development, implementation, and maintenance of the plan will be the responsibility of the Information Security Steering Committee who will assign specific responsibility for implementation and administration as appropriate. The Committee will review the standards set forth in this policy and recommend updates and revisions as necessary. It may be necessary to adjust the plan to reflect changes in technology, the sensitivity of student/customer data and internal or external threats to information security.

Revision History

July 6, 2020: Created and Approved

December 7, 2022: Reviewed, Edited, and Approved