DATA SECURITY PLAN

TENAJ Salon Institute

Institute Data Security Plan

Contents

Data Security Plan (DSP) 2
RGEES Platform Asset Contacts 2
Important DSP Links 3
Tenaj Salon Institute / Organization Requirements (Business, Functional and Technical) 4
Sensitive Data Protection 13
Privacy Statement 14
Family Educational Rights and Privacy Act (FERPA) 15

DATA SECURITY PLAN (DSP)

This Data Security Plan for TENAJ Salon Institute describes safeguards to protect data, information, and resources. These safeguards are provided to:

- Enable due diligence to ensure the security and confidentiality of covered data, information, and resources
- Protect against anticipated threats or hazards to the security or integrity of such information
- Protect against unauthorized access to or use of covered data, information, and resources that could result in substantial harm or inconvenience

This Data Security Plan also provides for mechanisms to identify and assess the risks that may threaten covered data, information, and resources. Manage and control these risks; implement and review the plan; and adjust the plan to reflect changes in technology, the sensitivity of covered data, information and resources, and internal or external threats to information security. Focus for this document is on the RGEES system.

RGEES Asset Information

The following tables provide information about the operational environment.

The Tenaj Salon Institute will utilize a virtual server residing at name and address . Name is an AICPA SOC accredited service organization. The facility features an N+1 rated data center fitted with fire-suppression systems, UPS, back-up generators and environmental controls to ensure high-quality, uninterrupted service. Using state of the art software and in-house facilities experts, the Atlanta data center is continuously monitored 24 hours a day, seven days a week, 365 days a year.

The facility deploys numerous security strategies including 24/7 on-site security, mantraps to prevent tailgating, keycard access systems, video surveillance cameras and system, isolated shipping and receiving area, precast reinforced concrete walls, equipment checks and is SOC Type II certified.

RGEES PLATFORM ASSET CONTACTS

Asset Role	*Name*	*Phone Number*	*Email*
Primary (User) Contact	Name		
Administrator			
Secondary Contact			

IMPORTANT DSP LINKS

Link Purpose	*Link Address*
To access soft copies of this report	https://DSP.tenajsaloninstitute.com
Tenaj Salon Institute/ Organization website	https://DSP. tenajsaloninstitute.com
Tenaj Salon Institute/ Organization Email	tenajsaloninstitute@tenajsaloninstitute.com

TENAJ SALON INSTITUTE / ORGANIZATION REQUIREMENTS (BUSINESS, FUNCTIONAL AND TECHNICAL)

ELEMENT	DESCRIPTION
Employee Management and Training	The Chief Compliance Officer will work directly with the REGEES system. If Other employees work with the RGEES platform they will undergo training. During employee RGEES training each employee working with the RGEES platform will receive proper training on the importance of confidentiality of student records, student financial information, and other types of covered data, information, and resources. Each employee is also trained in the proper use of computer information and passwords. Training includes controls and procedures to prevent employees from providing confidential information to an unauthorized individual, including "pretext calling" and how to properly dispose of documents that contain covered data, information, and resources.
Physical Security	The Tenaj Salon Institute has addressed physical security by placing access restrictions at buildings, computer rooms, and records storage facilities containing RGEES data, information, and resources to permit access only to authorized individuals. These locations and data storage containers are to be locked, and only authorized employees are permitted to possess keys or combinations to them. Paper documents that contain covered data and information are to be shredded at time of disposal. The Tenaj Salon Institutes data resides on a virtual server within an AICPA SOC II certified data center.
Information Systems	Access to covered data, information, and resources is limited to those employees who have been trained and have a business reason to know such information. Each employee is assigned a set of unique credentials. Databases containing personal covered data, information, and resources including, but not limited to, accounts, balances, and transactional information are available only to employees in appropriate departments and positions. The Tenaj Salon Institute will take reasonable and appropriate steps consistent with current technological developments to make sure that all covered data, information, and resources are secure and to safeguard the integrity of records in storage and transmission. The Tenaj Salon Institute requires that all systems meet necessary security requirements as defined by the system administrator. These requirements include maintaining the operating system and applications, including application of appropriate patches, and updates in a timely fashion. Authentication is also required of users before they can access system-protected data. In addition, security systems have been implemented to assist with detection and mitigation of

	threats, along with procedures to handle security incidents when they do occur. Encryption technology will be utilized for both storage and transmission. All covered data, information, and resources will be maintained on systems that are behind a firewall.
Management of System Failures and Compromises	The Tenaj Salon Institute has developed plans and procedures to detect actual or attempted attacks on the Tenaj Salon Institute's systems and has an Incidence Response plan in place which outlines 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 to the Tenaj Salon Institute if it determines it will not provide them 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 "Tenaj Salon Institute / Organization" to terminate the contract without penalty • A provision ensuring that the contract's confidentiality requirements shall survive any termination agreement.

Anti - Virus	1. All Tenaj Salon Institute systems must have anti-virus software installed. 2. The anti-virus software and the virus definitions must be kept up-to-date. 3. Virus-infected computers may be removed from the network until they are verified as virus-free. 4. The System Administrator is responsible for creating procedures that ensure anti-virus software is in place, operating correctly, and computers are virus-free. 5. Any activities with the intention to create and/or distribute malicious programs into the Tenaj Salon Institute's networks (e.g., viruses, worms, Trojan horses, etc.) are prohibited.
Network Control and Access	1. Anyone who uses the computing environment must be properly authorized. 2. Users must not: • Perform acts that negatively impact the operation of computers, peripherals, or networks or that impedes 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 actions resulting from unauthorized use of the Tenaj Salon Institute's network and system accounts. 4. The Tenaj Salon Institute has installed various network security devices, including account passwords and firewalls, to help ensure the safety and security of 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 by management, without prior approval from management, is strictly prohibited. 6. Prior to connecting any system to the RGEES system network, approval must be obtained in writing from management.

	7. Attachment of any the following devices to the RGEES network, other than those provided or approved by management, 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 or obtained through management is not permitted. 9. Only management staff or authorized agents may move Tenaj Salon Institute-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.
Security Assessment	1. Network and system security will be assessed on a periodic basis. 2. Security testing and audits will be conducted on a periodic basis. 3. If a security concern is found, the responsible party will be notified so the problem can be addressed. Depending on the severity of the concern the device may be removed from the network.
End-User Devices (Workstations, Laptops, Tablets, Mobile Devices, etc.)	1. Users are responsible for the security and integrity of the Tenaj Salon Institute's information stored on their end-user devices, which includes controlling physical and network access to the equipment. This includes personally owned devices to the extent they access the Tenaj Salon Institute's IT services or contain the Tenaj Salon Institute's data of any kind. Storage of Confidential or personal covered data on mobile devices is strictly prohibited. 2. Users may not run or otherwise configure software or hardware that may allow access by unauthorized users. 3. Employees must not access Tenaj Salon Institute-owned end-user devices that have not been provided to them for their work

	without the express permission of management. 4. Employees accessing the Tenaj Salon Institute's IT services and systems with their own personal devices must adhere to all IT polices 5. Anti-virus software must be installed on all workstations/laptops that connect to the Tenaj Salon Institute's network.
Software Licenses	1. Virtually all commercially developed software is copyrighted; and the users may use it only according to the terms of the license the Tenaj Salon Institute obtains. 2. Duplicating such software with the intent to redistribute or installing multiple instances of such software without authorization is prohibited. 3. All users are legally liable to the license issuer or copyright holder. 4. Placing unlicensed or illegally obtained software, music, movies, or documents on Tenaj Salon Institute's computers is strictly prohibited.
Physical Access	1. Electronic data is protected via the data center. During transmission and storage electronic data is encrypted. During storage traditional data (paper, surveys etc.) are stored within a locked file container within a locked office. 2. Access should only be granted to any person with proper authorization to access the corresponding area. 3. Unauthorized access to areas where personally identifiable information is stored is prohibited and prevented by locks. 4. Management 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. 5. Employees who are (involuntarily) dismissed from the Tenaj Salon Institute 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. 6. If an employee does not return his/her keys, areas controlled by the outstanding keys must be rekeyed. 7. Tenaj Salon Institute information or records may not be removed (or copied) from the office where it is kept except in performance of job responsibilities. 8. Access to the Tenaj Salon Institute's IT Infrastructure operations areas shall be restricted to those responsible for operation and maintenance.

	9. Adequate disaster recovery plans and procedures are required for critical systems data.
Systems	1. Administrative access to servers containing or processing protected data must be password protected. 2. Servers are physically located in an access-controlled environment at the data center. 3. All servers deployed at the Tenaj Salon Institute must be approved by management. System maintenance plans must be established and maintained and approved by management. 4. All servers must be approved by management. At a minimum, the following information is required to positively identify the point of contact: 5. Network Services should be kept up-to-date with any changes to system information. 6. Operating system configuration should be in accordance with approved security best practices. 7. Services and applications that will not be used must be disabled where possible. 8. Access to services should be logged and/or protected through access-control methods if possible. 9. The most recent patches must be installed on the system as soon as practical. 10. Do not use accounts with elevated privileges (such as administrator or root) access when a non- privileged account can be used. 11. Privileged access must be performed via an encrypted network protocol (such as SSH, HTTPS) and/or over an encrypted method). 12. All security-related events on critical or sensitive systems must be logged and audit trails saved for a minimum of 30 days. 13. Security-related events will be reviewed and, if necessary, corrective measures will be made as needed. Security-related events include, but are not limited to: • 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. 14. Audits may be performed on any device utilizing the Tenaj Salon

	Institute's Network resources at the discretion of management.
Passwords	1. Passwords are designed to prevent unauthorized access to information. Users are responsible for safeguarding passwords along with other authentication mechanisms (such as user names, PINs, etc.) and are accountable for negligent disclosure of passwords. 2. Passwords should be a minimum of 8 characters long and constructed of a combination of alpha and numeric characters. 3. Passwords changes are immediately if compromised. Passwords should be memorized and never written down. 4. Passwords should not be stored in electronic form – in computer files or on portable devices such as USB memory keys unless strongly encrypted. 5. Passwords should not be stored in browser caches or other "auto complete" types of features available in browsers and other software. These password "memorization" functions should be disabled and never utilized. 6. Passwords must not be inserted into email messages or other forms of electronic communication without the use of strong encryption. 7. Do not use the same password for the Tenaj Salon Institute's accounts as for other non-Tenaj Salon Institute access (e.g., personal ISP account, option trading, benefits, etc.). 8. The Tenaj Salon Institute's accounts or passwords should not be shared with anyone. All passwords are to be treated as confidential information. 9. Password "lockout" features should be enabled on any systems where it is available and reasonable to implement. Users will be locked out of systems after X number of unsuccessful attempts in Y period of time to log in and will require administrator intervention to regain access.
System Backup	Full backups along with snapshot are performed daily.
Physical Assets	1. Networking and computing hardware should be placed in a secure environment and space shall be dedicated to their functions whenever possible. 2. Employees must know where the fire suppression equipment is located and how to use it. 3. Materials should not be stored on top of or directly next to equipment; proper airflow and environmental conditions must be maintained.

Wireless Access	1. This policy strictly prohibits access to network resources via open, unsecured wireless communication mechanisms. 2. Wireless access points not sanctioned by the Tenaj Salon Institute are prohibited.
Destruction and Disposal of Information and Devices	1. 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. 2. When donating, selling, transferring, surplusing, or disposing of computers or removable media, care must be taken to ensure that confidential data is rendered unreadable. Any confidential 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 destroyed.
Security Monitoring	Information on the RGEES systems and security software will be monitored to ensure security incidents have not occurred. Logs should be reviewed routinely.
Incident Reporting	1. Any actual or suspected security incident that involves unauthorized access to electronic systems owned or operated by the Tenaj Salon Institute. 2. Malicious alteration or destruction of data, information, or communications 3. Unauthorized interception or monitoring of communications 4. Any deliberate and unauthorized destruction or damage of IT resources 5. Unauthorized disclosure or modification of electronic Tenaj Salon Institute or personal information. Incidents will be treated as confidential unless there is a need to release specific information.
Incident Response	The Tenaj Salon Institute's management is the primary point of contact for responding to and investigating incidents related to misuse or abuse of the Tenaj Salon Institute's Information Technology Resources. This includes computer and network security breaches and unauthorized disclosure or modification of electronic Tenaj Salon Institute appeal or personal information. Upon discovery of a security breach, provide initial notification of the breach to: Name: Kevin Thompson Title: Chief Compliance Officer

Phone Number: 770-635-5750

Management will then take steps to:

- Inform local law enforcement or the state attorney general as appropriate.
- Report stolen finances or identities and other cyber-crimes to the Internet Crime Complaint Center at www.ic3.gov.
- Report fraud to the Federal Trade Commission at www.onguardonline.gov/file-complaint.
- Report computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or www.us-cert.gov.

Steps to follow in case of an incident (Information law enforcement will need):

1. Create a log of all actions taken and maintain this log consistently throughout the incident response process.
2. 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.
3. 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 the Tenaj Salon Institute's resources and services. Document the decision process.
4. 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.
5. 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.
6. 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 Tenaj Salon Institute.

7. Correct any identifiable system or application vulnerabilities that allowed the intrusion to occur.
8. Verify system and data integrity.
9. Restore service once the integrity of the system and/or information has been verified.
10. Management 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;
11. Corrective actions taken to prevent future occurrences; Estimated costs of incident and any corrective actions; and Identity of those responsible for the incident (if available).

SENSITIVE DATA PROTECTION

Special care and awareness is 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 Tenaj Salon Institute or individuals to which it pertains. Unauthorized disclosure or mishandling of sensitive data can be a violation of federal and state law and the Tenaj Salon Institute 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 business. Other types of data such as medical information, tax returns, donor information, mailing lists, scholarship information, financial information, and bidding 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 the Tenaj Salon Institute's

employees handling any sensitive data to understand what data are sensitive and confidential and to adhere to the following guidelines and any applicable regulations.

- Data should be stored in as few places as possible and duplicated only when necessary. Unless absolutely necessary, data should be stored on the RGEES system only.
- Avoid storing data on departmental servers or creating "silo" databases that duplicate data
- 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.
- Do not store confidential 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.
- Know and understand your environment technically. Understand who has access to areas to which you send, receive, store, or transmit data.
- Transmission and storage of any sensitive data should be encrypted.
- Release of Tenaj Salon Institute data to 3rd Parties - Do not release Tenaj Salon Institute data of any kind to 3rd party, non- Tenaj Salon Institute 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 Tenaj Salon Institute's management enlisting the services of the 3rd party entity. Any of the Tenaj Salon Institute's employees releasing data to a non-Tenaj Salon Institute 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.
- Do not send, receive, or store any sensitive data using email under any circumstances. Email is not secure.
- Report any breaches, compromises, or unauthorized/unexplained access of confidential data immediately to management.
- All traditional data (paper, survey's etc.) must be kept in a locked file container within a locked room when not occupied or in use by an authorized person(s).

PRIVACY STATEMENT

1. The Tenaj Salon Institute endeavors to ensure that its treatment, custodial practices, and uses of "Personal Information" are in full compliance with all related federal and state statutes and regulations.
2. The Tenaj Salon Institute commits to take reasonable precautions to maintain privacy and security of students' and employees' personal information. The Tenaj Salon Institute cannot guarantee that these efforts will always be successful; therefore, users must assume the risk of a breach of the Tenaj Salon Institute's privacy and security systems.
3. The Tenaj Salon Institute does not intend to sell, or otherwise disclose for commercial purposes, outside the scope of ordinary Tenaj Salon Institute functions, students' and employees' name, mailing address, telephone number, e-mail address, or other information. While the Tenaj Salon Institute

makes reasonable efforts to protect information provided to us, we cannot guarantee that this information will remain secure and are not responsible for any loss or theft.

4. Personally identifiable information is defined as data or other information which is tied to, or which otherwise identifies, an individual or provides information about an individual in a way that is reasonably likely to enable identification of a specific person and make personal information known about them. All such data is stored in compliance with applicable laws.
5. Personal information includes, but is not limited to, information regarding a person's social security number, driver's license, marital status, financial information, credit card numbers, bank accounts, parental status, gender, race, religion, political affiliation, personal assets, medical conditions, medical records, and personnel or student records.
6. Some data items are considered directory information and will be released to the public unless a request is filed to prevent disclosure of the information, except for any other reason than official Tenaj Salon Institute business. Employees who request confidentiality of that information should contact management; and students should contact their executive director.
7. The Tenaj Salon Institute assumes that failure on the part of any student or employee to specifically request the withholding of categories of information indicates individual approval for disclosure.
8. The Tenaj Salon Institute is bound by the Family Educational Rights and Privacy Act (FERPA) regarding the release of student education records, and in the event of a conflict with Tenaj Salon Institute policies, FERPA will govern.

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA)

Notification of Rights

The Family Educational Rights and Privacy Act (FERPA) affords students certain rights with respect to their education records, including:

STUDENT RECORDS

The Student Services Coordinator is responsible for the maintenance of the official student record. All requests for copies should be made through this office. Official transcripts are released to other Tenaj Salon Institutes by request only. Request must be typed or printed in ink on a standard 8.5” by 11” sheet of paper. Request must include Tenaj Salon Institute name, address, city, state, zip code, area code, phone number, and contact person. Transcripts will be mailed within fourteen (14) business days from the date of the request. *All financial obligations must be met in order for the school to release a transcript.*

The Family Educational Rights and Privacy Act (FERPA) is a federal law designed to protect the privacy of a student's educational records. Because SCHOOL NAME is a post-secondary educational Tenaj Salon Institute, the rights described in FERPA belong to the students at HSI, rather than their parents. The term "student" as used in the following FERPA policy applies to currently enrolled students and former students who were accepted, began attending classes, and either graduated, withdrew or did not graduate. Questions about FERPA or FERPA rights should be addressed to the Executive Director.

Annual Notification

Students are notified of their FERPA rights by receipt of this document during orientation. Faculty and staff are notified of schools name FERPA policies and procedures by receipt of this document, given to all full and part-time employees at the time of hire.

Student Rights Under FERPA

Students (or parent or guardian if the student is a dependent minor) have the right to inspect and review their educational records according to the following procedure:

- Request amendment of their educational records - Students may ask SCHOOL NAME to amend a record that they believe is inaccurate or misleading. They may submit a written request for amendment of their record(s) to the Executive Director, specifying why they believe the record is inaccurate or misleading. The Executive Director will notify the student of the decision made on the request for amendment.
- Consent for disclosure of their educational records - The exceptions to disclosure of student records only with written consent are noted below.
- File a complaint with the U.S. Department of Education-Individuals who have questions about FERPA or who wish to file a complaint should contact:

  Family Policy Compliance Office, U.S. Department of Education, 600 Independence Avenue, S.W., Washington, D.C.
  20202-4605

Procedures to Inspect Educational Records

Students should submit to the Executive Director a written request, which identifies as precisely as possible the record or records he or she wishes to inspect. The Executive Director will make the needed arrangements for access as promptly as possible and notify the sstudent in writing of the time and place where the records may be inspected. Access will be given in 30 calendar days or less from the receipt of the request. When a record contains information about more than one student, the student may inspect and review only the records that relate to him or her.

Refusal to Provide Copies

School s name reserves the right to deny transcripts or copies of records not required to be made available by the FERPA in any of the following
situations:

- The student lives within commuting distance of HSI
- The student has an unpaid financial obligation to HSI
- There is an unresolved disciplinary action against the student

Disclosure of Education Records

Schools name will disclose information from students' education records only with the written consent of the student (or parent or guardian if the student is a dependent minor), EXCEPT:

- To school officials who have a legitimate education interest in the records. A school official is:
  - A person employed by SCHOOL NAME in an administrative, supervisory, academic or research, or support staff position.
  - A person employed by or under contract to SCHOOL NAME to perform a special task, such as an attorney, auditor or financial aid consultant.
- A school official has a legitimate education interest if the official is:
  - Performing a task that is specified in his or her position description or by a contract agreement.
  - Performing a task related to a student's education.
  - Performing a task related to the discipline of a student.
  - Providing a service or benefit relating to the student or student's family, such as health care, counseling, job placement or financial aid.

- To officials of another school, upon request, in which a student seeks or intends to enroll.
- To certain officials of the U.S. Department of Education, the Comptroller General, and state and local educational authorities in conjunction with an audit, review or evaluation of compliance with education programs.
- In connection with a student's request for or receipt of financial aid, as necessary to determine the eligibility, amount or conditions of the financial aid, or to enforce the terms and conditions of the aid.
- If required by a state law requiring disclosure that was adopted before November 19, 1974.
- To organizations conducting certain studies for or on behalf of HSI.
- To accreditation agency, government agency or the Your accrediting agency, or in direct response to a directive of the Commission.ja
- To comply with a judicial order or a lawfully issued subpoena.
- To appropriate parties in a health or safety emergency.
- The records of a disciplinary proceeding conducted by SCHOOL NAME against an alleged perpetrator of a violent crime will be disclosed to the alleged victim of that crime without the written consent of the alleged perpetrator.
- To parties requesting directory information, if a student has not provided a written request for the non-disclosure of such information.

Directory Information

School name designates the following items as Directory Information: Student name, address, telephone number, date and place of birth, major field of study (program), participation in officially recognized activities, dates of attendance, degrees, certificates and awards received, most recent previous school attended and photograph. School name may disclose any of those items without prior written consent unless notified in writing to the contrary by the tenth calendar date following a student's program start date.