GEORGIA CAREER INSTITUTE

Gramm-Leach-Bliley Act (GLBA)

Information Security Program

Version 1.2

Table of Contents

BACKGROUND

The Gramm-Leach-Bliley Act requires financial institutions—including colleges, universities, and technical schools—to protect the privacy of their customers, including customers' nonpublic, personal information. The GLBA governs colleges, universities, and technical schools and mandates that all institutions establish appropriate administrative, technical, and physical safeguards.

Georgia Career Institute has a responsibility to secure the personal records of its customers (past and present students) and employees.

REQUIREMENTS In the GLBA SAFEGUARDS RULE

The objective of the GLBA standards for safeguarding information is to

- Ensure the security and confidentiality of student information.
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any student (16 C.F.R 314.3(b)).

INFORMATION SECURITY PROGRAM

Contains administrative, technical, and physical safeguards that are appropriate to the size and complicity of our institution. The nature and scope of our activities and the sensitivity of any student information.

Also identifies mechanisms to:

- Identify and access the risks that may threaten covered data and information maintained by Georgia Career Institute.
- Adjust the program to reflect changes in technology, the sensitivity of covered data and information, and internal or external threats to information security.

DEFINITION

- **Customer-Customer Information**
  Information obtained as a result of providing a financial service to a student (past or present). Our institution provides a financial service, when they, among other things, administer or aid in the administration of Title IV programs; income share agreements; or certify education loans on behalf of the student.
- **Non-public personal information**
  This means any personally identifiable financial or other personal information, not otherwise publicly available, that the Institution has obtained from a customer in the process of offering a financial product or service; such information provided to the Institution otherwise obtained by the Institution in connection with providing a financial product or service; or any list, description, or other grouping of customers (and publicly available information about them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information

include names, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.

- **Financial product or service**
  Includes student loans, activities related to running parents' credit, management consulting and counseling activities, and other miscellaneous financial services.

- **Covered Data and Information**
  The purpose of this Program includes non-public personal information of customers required to be protected under GLBA. In addition to this required coverage, the institution chooses as a matter of policy to also define covered data and information to include any bank and credit card account numbers, income and credit information, tax returns, asset statements, and social security numbers received during business by the institution, whether or not such financial information is covered by GLBA. Covered data and information include both paper and electronic records.

- **Encryption**
  The transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key, consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material.

1. DESIGNATED AND QUALIFIED INDIVIDUALS

The institution has a management team that involves several designated and qualified individuals responsible for overseeing, implementing, and enforcing the information under the terms of this security plan.

The designated and qualified individuals are:

a) **Management**

Lauren Davis, COO is responsible for overseeing, implementing, and enforcing the institution's Information Security Program in compliance with this part.

School Directors are responsible for assessing the risks associated with unauthorized transfers of covered data, and information and implementing procedures to minimize those risks to the Institution.

Financial Aid Officers are responsible for safeguarding the integrity, confidentiality, and availability of customer information within the office of Financial Aid and its service providers.

b) **Technical**

Chris Avila, IT Director is the designed and qualified individual for overseeing, safeguarding, and implementing the technology and devices internal and external at Georgia Career Institute.

Internal Audit is conducted and reviews its areas that have access to covered data and information to assess. The internal control structure was put in place by the administration to review the controls and verify that all departments comply with the requirements of the security policies and practices delineated in this program.

2. RISK ASSESSMENT

Georgia Career Institute identifies reasonably foreseeable internal and external risks to the security, confidentially, and integrity of customer information (as the term customer information applies to our institution) that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information and assesses the sufficiency of any safeguards in place to control these risk (16 C.F.R. 314.4(b)).

3. SAFEGUARD TO CONTROL THE IDENTITY THROUGH RISK ASSESSMENT

Georgia Career Institute has policies and procedures in place to complement the physical and technical (IT) safeguards.

c) **Implements and periodically reviews access control**, including technical and as appropriate, physical control to;

- Authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information; and

- Limit authorized users' access only to customer information that they need to perform duties and functions, or, in the case of customers, to access their information;

1. **Identify and manage the data**, personnel, devices, systems, and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and the risk strategy.

2. **Protect by encryption all customer information** held or transmitted by the institution's personnel, both in transit over external Networks and at rest. To the extent the institution personnel determines the encryption of customer information, either in transit over external networks or at rest, is infeasible, the institution may instead secure such customer information using effective alternative compensating control reviewed and approved by the institution's Qualified Individual.

3. **Adopt secure development practices for in-house developed applications** utilized by you for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store customer information;

4. **The multi-factor authentication**
   The multi-factor authentication is done and performed in the Financial Aid Office due to handling FAFSA Applications, income and credit histories, COD accounts, balances, and transactional information with other authorized employees with an appropriate business need for such information.

5. **Secure Disposal of Customer Information** – To protect personally identifiable information (PII) of customer information and employees Georgia Career Institute physically disposes of PII in assigned locked console(s) for shredding.

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

Periodically the data retention policy is reviewed to minimize the unnecessary retention of data,

4. CONTROL & MONITORING

The activity of authorized users is done by the school director to detect unauthorized access or use of, or tampering with, customer information by such users.

- Safeguards' Key Controls and System- Are monitored and maintained by Georgia Career Institute.

- Cyber Security is reasonable and considering current risk assessments are sufficient to provide security and confidentiality to covered data and information maintained by the Institute. Additionally, these safeguards reasonably protect against currently anticipated threats or hazards to the integrity of such information.

5. CHANGE MANAGEMENT PROCEDURES

New employee receives proper training on the importance of confidentiality of customer information such as student records, financial information, covered data, and information. The training includes controls and procedures to prevent employees from providing confidential information to an unauthorized individual, as well as how to properly dispose of documents that contain covered data and information.

Social security numbers are considered protected information under both GLBA and the Family Educational Rights and Privacy Act (FERPA). As such, Georgia Career Institute has discontinued the use of social security numbers as student identifiers in favor of the ID# as a matter of policy. By necessity, student social security numbers will remain in the student information system; however, access to social security numbers is granted only in cases where there is an approved, documented business need.

Georgia Career Institute addressed the physical security of covered data and information by limiting access to only those employees who have a legitimate business reason to handle such information.

Employees who are no longer active with institution access are removed immediately. The school director sends an email notification to IT personnel to remove access from all devices and programs.

6. SYSTEMS INFORMATION

Is continuous monitoring and conduce regular test to monitor the effectiveness of the safeguards conducted by IT and personnel. This procedure is to detect actual and attempted attacks on, or intrusions into, information systems.

For information systems, the monitoring and testing include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring or other system to detect, on an ongoing basis, changes in information systems that may create vulnerabilities by conducting:

- Annual penetration testing of the institution's information system determined each given year based on relevant identified risks by the risk assessment; and

- Vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in the systems based on the risk assessment, at least every six months; whenever there are material changes to its operations or business arrangements; and whenever there are circumstances or have reason to know may have a material impact on the institution’s information security program.

The Institution provides for the implementation of policies and procedures to ensure the personnel are able to enact the information security program as mentioned above under change management procedures.

Management of System Failures
Georgia Career Institute Cyber Security has developed written plans and procedures to detect any actual or attempted attacks on Georgia Career Institute systems and has an Incident Response Plan which outlines procedures for responding to an actual or attempted unauthorized access to covered data and information.

7. CONTINUING EVALUATION AND ADJUSTMENT

This Information Security Program will be subject to periodic review and adjustment, at least annually. Continued administration of the development, implementation, and maintenance of the program will be the responsibility of the designated Information Security Program Coordinator(s), who will assign specific responsibility for technical (IT), logical, physical, and administrative safeguards implementation and administration as appropriate. The Information Security Program Coordinator(s), in consultation with the Office of Legal Affairs, will review the standards outlined in this program and recommend updates and revisions as necessary; it may be necessary to adjust the program to reflect changes in technology, and the sensitivity of data security.

Identification of Risks
Georgia Career Institute recognizes exposure to the external and internal risks to the security, confidentiality, and integrity of customer records could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such records.

Such risks are categorized below but not limited to:

- Unauthorized requests or access to printed, faxed, physically stored, or electronic records
- Interception of data during transmission
- Loss of data or data integrity
- System failure

Recognizing that this may not represent a complete list of the risks associated with the protection of covered data and information, Georgia Career Institute and Tech-Net will actively participate and monitor appropriate cybersecurity advisory groups for the identification of risks.

Current safeguards implemented, monitored, and maintained by Georgia Career Institute Cyber Security are reasonable, and considering current risk assessments are sufficient to provide security and confidentiality to covered data and information maintained by the Institute. Additionally, these safeguards reasonably protect against currently anticipated threats or hazards to the integrity of such information.

WRITTEN INCIDENT RESPONSE PLAN

The plan establishes and addresses the following areas: internal process for responding to a security threat, clear definition of roles, external and internal communication, and requirements for remediation. In the event of an incident, the institution's goal is to report, document, evaluate, and revise the response plan following a security event.

OVERSIGHT OF SERVICE PROVIDERS

GLBA requires the Institute to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. This Information Security Program will ensure that such steps are taken by contractually requiring service providers to implement and maintain such safeguards. The Security Program Coordinator(s) will identify service providers who have or will have access to covered data and will work with the Office of Legal Affairs and other offices as appropriate, to ensure that service provider contracts contain appropriate terms to protect the security of covered data.

MEDIA SANITATION

Media sanitization is a process by which data is irreversibly removed from media, or the media is permanently destroyed. Media sanitization is a key element in protecting personal privacy and proprietary information. The principal goal of media sanitization is to ensure that sensitive data is not unintentionally released.

Common media include physical documents, desktop and laptop computers, mobile devices, external hard drives, USB drives, and memory devices.

Media Sanitization Methods

Media sanitization methods come into play not only when storage devices reach end-of-life, but also when they are being repurposed for use within the institution. Clear, Purge, and Destroy are actions that can be taken to sanitize media:

- Clear uses standard rewriting techniques and tools to provide moderate protection against simple, non-invasive data recovery techniques. Most storage media support some level of Clear and media can be reused after Clear sanitization.

- Purge uses state-of-the-art laboratory overwrite, block erase, and cryptographic erase methods. It provides a higher level of media sanitization than Clear and is thus used when handling more confidential data. The storage media can be reused after Purge sanitization.

- Destroy uses physical destruction techniques, such as shredding, pulverizing, and incinerating, to render data recovery infeasible. Destroy can be used when media is beyond overwriting methods due to its physical condition or when it contains highly confidential data. Media cannot be reused.

Media Sanitization Steps

d) **Categorize Media According to Data Confidentiality Level**
Inventory all hardware, software, storage devices, systems, files, and any other data accessible by employees according to data confidentiality level. Media sanitization should be based on the confidentiality of the data on the media, rather than the media itself.

e) **Determine Media Life Cycle Stage**
Hardware and media that are being repurposed and reused within an educational institution may have different data destruction processes than media that have reached end-of-life. A common data vulnerability occurs when devices change hands within an institution or are sold, without properly removing data. Determines what type of sanitization method (Clear, Purge, or Destroy) is needed based on data confidentiality, media life cycle stage, and cost. If media are not intended for reuse, the simplest sanitization method may be Destroy.

f) **Sanitize Media**
Properly sanitize media based on the media type. Consult Appendix A of the NIST Guidelines for Media Sanitization for a comprehensive list of specific sanitization techniques for various media, including obsolete equipment. Common applications in higher education are below:

Paper documents: NIST guidelines recommend Destroy by using crosscut shredders that produce particles that are 1 mm x 5 mm in size (or smaller).

Desktop and Laptop Computers, External Hard Drives: For Clearing, NIST guidelines recommend overwriting media by using organizationally approved and tested overwriting technologies/methods/tools.

Mobile Devices: For Clearing or Purging, NIST guidelines recommend manually erasing all information and then performing a full manufacturer's reset to factory default settings.

g) **Document and Verify Data Sanitation**
Require sanitization documentation and signature certification regardless of the media sanitization method. Verify that sanitization occurred and review a media sample to ensure that no data is recoverable. Without verification, inadequate sanitization methods can be implemented and leave school data exposed.

RELATED INFORMATION

Pretext calling

Occurs when an individual attempts to improperly obtain personal information of Georgia Career Institute customers to be able to commit identity theft. It is accomplished by contacting the Institute, posing as a customer or someone authorized to have the customer's information, and through the use of trickery and deceit convincing an employee of the Institute to release customer-identifying information.

Student financial information

Offering a financial product or service includes offering student loans to students, receiving income tax information from a student, parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories, and Social Security numbers, in both paper and electronic format.

Ransomware
In the U.S., there was a shift away from targeting high-value organizations toward mid-sized victims to reduce scrutiny. Ransomware groups have increased their impact by targeting cloud infrastructures, managed service providers, industrial processes, and the software supply chain, and by launching their attacks on holidays and weekends.

The Joint Cybersecurity Advisory noted that if the ransomware criminal business model continues to yield financial returns, ransomware incidents will become more frequent. Authorities strongly discourage paying a ransom to criminal actors. Immediate actions the institution can take to protect against ransomware:

- Update your operating system and software.
- Implement user training and phishing exercises to raise awareness about the risks of suspicious links and attachments.
- If you use Remote Desktop Protocol (RDP), secure and monitor it.
- Make an offline backup of your data.
- Use multifactor authentication (MFA)

Note: The immediate action is taken by IT Jesus Rivas and his team

RELATED POLICIES, STANDARDS & GUIDELINES
Georgia Career Institute has adopted comprehensive policies, standards, and guidelines relating to information security, which are incorporated by reference into this Information Security Program. They include:

- **STANDARDS**
  Data Protection Safeguards

- **POLICIES**
  Cyber Security Policy
  Unit-Level Network Usage Policies
  Data Access Policy (including Sensitive Data & Server Registration)
  Credit Card Processing Policy

GLBA Policies and Procedures

Purpose: To continue to protect private information and data to comply with the requirements of the law of the Gramm-Leach-Bliley Act (GLBA). This security program applies to customers, prospects, students, parents, and employees' personal and financial information (covered data) that the institution receives in the course of business as required by GLBA.

Policy: The school officials coordinate oversight of this policy to identify reasonably foreseeable internal and external risks to the security, confidentially, and integrity of covered information.

Each Office is responsible for securing Covered Information in accordance with this policy. The Offices must comply with their own information safeguards for Covered Information.

The scope of such assessment and evaluation may include but is not limited to management (including students, prospects, parents, customers & employees) information systems (including network and software design, as well as information processing, storage, transmission, and disposal for both paper and electronic records); procedures for detecting, preventing and responding to attacks, intrusions, or other system failures (including data processing, and telephone communication), and contingency planning.

Procedure: **Protecting the Computer**

For the student or prospects, the following computer security guidelines should help protect you and the computer while accessing the campus network. We highly recommend following the advice in these guidelines, because, unfortunately, computers do get virus infections, laptops get stolen, and weak passwords get exploited. Computer security problems can be a real nightmare, leading to the loss of important data (along with loss of valuable time and effort), loss of access to services, degraded or slow performance and networking, and even theft of personal information. As you use your computer at Georgia Career Institute, there are steps to take to protect yourself from the threats that can cause these problems. We recommend the following:

- Use a strong password for your user account
- Run anti-virus/anti-malware software---------Done by IT Team
- Use your software firewall------------------------Done by IT Team
- Keep your computer up to date-----------------Done by IT Team
- Browse safely
- Desktop must be turned off when school officials are out to lunch and at the end of the day.
- Lock it up
- Back it up

Laptop Security

Company-issued laptops are restricted to those employees who need them to perform their jobs. Sensitive Information should not be stored on a laptop.

Employees are regularly reminded of this company's policy — and the legal requirement — to keep customer information secure and confidential. Employees are required to report suspicion of laptop misuse.

- Laptops must be secured in a secure place.
- Employees may access remotely company database remotely, but data should not be stored on the laptop.
- Access to a remote desktop requires a secure password.
- If a laptop must contain sensitive data, the data must be encrypted.
- Employees using laptops for travel must be mindful:
    - Never leave a laptop visible in the car.
    - If left in the car, it must be in a locked trunk.
    - Never leave a laptop at a hotel luggage stand.
    - Never pack or check in with luggage unless directed by airport security.
    - Employees should keep an eye on laptops at airport security as they go on the belt.

Passwords

Attackers can easily guess blank or weak system passwords to gain access to an account on your computer in person or, sometimes, over the network. Use a strong password with a mix of both capital and lower-case letters, numbers, and special characters (like '#', '@', or '$') to protect your computer.

Computer passwords and electronic access are the responsibility of every employee with direct access to student's electronic records. Employees are regularly reminded of this company's policy — and the legal requirement — to keep customer information secure and confidential.

- Passwords are maintained private and are not to be shared with others.
- Employees are required to create "strong" passwords that must be changed regularly. (Tough-to-crack passwords require the use of at least six characters, upper- and lower-case letters, and a combination of letters, numbers, and symbols.)
- Employees are prohibited from sharing passwords.
- Employees are prohibited from openly posting passwords in work areas or in view of others.
- Employees are required to report suspicion of password misuse.

Protect Data

The institution has adopted an information security program to safeguard private information and data and to comply with laws and regulations. While this program protects data in Georgia Career Institute systems, there are steps that students and users should take to protect their data while at Georgia Career Institute. Below are recommended actions you can take to protect your data on the Georgia Career Institute Network.

Send Files to Encrypt File Transfers

- Delete your browsing history when finished online.
- Do not save passwords on a public computer.
- Avoid online banking, shopping, entering credit card information, etc. on public computers.
- Avoid using email and other services that require a username and password while on public computers.
- Delete temporary files.
- Log off the machine when you are done.

Regardless of the cloud solution you may use, encrypting your files before uploading them will ensure the confidentiality and integrity of your data.

Faxing

Employees must take physical safeguards when faxing. Employees are regularly reminded of this company's policy — and the legal requirement — to keep customer information secure and confidential.

- Notify the recipient before sending the fax.
- Verify the fax number by telephone.
- Use a cover page, with the following Confidentiality disclosure:

CONFIDENTIALITY NOTICE:

This facsimile is intended for the person named above and is covered by the Electronic Communications Privacy Act is confidential and may include legally protected information. If you are not the intended recipient or you have received this facsimile by mistake, printing, copying, storing, or disseminating in any way is strictly prohibited, and doing so could subject you to civil and or criminal action. Please notify the sender by telephone you have received this facsimile by mistake and delete all information you received.

- Do not save a fax with Personal Identifiable Information.
- Do not leave a fax unattended in the printer or fax machine.
- Employees are required to report suspicion of faxing.

USB Drives and Externa Hard Drives

- Just pulling the USB out can potentially damage both your storage device and your data. Take time to eject your storage device correctly. Use the Safely Remove Hardware option to keep your data safe.
- Removing your storage device while files are still writing to it can result in data corruption. Always be sure that files have finished writing before removing your storage device.
- Be careful who you share your USB drives with. USB drives can become infected with computer viruses and malicious software if they are plugged into an infected machine.
- Remove your storage device when it is not in use. Leaving it attached to your computer makes your backup data vulnerable to any problems your computer might encounter--e.g. power surges, viruses, etc.

- USB sticks are small and easy to misplace or lose. You should have a secondary backup for your data just in case your USB stick fails or is lost.
- Encrypt any files that you consider confidential in case your storage device is ever lost or misplaced.

Documentation
Remember to protect Personal Identifiable Information (PII) and any hard copies of private data too.

- Keep documents that contain confidential information in a secure location.
- Limit the number of copies.
- Store and review documents before post
- Social Security numbers
- Disclose PII only to those authorized individuals.
- Tax Returns
- State IDs
- Asset Statements
- Dispose of documents properly when no longer needed on the shredding station box.
- Do not accept PII via text thru mobile phone devices.
- Student Financial Aid Files are stored in a file cabinet in the financial aid.

Physical Security of Paper Records/Preventing Identity Theft
Offices maintain procedures that reasonably assure the security of paper records and include guidelines relating to the university's records retention and disposal policy. Periodic evaluation of these procedures regarding physical paper records should be conducted.

Employees must take physical safeguards within offices that contain Personal Identifiable Information (PII) Employees are regularly reminded of this company's policy — and the legal requirement — to keep customer information secure and confidential.

- Offices containing Personal Identifiable Information (PII) must post the "LOCK IT" sign found on the following page.
- Offices containing Personal Identifiable Information (PII) must be lockable.
- Offices containing Personal Identifiable Information (PII) must have locking file cabinets & drawers.
- Offices containing Personal Identifiable Information (PII) may be accessed by authorized employees only.
- Documents containing Personal Identifiable Information (PII) must be stored properly when not in use and at the end of the day.
- Keys cannot be left unattended (e.g. in the car, at home, on top of desk, etc.)
- Report immediately when a key has been lost or stolen.
- Employees are required to report unauthorized access to PII.

Shredding & Disposal of Personal Identifiable Information

All documents that contain any of this confidential information that are no longer needed, must be disposed of in the locked console, located in the school.

Documents to be disposed of should be placed in the appropriate container and should not be left to accumulate in offices. The decision to "shred or not to shred" should be answered by the statement: if you can't decide and it is no longer being used, shred it.

Every 4 weeks, contracted staff will replace with an empty bag and the filled bag will be shredded and disposed of accordingly.

Office shredders should not be used at any time. Employees are required to report unauthorized access to PII. A sign is posted to identify the console made available to the employees.

Pretexting

Keeping others from gaining information under pretenses. When students, prospects, or customer calls or text the school. School official conducts security questions that only the student, prospect or customer will know before releasing information.

Example:

- The last 4 digits of her social
- Mother maiden name
- The last 4 digits of the telephone number
- School ID

Note: FERPA Regulation still applies to third parties requesting student's information.

Confidentiality of Company Information

All employees are asked to sign the following statement at the time of employment:

"In consideration of my employment with Georgia Career Institute, I will be exposed to information and material that are confidential and proprietary and of vital importance to the economic well-being of the institution. I will not at any time disclose or use, either during or after my employment, any information, knowledge, or data that I receive or develop during my employment that is considered proprietary by the institution or that relates to the trade secrets of the institution. Such information, knowledge, or data includes the following which is by example only: processes, know-how, accounting or financial data, salary data, marketing data, business plans, and strategies, negotiations and contracts, research, and customer or vendor lists. Employees are prohibited from removing any student or employee files.

I further agree that upon the termination of my employment with the institution, I shall promptly return any documents containing the above information, knowledge or data, or relating thereto, to the institution. This agreement shall be binding upon my successors and assigns of the institution. If a dispute arises concerning this agreement and a lawsuit is filed, the prevailing party shall be entitled to reasonable attorney's fees and costs.

I acknowledge that the proprietary and trade secrets are created at substantial cost and expense to the institution and that unauthorized use or disclosure would cause irreparable injury to the institution. I hereby consent to the order of an immediate injunction, without bond, from any court of competent jurisdiction, enjoining and restraining me from violating or threatening to violate this provision.

Security Standards & Handling Secure Information

All employees are reminded of the company's policies and practices- and the legal requirement- to keep customer information secure by physically and electronically safeguarding Personal Identifiable Information.

Cybersecurity

Is the protection of internet-connected systems, including hardware, software, and date, from cyberattacks. In a computing context, security comprises cybersecurity and physical security—both are used by Tech-Net to protect against unauthorize access to date centers and other computerized systems.

RISK ASSESSMENT FORM

Potential Risk	Location	Device	Risk Rating	Preventative Measurements	Responsible Party