GLBA Required Information Security Program

Overview: This document summarizes Coba Academy's (the "Institution, Coba") comprehensive written information security program (the "Program") mandated by the Federal Trade Commission's Safeguards Rule and the Gramm – Leach – Bliley Act ("GLBA"). This document describes the Program elements pursuant to which the Institution intends to (i) ensure the security and confidentiality of covered records, (ii) protect against any anticipated threats or hazards to the security of such records, and (iii) protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers. The Program incorporates by reference the Institution's policies and procedures enumerated below and is in addition to any institutional policies and procedures that may be required pursuant to other federal and state laws and regulations, including, without limitation, FERPA.

Designation of Representatives: Coba Academy's Vice President is the designated IT Security Officer (ISO) with the collaboration of the IT Support Company, SMB Techforce. The IT Support Company is hired to work with the ISO Officer who shall be responsible for coordinating and overseeing the Program. Any questions regarding the implementation of the Program or the interpretation of this document should be directed to the IT Security Office or his or her designees.

Scope of Program: The Program applies to any record containing nonpublic financial information about a student or other third party who has a relationship with the Institution, whether in paper, electronic or other form that is handled or maintained by or on behalf of the Institution or its affiliates. For these purposes, the term nonpublic financial information shall mean any information (i) a student or other third party provides in order to obtain a financial service from the Institution, (ii) about a student or other third party resulting from any

transaction with the Institution involving a financial service, or (iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person.

Elements of the Program:

1. Risk Identification and Assessment. The Institution intends, as part of the Program, to undertake to identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information. In implementing the Program, the Program Officer will establish procedures for identifying and assessing such risks in each relevant area of the Institution's operations, including:

- *Employee training and management*. The Program Officer will coordinate with representatives in the Institution's Office of Financial Aid to evaluate the effectiveness of the Institution's procedures and practices relating to access to and use of student records, including financial aid information. This evaluation will include assessing the effectiveness of the Institution's current policies and procedures in this area, including Employee/Instructor Policy and Procedure Handbook, School Catalog, and Campus Security Policy/ Clery Report.
- *Information Systems and Information Processing and Disposal.* The Program Officer will coordinate with representatives of the Institution's external IT support company to assess the risks to nonpublic financial information associated with the Institution's information systems, including network and software design, information processing, and the storage, transmission, and disposal of nonpublic financial information. This evaluation will include assessing the Institution's current policies and procedures relating to the acceptable use of the Institution's network and network security, document retention and destruction. The Program Officer will also coordinate with the Institutions to assess procedures for monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.

- *Detecting, Preventing and Responding to Attacks*. The Program Officer will coordinate with the Institution's IT Support Company to evaluate procedures for and methods of detecting, preventing, and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. In this regard, the Program Officer may elect to delegate to a representative of the IT Support Company the responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by the Institution.

2. Designing and Implementing Safeguards. The risk assessment and analysis described above shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper, or other form. The Program Officer will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

3. Overseeing Service Providers. The Program Officer shall coordinate with those responsible for the third-party service procurement activities with and other affected departments to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for nonpublic financial information of students and other third parties to which they will have access. In addition, the Program Officer will work with the Financial Aid Office to develop and incorporate standard, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards. Any deviation from these standard provisions will require the approval of the Financial Aid Office. These standards shall apply to all existing and future contracts entered with such third-party service providers if amendments to contracts entered into prior to 2/1/2020.

4. Adjustments to Program. The Program Officer is responsible for evaluating and adjusting the Program based on the risk identification and assessment activities undertaken pursuant to the Program, as well as any material changes to the Institution's operations or other circumstances that may have a material impact on the Program.

Coba Academy Privacy Policy Disclosures

General

Coba Academy respects the privacy of every individual who visits our websites or responds to our promotions. Coba Academy intends to act reasonably to protect your privacy, but obviously cannot guaranty security against "hackers" or other issues beyond our control. To better protect your privacy, we provide this notice explaining our online information practices and the choices you can make about the way your information is collected and used. This notice applies to all information collected or submitted on Coba Academy website, unless otherwise posted.

Information Collected from You

Personal Identifiable Information refers to information that is collected in conjunction with your name. Coba Academy does not collect any personal identifiable information from you unless you provide it voluntarily. If you do not want your personal identifiable information collected, do not submit it to us.

How We Use the Information We Collect

We use the information that we collect to complete a contact or request; to better understand your needs, to provide to Coba Academy marketing, to improve our products and services, and to contact you.

Information Provided by You

In addition to the information collected automatically through the site, our site provides an opportunity to provide personal information through forms to request more information. Coba Academy does not involuntarily collect your personal information when you use this web site. You agree that if you provide any personal information to us through this web site, we may use

this information and disclose it to others for the purpose of responding to your request.

Cookies

Coba Academy may collect other information from' you that is not in conjunction with your name. Cookies are small, text files that a website can send to your browser for storage on your hard drive. Cookies make your Internet use easier by saving your status and preferences about a website. Most browsers are initially set up to accept cookies, but you can change the setting to refuse them or to be alerted when cookies are being sent. We do not store email addresses or passwords in any cookie we create because of security concerns regarding cookies. Cookie acceptance does not interfere with your ability to interact with our website, although allowing cookies does help streamline many of the possible functions performed on this site. You may read more about cookies at www.cookiecentral.com. Individuals who use the websites need to accept cookies to use all of the features and functionality of the websites.

SMS

After you opt-in to receive messages via online, in-person or SMS, you may cancel the SMS service at any time by replying "**STOP**" to the SMS message. After this, you will no longer receive SMS messages from Coba Academy. Text "**HELP**" for help. Coba Academy does not sell or share SMS opt in or phone numbers for the purpose of SMS. The mobile carriers are not liable for delayed or undelivered messages. For all questions about the SMS message service, you can contact us at 714-533-1400 or info@coba.edu.

Coba Academy Security and Safeguard Policies

Identify and assess the risks to student information in each relevant area of the company's operation and evaluate the effectiveness of the current safeguards for controlling these risks.

Design and implement a safeguards program, and regularly monitor and test it, select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards and oversee their handling of student information.

To evaluate and adjust the program considering relevant circumstances, including changes in the firm's business or operations, or the results of security testing and

monitoring. Coba Academy's security safeguard policy allows us to assess and address the risks to student information in all areas of our operation, including three areas that are particularly important to information security: Employee Management and Training.

Information Systems; and Detecting and Managing System Failures

ISO Officer: Ms. Michele Malkasian, Vice President| Coordinators for information security with ISO: SMB Techforce.

Risks to Student Information

Information at risk: student's personally identifiable information (Pll), especially Social Security Number. Student Identification Numbers are issued to students upon enrollment.
Risks: Data in databases on servers, printed data, data transmissions, and data in files on in-house network, data on remote staff Personal Computer.

Employee Management and Training (Vice President)

- We check references or do background checks before hiring employees who will have access to student information.
- We ask every new employee to sign an agreement to follow Coba Academy confidentiality and security standards for handling student information.
- We limit access to student information to employees who have a business reason to see it.
- For example, give employees who respond to student inquiries access to student files, but only to the extent they need it to do their jobs.
- We control access to sensitive information by requiring employees to use "strong" passwords that must be changed on a regular basis. (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.)
- We have policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices. For example, we educate our employees to store these devices in a secure place when not in use.

- We train employees to take basic steps to maintain the security, confidentiality, and integrity of student information, including locking rooms and file cabinets where records are kept.
- We do not share or openly post employee passwords in work areas.
- We encrypt sensitive student information when it is going to be transmitted electronically via public networks.
- We refer calls or other requests for student information to designated individuals who have been trained in how safeguards personal data.
- We report suspicious attempts to obtain student information to designated personnel.
- We regularly remind all employees of Coba Academy's policy — and the legal requirement — to keep student information secure and confidential.
- We impose disciplinary measures for security policy violations.
- We prevent terminated employees from accessing student information by immediately deactivating their passwords and usernames and taking other appropriate measures.

Information Systems (SMB Techforce)

Information systems include network and software, and information processing, storage, transmission, retrieval, and disposal.

All Coba Academy student data is stored in a secure database server, accessible only to designated staff. Our vendors database server and the database itself is being backed up daily.

Copies of this backup are stored off-site and offline in a physically secure area. Servers, workstations, and offline storage are protected by strong passwords. Coba's database servers are located on a separate network subnet, accessible only to vendors Developer Team and does not have direct Internet access.

We maintain an inventory list of computers and other equipment that student information may have passed through during our business and physically destroy old hard drives after it was erased of any content, using industry- standard software for this purpose.

We provide company owned computers with end-point protection against viruses, spyware

and other unauthorized intrusions. These computers are configured to disallow installation of

any software other than those installed by Coba Academy's IT Department. Our student application is secured by Secure Sockets Layer (SSL) for transmission between our network and our clients.

We immediately notify clients who transmit sensitive data specially Personally Identifiable Information (PII) by mistake such as but not limited to screenshots and emailing a student SSN.

We use a secure FTP server for file transmission between our network and our software vendor. If we must use email to transmit any data like those in spreadsheets, we use strong password to encrypt them and provide this password through a different means of communication like a phone call.

We shred papers containing student information so that the information cannot be read or reconstructed.

Detecting and Managing System Failures (SMB Techforce)

Effective security management requires Coba Academy to deter, detect, and defend against security breaches. That means taking reasonable steps to prevent attacks, quickly diagnosing a security incident, and having a plan in place for responding effectively.

- We monitor the websites of our software vendors and read relevant industry publications for news about emerging threats and available defenses.
- We maintain up-to-date and appropriate programs and controls to prevent unauthorized access to student information.
- We check with software vendors regularly to get and install patches that resolve software vulnerabilities.
- We use anti-virus and anti-spyware software that updates automatically. We maintain up-to-date firewalls.
- We regularly ensure that ports not used for our business are closed.
- We promptly pass along information and instructions to employees regarding any new

security risks or possible breaches.

- We use appropriate oversight or audit procedures to detect the improper disclosure or theft of student information.
- We keep logs of activity on our network and monitor them for signs of unauthorized access to student information.
- We use an up-to-date intrusion detection system to alert us of attacks.
- We monitor both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from our system to an unknown user.
- We take steps to preserve the security, confidentiality, and integrity of student information in the event of a breach.
- If a breach occurs, we take immediate action to secure any information that has or may have been compromised. (For example, if a computer connected to the Internet is compromised, disconnect the computer from the Internet).
- We preserve and review files or programs that may reveal how the breach occurred.
- If feasible and appropriate, we will bring in security professionals to help assess the reach as soon as possible.
- We will notify consumers, the U.S. Department of Education, law enforcement, and clients in the event of a security breach.

Technology Security Plan

I. Purpose

The purpose of this plan is to ensure the secure use and handling of all campus data, computer systems and computer equipment by Coba Academy (Coba) students, patrons, and employees.

II. Plan

A. It is the plan of Coba to support secure network systems, processes, and procedures, and to protect all personally identifiable or confidential information that is stored, on paper or digitally, in campus facilities or on campus-maintained servers, computers and networks. This plan supports efforts to mitigate threats

that may cause harm to the campus, its students, or its employees.

B. Data loss or compromises can be caused by human error, hardware malfunction, natural disaster, security breach, etc., and may not be completely preventable.

C. All persons who are granted access to the campus network and other technology resources are expected to be careful and aware of suspicious communications and unauthorized use of campus devices and the network. When an employee or other user becomes aware of suspicious activity, he/she is to immediately contact the campus Help Desk with relevant information.

D. This plan and procedure also cover third party vendors/contractors that house or have access to Coba personally identifiable information. All third-party entities will be required to sign the *Restriction on Use of Personally Identifiable or Confidential Information Agreement* before accessing Coba systems or receiving information.

E. It is the plan of Coba to fully conform to all federal and state privacy and data governance laws.

F. Professional development for staff and students regarding the importance of network security and best practices are included in the procedures. The procedures associated with this plan are consistent with guidelines provided by cyber security professionals worldwide. Coba supports the development and implementation of, and ongoing improvements for, a robust security system of hardware and software that is designed to protect Coba data, users, and electronic assets.

III. Definitions

A. **Access**: To directly or indirectly use, attempt to use, instruct, communicate with, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, computer network, or any means of communication with any of them.

B. **Authorization**: Having the express or implied consent or permission of the Vice President/IT Security Officer, or of the person authorized personnel, to give consent or permission to access personally identifiable information.

C. **Computer**: Any electronic device or communication facility that stores,

retrieves, processes, or transmits data.

D. **Computer network**: The interconnection of communication or telecommunication lines between computers; or computers and remote terminals; or the interconnection by wireless technology between computers; or computers and remote terminals.

E. **Confidential**: Data, text, or computer property that is protected by a security system that clearly evidences that the Program Coordinator or custodian intends that is not to be available to others without the owner's or custodian's permission.

F. **Encryption or encrypted data**: The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

G. **Personally Identifiable Information (PII)**: Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered protected data.

H. **Security system**: A computer, computer system, network, or computer property that has some form of access control technology implemented, such as encryption, password protection, other forced authentication, or access control designed to keep out unauthorized persons.

I. **Sensitive data**: Data that contains personally identifiable information.

J. **System level**: Access to the system that is considered full administrative access. Includes operating system access and hosted application access.

IV. Security Responsibility

A. Coba shall appoint an IT Security Officer (ISO) responsible for overseeing campus-wide IT security, to include development of campus policies and adherence to the standards defined in this document.

V. Training

A. Coba, led by the ISO, shall ensure that all campus employees having access to personally identifiable or confidential information undergo annual IT security training which emphasizes their personal responsibility for protecting student and

employee information. Training resources will be provided to all campus employees.

B. Coba, led by the ISO, shall ensure that all students are informed of Cyber Security Awareness.

VI. Physical Security

A. Computer Security

a. Coba shall ensure that any user's computer will not be left unattended and unlocked, especially when logged in to sensitive systems or data including student or employee information. Automatic log off, locks and password screen savers should be used to enforce this requirement.

b. Coba shall ensure that all equipment that contains sensitive information will be secured to deter theft.

B. Server/Network Room Security

a. Coba shall ensure that server rooms and telecommunication rooms/ closets are protected by appropriate access control which segregates

and restricts access from general school or campus office areas. Access control shall be enforced using either keys, electronic card readers, or similar method, with only those IT or other staff members requiring access necessary to perform their job functions allowed unescorted access.

b. Telecommunication rooms/closets may only remain unlocked or unsecured when, because of building design, it is impossible to do otherwise, or due to environmental problems that require the door to be opened.

C. Contractor access

a. Before any contractor is allowed access to any computer system, server room, or telecommunication room, the contractor will need to present a company-issued identification card, and his/her access will need to confirm directly by the authorized employee who issued the service request or by Coba's Technology Department.

CI. Network Security

A. Network perimeter controls will be implemented to regulate traffic moving between trusted internal (campus) resources and external, untrusted (Internet) entities. All network transmission of sensitive data shall require encryption where technologically feasible.

B. Network Segmentation

a. Coba shall ensure that all untrusted and public access computer networks are separated from main campus computer networks and utilize security policies to ensure the integrity of those computer networks.

b. Coba will utilize industry standards and current best practices to segment internal computer networks based on the data they contain. This will be done to prevent unauthorized users from accessing services unrelated to their job duties and to minimize potential damage from other compromised systems.

C. Wireless Networks

a. No wireless access point shall be installed on Coba's computer network that does not conform to current network standards as defined by the IT Support Company. Any exceptions to this must be approved directly in writing by the ISO.

b. Coba shall scan for and remove or disable any rogue wireless devices on a regular basis.

c. All wireless access networks shall conform to current best practices and shall utilize, at minimal, WPA encryption for any connections. Open access networks are not permitted, except on a temporary basis for events when deemed necessary.

D. Remote Access

a. Coba shall ensure that any remote access with connectivity to the campus internal network is achieved using the campus centralized VPN service, which is protected by multiple factor authentication systems. Any exception to this plan must be due to a service provider's technical requirements and must be approved by the ISO.

DI. Access Control

DII. System and application access will be granted based upon the least amount of access to data and programs required by the user, in accordance with a business need-to-have requirement.

DIII. Authentication

a. Coba shall enforce strong password management for employees, students, and contractors.
b. Password Creation
    i. All server system-level passwords must conform to the *Password Construction Guidelines* posted by the ISO internally.
c. Password Protection
    i. Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
    ii. Passwords must not be inserted into email messages or other forms of electronic communication.
    iii. Passwords must not be revealed over the phone to anyone.
    iv. Passwords must not be revealed or shared on questionnaires or security forms.
    v. User must not hint at the format of a password (for example, "my family name").
    vi. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

C. Authorization

a. Coba shall ensure that user access shall be limited to only those specific access requirements necessary to perform the user's job. Where possible, segregation of duties will be utilized to control authorization access.
b. Coba shall ensure that user access should be granted and/or terminated upon timely receipt, and management's approval, of a

documented access request/termination.

CI. Accounting

a. Coba shall ensure that audit and log files are maintained for at least 90 days for all critical security-relevant events such as: invalid logon attempts, changes to the security policy/configuration, and failed attempts to access objects by unauthorized users, etc.

CII. Administrative Access Controls

a. Coba shall limit IT administrator privileges (operating system, database, and applications) to the minimum number of staff required to perform these sensitive duties.

IX. Incident Management

a. Monitoring and responding to IT related incidents will be designed to provide early notification of events and rapid response and recovery from internal or external network or system attacks.

X. Business Continuity

a. To ensure continuous critical IT services, IT will develop a business continuity/disaster recovery plan appropriate for the size and complexity of campus IT operations.

b. Coba shall develop and deploy a campus-wide business continuity plan which should include as a minimum:

c. Backup Data: Procedures for performing routine daily/weekly/monthly backups, and for storing backup media at a secured location other than the server room or adjacent facilities. As a minimum, backup media must be stored off-site at a reasonably safe distance from the primary server room.

d. Secondary Locations: Identify a backup processing location, such as another school or campus building.

e. Emergency Procedures: Document a calling tree with emergency actions to include recovery of backup data, restoration of processing at the secondary location, and generation of student and employee listings for ensuring a full head count of all.

XI. Malicious Software

a. Server and workstation protection software will be deployed to identify and eradicate malicious software attacks such as viruses, spyware, and malware.
b. Coba shall install, distribute, and maintain spyware and virus protection software on all relevant campus-owned equipment, i.e., servers, workstations, and laptops.
c. Coba shall ensure that malicious software protection will include frequent update downloads (minimum weekly), frequent scanning (minimum weekly), and that malicious software protection is in active state (real time) on all operating servers/workstations.
d. Coba shall ensure that all security-relevant software patches (relevant workstations and servers) are applied within 30 days, and critical patches shall be applied as soon as possible.
e. All computers must use the relevant campus- approved anti-virus solution.
f. Any exceptions to section XI must be approved by the ISO.

XII. Internet Content Filtering

a. In accordance with federal and state law, Coba shall filter internet traffic for content defined in law as harmful to minors.
b. Coba acknowledges that technology-based filters are not always effective at eliminating harmful content and due to this, Coba uses a combination of technological means and supervisory means to protect students from harmful online content.
c. If students take devices home, Coba will provide a technology-based filtering solution for those devices. However, the campus relies on parents to provide the supervision necessary to fully protect students from accessing harmful online content.
d. Students are supervised when accessing the internet and using campus-owned devices on school property.

XIII. Data Privacy

XIV. Coba considers the protection of the data it collects on students, employees, and their families to be of the utmost importance.

XV. Coba protects student data in compliance with the GLB Act 16 CFR 314.

A. Coba shall ensure that access to employee records shall be limited to only those individuals who have specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.

XIV. Security Audit and Remediation

XV. Coba performs routine security and privacy audits in congruence with the campus *Information Technology Security Plan.*

A. Campus personnel develops remediation plans to address identified lapses that conforms to the campus *Information Technology Security Plan*.

XVI. Employee Disciplinary Actions

A. Employee disciplinary actions shall be in accordance with applicable laws, regulations and campus policies. Any employee found to be in violation may be subject to disciplinary action up to and including termination of employment with Coba Academy.

USERS and ACCESS

Information Systems	**Type of Service**	**Who Has Access**
Rafael Gonzales Management (RGM) System	Third Party Servicer	President, Vice President, School Treasurer, Director of Education, Financial Aid Director, Financial Aid Administrator, Admission's Representative
FA360	Third Party Servicer	School Treasurer, Vice President, Director of Education, Financial Aid Director, Financial Aid Administrator, Admission's Representative
Wright International Services (WIS)	Third Party Servicer – Default Management	Financial Aid Administrator
QuickBooks	Software	School Treasurer
NSLDS	Department of Education internet-based application	Financial Aid Administrator
Common Origination Disbursement (COD)	Department of Education internet-based application	Financial Aid Director, Financial Aid Administrator
SlickText	SMS	Vice President
GoToConnect	SMS	Vice President, Financial Aid Administrator, Admissions Representative
VA-Once	It is a completely Internet based application developed by a team of schools and **VA** representatives.	Vice President
Guest Vision	Locally installed on POS system. Serves as an ERP system.	Vice President & Guest Vision Support

Dropbox	Cloud based file share system. Used to upload photos of class work completed by distance learning students.	Vice President, Director of Education
Cima	Platform is used for distance learning and teaching.	Vice President, Director of Education, Instructors, Students