THE GRAMHAM-LEACH BLILEY ACT (GLBA) INFORMATION SECURITY POLICY

Gramm-Leach-Bliley Act Security Background

The Gramm-Leach-Bliley Act (GLBA) governs the use, sharing, and collection of financial information. GLBA requires financial institutions to take steps to protect customers' nonpublic personal information. Because Ohio Business College/Tri-State Educational Systems, Inc. participates in financial activities such as Title IV funding and making student loans, The Federal Trade Commission's regulation of FTC Safeguards Rule considers OBC a financial institution and subject to certain GLBA regulations. Higher education institutions must comply with the GLBA Safeguards Rule and Pretexting Provisions. They are exempt from the GLBA Privacy Rule because they must be compliant with the Family Educational Rights and Privacy Act (FERPA).

Purpose of the Policy

The purpose of the GLBA Information Security Plan is to outline how Ohio Business College complies with federal regulations related to the GLBA Safeguards Rule. The GLBA Information Security Plan primary objectives include:

- Ensuring the security and confidentiality of customer financial information
- Protect against any anticipated risks or threats to the security and integrity of covered data
- Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to the customer

Policy

Ohio Business College/Tri-State Educational Systems, Inc. will protect, to the extent reasonably possible, the privacy, security, and confidentiality of personally identifiable financial records and information. This policy applies to all personally identifiable financial records and information and covers employees and all other individuals or entities using these records and information for any reason. This policy also establishes an expectation that members of the Ohio Business College community act in accordance with this policy, relevant laws, contractual obligations, and the highest standards of ethics.

Policy Process

Definition of Terms used in the Policy Process:

- Security Plan Coordinator is the person assigned to coordinate the safeguards.
- Risk assessment is the plan to identify potential risks to customers information.
- Customer in the context of this policy, is identified as potential students, current students, parents of students, withdrawn students, graduated students.

- Customer Information refers to any record containing nonpublic, personally identifiable financial information about a customer of the college, whether in paper, electronic, or other form that Ohio Business College obtains from a student, a student's parent, or spouse, a college employee, alumnus, or any other third party in the process of offering a financial product or service.
- Financial Services in this context are the services offered and available to students to enroll or enrolled in college. This includes, but not limited to federal, state, and private college financial aid programs.
- Serviced Providers are defined as all third parties who receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to Ohio Business College and its students.
- FERPA is the Family Educational Rights and Privacy Act Policy

Security Plan Coordinator – Mr. Greg Schultz

Mr. Greg Schultz is the qualified IT Coordinator for Ohio Business College. Mr. Schultz works within each campus on data safeguards necessary. In this position Mr. Schultz will:

- Coordinate working in conjunction with third party Service Providers such as Radtech, Canvas, DiamondSIS, etc.
- Identify what data safeguards need to be put in place to conform to the GLBA requirements.
- Identify potential and actual risks to the security and privacy of covered data.
- Evaluate the effectiveness of current safeguards for controlling these risks.
- Design and implement additional required safeguards.
- Regularly monitor and test the Security Plan.
- Make sure staff and faculty are adequately trained on access to covered data and that existing policies and procedures that provide for the security of covered data are reviewed and adequate.
- Make recommendations for revisions to policy or the development of new policy, as appropriate.

Risk assessment

Mr. Schultz take steps to identify and assess internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of the current safeguards for controlling these risks. This includes paper/file documents, transferring/sharing documents virtually, fireproof file cabinets, backup of computer systems, controls in who and why they have access to student information.

Safeguards currently in place:

- Employ firewalls to protect all WAN connections
- Periodically check PCs to ensure software updates are applied to operating systems and any application programs.

- Employ antivirus on all systems on each campus.
- Network access-all users (staff, faculty, and students) have individual user accounts that provide unique usernames and passwords.
- Computer access accounts are disabled or passwords changed when employees are no longer employed with OBC. Student network access accounts are disabled.
- Staff and Faculty only have access to the network areas needed to perform their duties.
- Students do not have access to onsite network storage or other network file locations. Course materials are only available through Canvas or the cloud-based student learning management system.
- Open public WiFi is available to all persons on campus through the provided access password. This connection only provides internet access.
- A secured WiFi is available to allow access to onsite copiers and printers. This is granted on an as needed basis.
- The transferring of data between campuses through a shared drive is protected though a VPN, Virtual Private Network. The VPN is secured though Fortigate, hardware-based systems, maintain through Radtech.
- Radtech oversees the email server and the access of Staff and Faculty email accounts. Currently email can only be viewed from in network devices.
- Permission can be granted on approval for email access on a phone. The email is granted on a per user and per device basis. That is if a user had email on their phone allowed and then got a new phone, permission would be to be granted to allow the new phone to have access.
- Radtech creates all local computer user accounts for Dayton, Columbus and Middletown.
  Sandusky and Sheffield computer user accounts are created by Dee Bowersock and Greg Schultz. Sheffield server also hosts all staff and faculty user access accounts for Canvas.
- Students in Dayton and Columbus do not need credentials to access computers in Dayton, since the computers only allow access to the internet for Canvas and OSHAcademy. The PCs are set to not remember user accounts and passwords. User account credentials for access to Canvas are run through the Sheffield Campus server.
- Student Emails, all locations are run through a Microsoft Cloud based Azure servers. All student email accounts created by Dee Bowersock or Greg Schultz
- DiamondD, only certain individuals may request the creation of account to access DSIS. Currently, Melissa Warner and Greg Schultz have that capability. DSIS creates the user accounts that allows access to the remote databases. Also, when accounts are created, individuals are only given access to the databases needed for their position. User accounts are created in each database by Melissa Warner or Greg Schultz, the accounts inside of the database, restricts the users to the data they are allowed to see and/or manipulate based upon their job duties.
- Students have no access to DSIS unless they have a position with OBC and confirmed FERPA training.

- Backup devices and plans are in place. Redundant servers are employed to provide login reliability in the event of an equipment breakdown.
- Data backups of the local servers are performed nightly. Backup devices are rotated to provide redundancy and stored offsite in locked containers.
- DSIS (Diamond Student Information System) backups are conducted daily with continuous off-site rotation of backups.
- Canvas, the learning management system, which contains all the courses and student coursework has their own Disaster Recovery Plan and is audited by a third party each year.

Identify Potential and Actual Risks

When an actual or potential risk to covered data is identified, Mr. Schultz work with the corporate office and any third-party Service Providers to put a safeguard in place to alleviate that threat.

Annual Review of Security Plan

Mr. Schultz will do an annual evaluation of the Security Plan in order to determine where revisions, updates, deletions need to be made.

Family Educational Rights and Privacy Act (FERPA) Policy

Student educational records are official documents protected by the Family Educational Rights and Privacy Act (FERPA). The Family Education Rights and Privacy Act (FERPA) affords a student certain rights with respect to educational records. Copies of educational records or personally identifiable information concerning student records will not be released to anyone outside Ohio Business College, except as required or allowed by law, without the student's written consent. No provisions have been made for providing electronic signatures. Disclosures to school officials with legitimate educational interests are permitted without consent. A school official is a person employed by the school in an administrative, supervisory, academic or research, or support staff position; a person or company with whom the school has contracted (such as an attorney, auditor, or collection agent; or a student serving on an official committee or assisting another school official in performing his or her tasks.

Risks to security and confidentiality of information are assessed periodically and adjusted as deemed necessary and appropriate. According to the Family Education Rights and Privacy Act (FERPA), students have the right to inspect and review their educational records. To do so, a student must submit a written request to the Registrar, specifying the records desired and their location. The request will be granted as soon as practicable, but in no case more than 45 days after the request is received by the Registrar. Should a student request copies, they must identify what specific documents from their file they would like copied. There will be a $.25 per page charge.

In order to keep staff and faculty knowledge on the FERPA Policy, they do annual training in the fall each year.

Definition of Terms

Restricted access to directory or public information – Students have the right to restrict access to directory or public information. This request must be done in the Registrar's office. When a student restricts their directory or public information, that information will only be used to meet the direct educational needs of the student.

If a student requests restriction to their directory or public information, the college will respond to inquiries as follows: "We are not permitted under FERPA regulations to give out any information without the student's consent." If a student signs a consent form to release specific information, the college will only release information after verification of a picture identification.

Education record – any record maintained by the institution that is directly related to a student or students; any record that contains a student's name(s) or information from which an individual student can be personally (individually) identified; these records include: files, documents, and materials in whatever medium (handwriting, print, tapes, disks, film, microfilm, microfiche) which contain information directly related to students and from which students can be personally (individually) identified. The contents of an education record may appear in a variety of forms, such as: handwritten document, computer file, computer screen, printout, verbal exchange. Student information must be handled with care regardless of the form it is presented.

School official – a person employed by the college in an administrative, supervisory, academic research, or support staff position (including law enforcement and health staff personnel); a person elected to the Board of Trustees; a company employed by or under contract to the college to perform a special task such as the attorney, auditor, or collection agency; a student serving as an official. Campus Directors are designated as responsible for safeguarding all student records.

Directory or public information – Ohio Business College has designated the following information as Directory or Public Information:

- The following Directory information may be released by telephone:
    * Student's dates of attendance
    * Date of graduation and degree or diploma earned
- The following Directory Information will be released only in response to a written request:
    * Student's address
    * Telephone listing
    * Program of study
    * Awards received
    * Most recent previous education agency or previous institution attended
    * Photo
    * Honors received

Personally identifiable information – personally identifiable information includes, but is not limited to: student number; grades/exam scores; grade point average; social security number; parent address; parent phone; detail of registration information (i.e., courses, times); race; ethnicity; nationality; gender; date of birth; total credits; academic advisement; number of credits enrolled in a quarter; emergency contact; personal characteristics or other information which would make the student's identify easily traceable, bank and credit card account numbers, income and credit.

Grades can be issued to students only via their school issued student email "@students.ohiobusinesscollege.edu."

Sole possession notes – a record you never share with anyone else and that is maintained solely by you. Best advice – if you don't want it reviewed don't write it down.

The right to inspect and review records does not extend to personal notes of faculty or staff, medical treatment records, parents' financial records, and other documents of a confidential nature.

If, after inspecting the records, a student wishes to alter, correct, or delete inaccurate or misleading information that is believed to violate privacy or other rights, the student may request a correction or deletion in writing. If this request is denied, the student will be given a copy of the questioned records and may request a hearing in writing. The student will submit the request to the Campus Director specifying the portion of the record being questioned, the reason, and the desired change. A review of this request will be conducted within a reasonable time, and a written decision will be issued. If the student is not satisfied with the review results, he or she may submit written comments, which will be maintained with the questioned records.