Information Security Program

College Unbound's Information Security Program is designed to comply with the Gramm-Leach Bliley Act (GLBA). The program is designed to ensure the security and confidentiality of customer information in compliance with applicable GLBA rules as published by the Federal Trade Commission (16 CFR Part 314). It outlines administrative, physical, and technical safeguards to ensure compliance and safeguard against anticipated threats to the security or integrity of protected electronic data. The program also seeks to guard against unauthorized access to or use of protected data that could result in harm or inconvenience to any customer. Customers of College Unbound include prospective students, currently enrolled students and former students. The policy also covers electronic information about employees.

I. Coordination and Responsibility for the Information Security Program

The Coordinator of the Information Security Program is the Chief Information Officer (CIO) for College Unbound. The Coordinator is responsible for the development, implementation, and oversight of College Unbound's compliance with the policies and procedures required by the Gramm-Leach Bliley Act (GLBA) Safeguards Rule. Although ultimate responsibility for compliance lies with the Coordinator, various individuals and departments assist with its implementation and maintenance.

II. Risk Assessment and Safeguards

The College takes active steps to mitigate internal and external risks associated with storing digital data. The below steps are designed to minimize the risk that information is exposed to unauthorized parties, misused by any party, destroyed or otherwise compromised.

- To minimize risk, the College uses physical systems (locks, swipe cards, alarms and human security) to control physical access to computers and servers on its campus.
- To minimize risk, the College requires passwords on personal computers and servers that house protected customer information regardless of their location. Usernames and passwords are unique to the individual logging in.

- To minimize risk, all software systems that contain protected customer information require usernames and passwords to access. Usernames and passwords are unique to the individual logging in.
- To minimize risk, the College regularly reviews physical and administrative access to its systems that contain customer data and adjusts or removes access as appropriate. Accounts of terminated employees are either closed or otherwise adjusted to remove access to customer data.
- To minimize risk, the College practices the principle of least privilege that assigns users the minimal access to the system required to perform their duties.
- To minimize risk, the College requires system administrators and/or those with high levels of access to personally identifiable information (PII) to enable two-factor authentication in systems that offer it.
- To minimize risk, the College provides antivirus software on computers and servers.
- To minimize risk, the College continually applies security patches, antivirus and other updates to its computers and servers.
- To protect against unauthorized access and misuse, the College implements logging of access to all systems that offer logging ability.
- To guard against a disruption of data, the College, whenever possible, makes backups of key systems such as the student information system and stores them offsite.
- To guard against a disruption of data, the College ensures that all key systems have at least two system administrators.

III. Employee Training and Management

To perform their jobs, College employees have access to protected customer information. Employees must request access to systems with protected information and the request must be approved by the CIO or designee. Upon obtaining credentials, employees are informed that:

- information accessed must not be shared with third parties, including others in the organization not already authorized.
- accessing information is on a “need to know” basis and “curoristy” does not constitute a valid reason for accessing information.
- not to share usernames or passwords.
- advised of consequences - including termination of employment - resulting from unauthorized use of information.

Employees are also periodically reminded of phishing schemes and other social engineering tactics that seek to compromise accounts.

IV. Oversight of Service Providers

To carry out its mission the College engages third-party computer hardware and software vendors and requires they:

- have a written information security plan that outlines physical security, access control and backup procedures and meets the requirements of the Gramm-Leach Bliley Act
- have a process to securely backup and restore data
- Incorporate in the contract an acknowledgement of the confidentiality of student information under the Family Educational Rights and Privacy Act (FERPA) if the system contains student information

V. Offices Engaged in Processes Covered under GLBA

While all offices are instructed to take steps to protect customer data, the below offices have key roles in protecting customer data.

- Registrar (student biographical information, student academic records)
- Bursar (student biographical information, student financial records)
- Financial Aid (student biographical information, student financial records)
- Provost (student biographical information, student financial records)
- Human Resources/Payroll (employee biographical information)
- Information Technology (access to systems housing customer information)