Technology Requirements

The following lists the minimum recommended hardware and software requirements a student will need to successfully access Lakewood University's online academic programs:

- **Supported Operating Systems**
  - **Windows XP (service pack 3 for 32-bit, service pack 2 for 64-bit), Windows Vista, Windows 7, Windows 8, Windows 10**
  - **MAC OS X 10.6 (Snow Leopard) and Higher**
- **Audio: sound card and speakers or headphones for listening**
- **Internet connection: 56 Kbps (caution: videos may not play properly at this internet speed)**
- **Screen resolution: at least 800 x 600**
- **Internet browser: IE 9 or greater, Firefox 24 or greater, Chrome 32 or greater, Safari 5.1 or greater, browser set to accept cookies and to show the newest version of a page**
- **Media Player such Windows Media Player, Camtasia, or Vidster (all of which can be downloaded for free at the respective websites).**
- **Pop-up blocker must be disabled**

For optimal results the following is recommended:

- **Internet connection: Cable modem, DSL or better (required for high-quality video)**
- **Screen resolution: 1024 x 768**

****For degree program students the following is required*:**

- **Working webcam (for proctored exams)**
- **Working microphone (for proctored exams)**

Laptop Policy

Students who enroll at Lakewood University are eligible to receive a refurbished Chromebook laptop. Each enrolled student qualifies for one laptop per program. The refurbished Chromebook will be shipped to the student upon enrollment.

All necessary software to complete your program will be pre-installed on the laptop through Google Docs.

For any further inquiries or clarifications regarding this policy, please feel free to reach out to us.

Gramm Leach Bliley Act (GLBA) Information Security Plan

This Information Security Plan ("Plan") describes Lakewood University's safeguards to protect information and data ("Protected Information") in compliance with the Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. Section 6801. These safeguards:

- **Protect the security and confidentiality of Protected Information**
- **Protect against anticipated threats or hazards to the security or integrity of such information**
- **Protect against unauthorized access to, or use of, Protected Information that could result in substantial harm or inconvenience to any customer**

This Information Security Plan also provides for mechanisms to:

- **Identify and assess risks that may threaten Protected Information maintained by Lakewood University**
- **Designate employees responsible for coordinating the program**
- **Design and implement a safeguards program**
- **Manage the selection of appropriate service providers**

- **Adjust the Plan to reflect changes in technology, the sensitivity of protected Information, and internal or external threats to information security**
- **Reference related policies, standards, and guidelines**

See: https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

Identification and Assessment Risks to Customer Information

Lakewood University recognizes that it has both internal and external risks, which include, but are not limited to:

- **Unauthorized access of Protected Information by someone other than the owner of the covered data and information**
- **Compromised system security as a result of system access by an unauthorized person**
- **Interception of data during transmission**
- **Loss of data integrity**
- **Physical loss of data in a disaster**
- **Errors introduced into the system**
- **Corruption of data or systems**
- **Unauthorized access of covered data and information by employees**
- **Unauthorized requests for covered data and information**
- **Unauthorized access through hardcopy files or reports**
- **Unauthorized transfer of covered data and information through third parties**

Lakewood University recognizes that this may not be a complete list of the risks associated with the security of Protected Information. Since technology growth is not static, new risks are created regularly. Accordingly, the Information Technology Services (ITS), the Office of Student Success, and other designated stakeholders will actively participate with and seek advice from university representatives for identification of new risks. Risk assessments include advisory review for mitigation, acceptance of risk, gap analysis, or other appropriate review based on outcomes of the risk assessment on an annual basis. Lakewood University believes current safeguards used by the Information Technology Office are reasonable and, in light of current risk assessments, are sufficient to provide security and confidentiality to Protected Information maintained by the University.

Information Security Plan Coordinators

An internal committee is responsible for the maintenance of information security and privacy. The advisory committee will include representatives from the departments primarily responsible for safeguarding Protected Information. Each department responsible for safeguarding Protected Information will provide an annual update report indicating the status of its safeguarding procedures. The advisory committee is responsible for assessing the risks associated with unauthorized transfers of Protected Information and implementing procedures to minimize those risks that are appropriate based upon severity, complexity, and the nature and scope of its activities.

Design and Implementation of Safeguards Program

Employee Management and Training

In accordance with Lakewood University policies, standards, and guidelines, reference checking and background reviews are conducted for all new hires. During employee orientation, each new employee in departments that handle Protected Information are required to participate in several training sessions on the importance of confidentiality of Protected Information. They are also trained in the proper use of computer information and passwords. Departments responsible for maintaining Protected Information will also provide staff with updated training to minimize risk and safeguard data and maintain information security.

Physical Security

Lakewood University maintains physical security of Protected Information by limiting access to authorized employees who have signed an acknowledgement of their obligation to keep Protected Information private. Established procedures for the prompt reporting of the loss or theft of Protected Information must be followed. Offices and storage facilities that maintain Protected Information limit customer access and are appropriately secured. Paper documents that contain Protected Information are shredded at the time of disposal.

Information Systems

Information systems is an integration of hardware and software that forms a network used to collect, store, process, analyze and distribute data. Lakewood University has policies, standards, and guidelines governing the use of electronic resources and firewall and wireless policies. It takes reasonable and appropriate steps consistent with current technology to make sure that all Protected Information is secure during storage and encrypted during transmission.

Management of System Failures

Lakewood University maintains effective systems to prevent, detect, and respond to attacks, intrusions and other system failures. Such measures include:

- **Maintaining up-to-date anti-virus software**
- **Regularly obtaining and installing patches to correct software vulnerabilities**
- **Maintaining filtering or firewall technologies**
- **Alerting those with access to sensitive data of threats to security**
- **Imaging documents and shredding paper copies**
- **Backing up data regularly and storing it off site**
- **Observing other reasonable measures to protect our information systems.**

Selection of Appropriate Service Providers

Due to their specialized technology expertise, vendors may provide resources that Lakewood University can not provide on its own. A service provider that will maintain or access Protected Information must demonstrate the ability to safeguard Protected Information when being evaluated. Contracts with service providers may include the following requirements:

- **The Protected Information will be held in strict confidence and accessed only for the explicit business purpose of the contract**
- **The service provider has documented appropriate safeguards and controls (example, SOC2) to protect the sensitive information it receives, and that it must promptly report any security incidents that may affect our protected information**
- **A requirement (when appropriate) that the service provider maintain certain types of insurance to cover potential liability in the event of a security incident**
- **A requirement (when appropriate) that the service provider submit to audits of its information security and privacy policies, procedures, and controls.**

Continuing Evaluation and Adjustment

Due to constantly changing technology and evolving risks, this Information Security Plan will be subject to periodic review and adjustment. The coordinators, in consultation with the Office of General Counsel, will review the standards set forth in this policy and recommend updates and revisions as necessary. It may be necessary to adjust the plan to reflect changes in technology, the sensitivity of student and customer data, and internal or external threats to information security.

Policies, Standards, and Guidelines

GLBA Audit Requirements

FERPA