Gramm-Leach-Bliley Act

Purpose:

In order to be in compliance with the GLB Act, Davines Professional Academy of Beauty and Business will protect as reasonably as possible the privacy, security and confidentiality of personally identifiable records and information. Incorporated into this policy and procedure are the following goals:

- To ensure that employees only have access to the data they need to conduct school business
- To ensure the security, privacy and confidentiality of customer records and information
- To safeguard and prevent unauthorized access to financial records and information
- To comply with applicable federal, state and local regulations

Background:

The Gramm-Leach-Bliley (GLB) Act requires financial institutions to take steps to ensure the privacy, security and confidentiality of customer records. Because higher education institutions engage in financial activities, such as making Federal Perkins Loans, Federal Trade Commission (FTC) regulations consider them financial institutions for GLB Act purposes.

The GLB act dictates several specific requirements regarding the privacy of customer financial information. Under the regulations announced in May 2000, colleges and universities are deemed to be in compliance with the privacy provision of the GLB Act if they are in compliance with the Family Educational Right and Privacy Act (FERPA). However, higher education institutions are subject to the Safeguards Rule of the Act related to the administrative, technical, and physical safeguarding of customer information.

The Safeguards Rule of the **Gramm-Leach-Bliley Act (GLBA)** requires financial institutions to develop and maintain a security plan to protect the confidentiality and integrity of personal information. The college's program seeks to (1) ensure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. This program is a plan to assess existing risks to customer information including ways to manage and control the existing risks, and to monitor third-party outsourcing arrangements to ensure compliance with the college's policies and procedures.

Information Security Program:

The Information Security Program must include five main elements: designation of an employee(s) as coordinator of the information security program, identification of internal and external risks to the security and confidentiality of customer information and evaluation of current safeguards, employee training, oversight of service providers, and evaluation of the information security program.

1. Davines Professional Academy has designated as the GLB program coordinator Kelly Rendel-Wilmer, who is the Co-Director and Financial Aid Leader of the school. The program coordinator will be supported by Adam Bromberg, Marketing and Information Technology Director.

2. The school will conduct an annual security review and the program coordinators will identify anyone who works with covered data and information. The coordinators will also review procedures, incidents and responses quarterly.
3. The school is developing training and education for employees with access to covered data, including social security numbers and financial information.
4. Letters will be sent to all third- party servicers requesting assurance of GLB compliance.
5. Davines Professional Academy of Beauty and Business's Information Security Policy and Plan will be subject to periodic review and adjustment as required by GLB Act.

Procedure:

1. Employee Responsibilities and Access: The following restrictions apply to all personally identifiable financial records and information maintained by Davines Professional Academy of Beauty and Business and are meant to safeguard the security of these records and to maximize the integrity of the information. Davines employees are responsible for ensuring that, within their areas of responsibility, appropriate enforcement of the GLB program will be maintained.
2. Davines employees are granted access to those data and information resources required to carry out the responsibilities of their position and may not access additional resources without authorization (in other words, employees may not access customer information unless they have a need to know that information to perform their job duties).
3. Access is determined based on the duties and responsibilities of each position and each employee is responsible for protecting their means of access from misuse. (for example, employees must not share their username/password(s) with anyone else, or allow others to have access to their keys, etc.).
4. Employees shall not knowingly alter, destroy, or misuse customer information.
5. Employees must ensure that any release of customer information is conducted in an appropriate and secure manner (for example, employees should not release customer information without verifying the identity of the person(s) requesting the information, employees should use password protected file attachments and/or encrypted emails when transmitting confidential information, etc.).

Security Requirements:

1. All confidential student information files are kept in a locked filing cabinet in the Financial Aid Office which is always locked when the Financial Aid Leader is not on the premises.
2. Centralized computers and servers must have the appropriate level of physical and electronic security. (for example: passwords and anti-virus software)

Definitions:

The following definitions apply to this program:

Customer: an individual who has obtained a financial product or service from the school to be used primarily for personal, family or household purposes and who has a continuing relationship with the school. Examples of activities which create customer relationships with the school could include obtaining a loan from the school or having a loan for which the school has servicing rights or responsibility.

Customer Information: non-public personal information about an individual who has obtained a financial product or service from the school for personal, family or household reasons, that results in a continuing relationship with the school. Examples would be any extension of credit by the school for household, personal or family purposes, such as an extension of credit for tuition, fees, housing, medical services, etc; the making and/or servicing of loans and/or financial aid. These situations are subject to GLB, even if the individual ultimately is not awarded any financial aid or provided with a credit extension, in which case their non-public personal information would still be protected under GLB.

Information Security Program: A program developed, maintained and enforced by the office of Information Technology to ensure that the information assets of the university are maintained securely.

Service Provider:
any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its direct provision of services to the school.