Lamson Institute

Establishing and Maintaining an Information Security Program

Date: 06/23/2016
Policy Number: 06.23.2016
Category: Information Technology

Purpose of Policy
The Gramm-Leach-Bliley Act (Public Law 106-102) provides consumers the right to the protection of their nonpublic Personally Identifiable Information and requires financial institutions possessing such information about consumers to publish a privacy policy ("Policy") and implementing an Information Security Program (the "Program"). This Policy is published on the School's website and a notice of the web location is published in the School's catalog. This Information Security Program applies to Mikhail Education Corporation doing business as Advanced Training Institute and the three schools operated by the Institute for Business & Technology, Inc.; those being the Institute for Business and Technology, National Career Education and Lamson Institute.

General Privacy Policy
The School carefully protects all nonpublic personal information in our possession regarding students and their families. The School will not release nonpublic, private, personal, or financial information about our students or applicants to any third party, except as specifically provided in this policy. The School will release certain nonpublic personal information to federal and state agencies, government contractors, student loan providers/servicers, and other parties as necessary for the administration of the federal student aid programs, for enforcement purposes, for litigation, and for use in connection with audits or other investigations. Disclosure is permitted to law enforcement or emergency services agencies in the performance of their duties or when student safety or health may be in jeopardy. The School will not sell or otherwise make available personal information for marketing purposes to any third party at any time.

Protection of Personally Identifiable Information
The School employs office procedures and password-protected computer systems to ensure the security of paper and electronic records. The School does not disclose specifics of its internal security procedures to students or the general public to protect the effectiveness of those procedures.

Access to social security numbers and other Personally Identifiable Information is strictly limited to those School officials with a need-to-know. Each department director is responsible for enforcement of this Policy with regard to the information within his/her office. The Chief Operating Officer ("COO") is responsible for overall control of information release and will resolve any disagreements and make final decisions as necessary in accordance with this Policy.

The School's information is an important asset that is critical to providing an effective and comprehensive learning environment, openly communicating ideas, providing outstanding

community service, and supporting the School's operations and its offering of educational services. This information includes sensitive and personal student, faculty, and staff data as well as the School's operational data. To maintain effectiveness and protect individuals, the School's information assets must be protected from misuse, unavailability, destruction, and unauthorized disclosure or modification. The executive leadership of the School is committed to protecting the value of the School's information assets. Its IT Department is charged with establishing and maintaining a program that preserves the confidentiality, integrity, and availability of information and information systems. This responsibility is addressed by:

- Continually assessing risks and defining appropriate protection strategies.
- Complying with applicable legal and regulatory requirements.
- Protecting the reputation, image and competitive advantage of the School.
- Supporting the School's strategic mission and goals.
- Maintaining partnership with administrative units, faculty, and staff to ensure a collaborative approach to information security.

The IT Department deals with numerous threats and challenges including data loss or theft, malicious software (e.g., viruses, worms, Trojan horses), identity theft, social engineering, phishing scams, and other risks associated with new technologies. Security measures also must be implemented to comply with several laws and regulations that address student information (FERPA), financial information, individuals' privacy data and individuals' health information. The IT Department offers a wide range of services to address information security risks and requirements. These offerings are designed to balance strategic, tactical, and operational needs, and they include the following specific products and services:

- Security policies, procedures, standards, and methodologies.
- Security awareness and training.
- Legal and regulatory compliance.
- Security strategy, architecture, and technologies (including technologies to protect against malicious software).
- Technical system configurations and vulnerability management.
- Response to information security incidents or breaches.
- Security requirements for software development and acquisition.
- Disaster recovery and continuity planning.

Policies and procedures provide the foundation of an effective Information Security Program and define minimum requirements for protection of information. The IT Department has developed and implemented technologies that specify appropriate controls and conduct. These technologies have been approved by the School's COO, are applicable to all faculty, staff, and students, and they are required to be followed as follows:

Designation of Representative(s)

The School's Chief Operating Officer is designated as the Program Officer who is responsible for coordinating and overseeing this Information Security Program. The COO may designate other representatives of the School to oversee and coordinate particular elements of the Program. Questions regarding implementation or interpretation of the Program should be directed to the COO or her designee(s). Please note, the definition of a "customer" as used herein is anyone about whom the School collects, views, or keeps any type of financial information. Customers can be students, parents of students (or other relatives), employees, and vendors.

Program Objectives

- Protect the security and confidentiality of customer records and information.
- Identify and assess the risks to student information in each relevant area and evaluate the effectiveness of the current safeguards for controlling these risks.
- Select appropriate service providers and contract with them to implement safeguards.
- Evaluate, test and monitor the Program and make changes as necessary

Risk Assessment

The following is a list of potential threats to customer financial information that the Program is intended to mitigate.

1) Unauthorized access to data through software applications.
2) Unauthorized use of another information system user's account and password.
3) Unauthorized viewing of printed or computer displayed customer financial information.
4) Improper storage of printed customer financial data information.
5) Improper destruction of printed material that contains customer financial information.

Information Security Program Components

1) Access to the School's information systems is limited to authorized personnel. Authorized personnel are assigned a username and a password to gain access to the appropriate information system. Approval for access to the various modules in the School's information systems is given by different managers. For example, access to the financial aid information system requires the Financial Aid Director's approval and access to the School's salary information system requires authorization by the Controller.
2) Passwords may not be shared.
3) Students requiring access to customer financial information are given their own account and password with appropriate privileges assigned.
4) Computer terminals used to display customer financial information are not to be left unattended with customer financial information displayed.
5) In unsecured areas, all users must log off their computer terminals when they are away from their work area.
6) Computer terminals are to be placed to prevent casual viewing by unauthorized personnel.
7) Entry access to the Business Office, Financial Aid Office, Registrar's Office, and other offices in the School are limited to authorized personnel.
8) Printed copies of customer financial information are to be handled only by authorized personnel and kept in areas with restricted access.
9) Printed financial documentation and information of customers (including, but not limited to, credit card information, social security information, including social security numbers, bank information, loan information, salary and other personal financial information) must be kept secured at all times. This type of information cannot be left in full view of unauthorized individuals. Records with customer financial information are located in a number of areas, including, but not limited to, filing cabinets, folders, information from emails, information from phone calls whether verbal or written, binders, cash drawers, credit card machines, information in computer documents. Access to these areas is limited to authorized personnel.
10) Customer financial information, regardless of where the information is housed or how it is kept (in computer systems/programs, email, paper copies, etc.), is confidential and is not available to anyone except those who have a legitimate purpose for the information that is related to the School's mission. The following are examples of customer financial information that is confidential. This is not all inclusive:
    - Salary and benefit information for an employee.

- Wage information for students.
- Social Security Numbers (employees, students, vendors, etc.).
- Credit Card Information.
- Loan Information.
- Bank Information.
- Dates of Birth.
- Home addresses and phone numbers.

11) Offices must be kept locked when unattended or unsupervised.
12) Fraudulent attempts to obtain information will be reported to the appropriate office/individual.

Consequences
Disciplinary measures for employees, up to and including termination, may be imposed for breaches of the security components of this Program. Disciplinary measures for students, up to and including termination of enrollment, may be imposed for breaches of the security components of this Program.

Information Systems Management
The School's IT Department is tasked with providing effective security management to prevent, detect and respond to attacks of intrusion or other system failures. The IT Department provides the following security measures:

- Maintain up-to-date firewalls.
- Provide appropriate antivirus software that can be updated automatically.
- Keep the Schools electronic information systems updated with patches, new releases, etc., as appropriate.
- Backup customer information daily and keep weekly backups off site at a secured location and protected against destruction or damage.
- Allow only approved users access.
- Notify users about any security risks or breaches.
- Use a password protected system.
- When transferring data from one computer to another, erase data from former computer.

Monitoring and Testing
This Program shall be reviewed periodically and adjusted as and when necessary. The most frequent of these reviews should occur within the IT Department, which will monitor software updates and new releases for security software and implement appropriate upgrades and new releases in a timely fashion. In addition, the COO shall hold such formal and informal meetings with appropriate employees and IT Department staff on an "as needed basis" to review the effectiveness of the Program and revise as necessary. Any suspected information security breach or issue should be reported immediately to the IT Department.