

Delaware Learning Institute of Cosmetology Information Security Plan

Background

This Information Security Plan (“Plan”) describes Delaware Learning Institute of Cosmetology’s (“DLIC”) safeguards to protect covered data and information. These safeguards are provided to:

- Ensure the security and confidentiality of covered data and information;
- Protect against anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of covered data and information that result in substantial harm or inconvenience to any student, employee or customer.

This Information Security Plan also provides for mechanisms to:

- Identify and assess the risks that may threaten covered data and information maintained by DLIC;
- Develop written policies and procedures to manage and control these risks;
- Implement and review the plan; and
- Adjust the plan to reflect changes in technology, the sensitivity of covered data and information and internal or external threats to information security.

“Covered data” is defined as educational records, and the personal and financial information of students, prospective students, faculty members, staff members, alumni and customers. When in doubt as to whether a piece of data or information is to be safeguarded as covered data and information, DLIC employees/contractors will err on the side that it is covered data and information. It includes data maintained at DLIC as well as centrally-stored data, regardless of the media on which they reside. Employees are charged with safeguarding the integrity, accuracy, and confidentiality of covered data and information as part of the condition of employment.

DLIC recognizes that it has both internal and external risks. These risks include, but are not limited to:

- Unauthorized access of covered data and 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

DLIC recognizes that this may not be a complete list of the risks associated with the protection of covered data and information. Because technology growth is not static, new risks are created regularly. Accordingly, DLIC works with information technology vendors to actively monitor for identification of new risks. DLIC believes its current safeguards are reasonable and, in light of DLIC's current risk assessments are sufficient to provide security and confidentiality to covered data and information maintained by DLIC. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information.

As required by the Student Aid Internet Gateway (SAIG) Enrollment Agreement entered into by DLIC, DLIC must ensure that all Federal Student Aid (FSA) applicant information is protected from access by or disclosure to unauthorized personnel. Under various Federal and state laws and other authorities, including the Higher Education Act of 1965, as amended ("HEA"); the Family Educational Rights and Privacy Act (FERPA); the Privacy Act of 1974, as amended; the Gramm-Leach-Bliley Act; state data breach and privacy laws; and potentially other laws, DLIC may be responsible for losses, fines and penalties (including criminal penalties) caused by data breaches.

The HEA also requires DLIC to maintain appropriate institutional capability for the sound administration of the Title IV programs. Such capability includes satisfactory policies, safeguards, monitoring and management practices related to information security. Further, FERPA generally prohibits institutions from having policies or practices that permit the disclosure of education records or personally identifiable information contained therein without the written consent of the student, unless an exception applies. Any data breach resulting from a failure of an institution to maintain appropriate and reasonable information security policies and safeguards could also constitute a FERPA violation.

To support the expectation and the SAIG requirements described above, DLIC is committed to follow industry standards and best practices in managing information and information systems and in securing covered data, including personally identifiable information.

Designated Security Program Officer

John Cook is the designated Security Program Officer for DLIC. All correspondence and inquiries about DLIC's Information Security Plan should be directed to Mr. Cook.

Student Privacy Provisions & Access to Cumulative Records

DLIC respects each student's right to privacy, and acts in accordance with the Family Educational Rights and Privacy Act (FERPA) of 1974. FERPA provides students certain rights with respect to the student access to and amendment of educational records and governs when DLIC can disclose educational records without student consent. FERPA also provides students with the right to complain to the U.S. Department of Education if the student believes DLIC is

not in compliance with the statute and governs when DLIC can disclose directory information about students.

FERPA generally requires that DLIC have the student's written permission to release any information from their records except certain types of "directory information." Certain information, classified as "directory information," is available for public consumption unless the student specifically directs that it be withheld. The student may direct DLIC not to disclose such information. Public directory information as defined by FERPA includes: student's name, telephone number, honors and awards and dates of attendance. However, DLIC will notify parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them.

Students seeking access to their records should submit a written request that identifies the record or records they wish to inspect to DLIC's School Director. DLIC will arrange for access and notify the student of the time and place where the records may be inspected. DLIC may charge a reasonable fee for copies of student records

In accordance with FERPA, DLIC will disclose information from the academic records of a student to authorized persons, provided DLIC has on file written consent of the student. The form is available from DLIC's Director of Education. A student must submit a written consent for each third-party request for information.

Security Provisions

The DLIC Information Security Plan herein is designed to ensure the security, integrity, and confidentiality of covered data, including but not limited to non-public personally identifiable information, protecting it against anticipated threats, and guarding it against unauthorized access or use. Covered under the Plan are administrative, technical, and physical safeguards used in the collection, distribution, processing, protection, storage, use, transmission, handling, or disposal of covered data. The Plan covers actions by both employees of DLIC and outside service providers.

DLIC uses direct personal control or direct supervision to control access to and handling of all covered data when an office is open. Whether the information is stored in paper form or any electronically accessible format, covered data is maintained, stored, transmitted and otherwise handled under the direct personal control of an authorized employee of DLIC.

Covered data is collected, processed, transmitted, distributed and ultimately disposed of with constant attention to its privacy and security. Conversations concerning covered data are held in private. Papers with covered data are mailed via US mail, or private mail carrier. When best practices permit the disposal of non-public information, it is destroyed; paper containing such information is routinely shredded or otherwise destroyed.

DLIC employees are required to password-protect electronic files of non-public personally identifiable information when transmitting electronically.

Confidential material is kept secure. Most offices have locked windows and locked doors with restricted access. For those that do not, materials are kept in locked filing cabinets or other locked storage areas. When offices are open, confidential information is kept out of sight from visitors, and computer screens are not visible to visitors. Offices and/or computers are locked when the office will be vacant for an extended length of time.

Key access is limited to authorized DLIC employees only, and DLIC's School Director governs the distribution of keys. DLIC's School Director further ensures the security of offices at the campus after hours.

Employee Management and Training

All DLIC employees, including part-time and temporary employees, are given specific training by their supervisors about issues of security of sensitive and confidential material used in their respective offices. Employees are held accountable to know that although they have access to non-public information in order to perform their duties for DLIC, they are not permitted to access it for unapproved purposes or disclose it to unauthorized persons. The Employee Handbook, which is provided to all employees, states that violation of security policies could result in termination of employment or legal action, or both.

Outside Service Providers

Third party service providers are required to maintain appropriate safeguards for nonpublic information to which they have access. Contracts with service providers, who within their contracts have access to DLIC's non-public student, prospective student, employee and/or customer information, shall include the following provisions as appropriate:

- Explicit acknowledgment that the contract allows the contract partner access to confidential information;
- Specific definition of the confidential information being provided;
- Stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- Guarantee from the contract partner that it will ensure compliance with the protective conditions outlined in the contract;
- Guarantee from the contract partner that it will protect the confidential information it accesses according to commercially acceptable standards and no less rigorously than it protects its own customers' confidential information;
- Provision allowing for the return or destruction of all confidential information received by the contract partner upon completion of the contract;
- Stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles DLIC to immediately terminate the contract without penalty;

- Provision allowing auditing of the contract partners' compliance with the contract safeguard requirements;
- Provision ensuring that the contract's protective requirements shall survive any termination agreement.

If DLIC has entered into an arrangement with an outside servicer provider, note that Federal regulation 34 CFR §668.25 includes a provision that DLIC remains liable for any action by its third-party servicers.

Reassessment of Plan

This Plan is reviewed at least annually and adjusted as needed. The School Director shall circulate this policy to DLIC's advisory board and request a reassessment. The annual review includes identification and assessment of internal and external risks to the security, integrity, and confidentiality of non-public personally identifiable information, including review of outside contractors and their contracts to ensure that proper safeguards are in place.

Information Technology Systems Practices/Policies:

Access to covered data and information via DLIC's computer information system is limited to those employees who have a business reason to know such information. Each employee is assigned a user name and password. Databases containing personal covered data and information, including, but not limited to, accounts, balances, and transactional information, are available only to DLIC employees in appropriate departments and positions. Account and password information is only provided after receipt of documentation from the appropriate supervisor. DLIC will take reasonable and appropriate steps consistent with current technological developments to make sure that all covered data and information is secure and to safeguard the integrity of records in storage and transmission. User and system passwords are required to comply with DLIC's password policy described below. When commercially reasonable, encryption technology will be utilized for both storage and transmission. All covered data and information will be maintained on servers that are either behind DLIC's firewall or stored in cloud-based data storage solutions with vendors whose data security systems comply with this Policy. All firewall software and hardware maintained by DLIC will be kept current.

Student Information System: DLIC utilizes Genesis school management system. DLIC's Security Program Officer is responsible for authorizing system access to Genesis school management system. Each employee's new hire paperwork will indicate whether the employee is authorized to have access to Genesis school management system and, if so, the access credentials to be provided. For example, employees in DLIC's education office will be provided full access to the Genesis school management system student profile database (exclusive of user administration). Access for instructors will generally be limited to student grades and attendance records and will exclude access to student personally identifiable information (including but not limited to financial aid information). Each employee's access will be determined by the Security Program Officer and the employee's supervisor in consideration of the employee's job responsibilities.

System privileges are authorized by the Security Program Officer. Staff granted access to institutional data may do so only to conduct DLIC business. In this regard, employees must:

- Respect the confidentiality and privacy of individuals whose records they access
- Observe ethical restrictions that apply to the data to which they have access
- Abide by applicable laws or policies with respect to access, use, or disclosure of information

Employees may not:

- Disclose data to others, except as required by their job responsibilities
- Use data for their own personal gain, nor for the gain or profit of others
- Access data to satisfy their personal curiosity

Employees and students who violate this policy are subject to the investigative and disciplinary procedures of DLIC. DLIC's President handles complaints against students as well as complaints against staff and administrators.

Access to information technology systems is granted based on the employee's need to use specific data, as defined by job duties, and subject to appropriate approval. ***As such, this access cannot be shared, transferred or delegated.*** Failure to protect these resources may result in disciplinary measures being taken against the employee, up to and including termination.

Employee Information

All aspects of personnel records are confidential. Directory information for employees is public. Directory information may include some or all of the following: name, department, position title, DLIC address, DLIC phone and email address. Employees may request that this data be classified as confidential. All other employee related data must be vigilantly safeguarded and treated as confidential.

Passwords

Administrative information is protected through the vigilant use of user-defined passwords. Passwords must be:

- Consist of both letters and numbers
- Eight characters in length, minimum
- Individuals are expected to protect passwords from disclosure. Every individual must have a unique user login.

Communication to New Employees

DLIC's President or the Security Program Officer is responsible for discussing this policy with each employee at the time system privileges are issued. Effective, on-going communication of this security policy along with instruction regarding office procedures is the responsibility of DLIC's Security Program Officer.

Unauthorized Disclosure of Covered Information

DLIC's SAIG Agreement includes a provision that in the event of an unauthorized disclosure or an actual or suspected breach of applicant information or other sensitive information (such as personally identifiable information) DLIC must immediately notify the U.S. Department of Education Federal Student Aid at CPDLICIG@ed.gov. The Security Program Officer shall notify the President of DLIC that an unauthorized disclosure or suspected breach of applicant information or other sensitive information has occurred. The President, working with the Security Program Officer, shall then submit the required notification to FSA as required under the SAIG Agreement.

[Page intentionally blank]

EMPLOYEE GUIDELINES FOR SECURING COVERED DATA AND INFORMATION:

“Covered Data” is defined as educational records, and the personal and financial information of students, prospective students, faculty members, staff members, alumni and customers. When in doubt as to whether a piece of data or information is to be safeguarded as covered data and information, DLIC employees/contractors will err on the side that it is covered data and information. Covered data and information includes both paper and electronic records. Examples of personal and financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories, and social security numbers.

Every DLIC employee who has access to covered data and information is responsible for:

1. Maintaining physical security by locking rooms and/or file cabinets where covered data and information is stored. Ensuring windows are locked and using safes when practicable for especially sensitive covered data and information.
2. Maintaining adequate key control and limiting access to sensitive areas to those individuals with a “need to know” in order to perform their job.
3. Using passwords to access automated systems that process covered data and information. Also encouraging the use of “strong” passwords (e.g. at least 8 characters, and not easily guessable). Also encouraging the safeguarding of passwords (e.g. do not leave passwords written down in easy view of others in the vicinity of an employee’s work area).
4. Using firewalls and encrypting covered data and information when appropriate and feasible.
5. Referring calls and mail requesting covered data and information to those individuals who have been trained in safeguarding covered data and information for these types of requests.
6. Shredding and erasing customer information when no longer needed in accordance with DLIC policy.
7. Taking reasonable efforts to limit the view of computer screens and other mediums (e.g. paper) displaying covered data and information to only those employees who have a “need to know” in order to perform their job.
8. Erasing covered data and information from computer screens when it is no longer in use. And never leave your desk area with covered data and information still displayed on a computer screen or on some other medium (e.g. paper) on the desk in clear site of a casual passerby.
9. Encouraging employees to report suspicious activity to supervisors and/or DLIC’s Director, as appropriate.
10. Encouraging password-activated screen savers and using them when an employee is away from his/her desk.
11. Taking reasonable steps to ensure that all future contracts are with service providers that are capable of maintaining appropriate safeguards for the covered data and information at issue.

Disciplinary measures (including job termination) may be taken against any employee who intentionally, or through gross negligence, violates any of the above guidelines.

Statement of Understanding

Please read the following information and sign this form at the bottom indicating your agreement to comply with students' privacy rights as protected by the Family Educational Rights and Privacy Act (FERPA) and the Gramm-Leach-Bliley Act (GLBA). Return this form to DLIC's School Director.

Family Education Rights and Privacy Act ("FERPA")

The purpose of the Family Educational Rights and Privacy Act is to afford certain rights to students concerning their education records, and one of these FERPA rights is to have some control over the disclosure of personally identifiable information from their records. Personally identifiable information contained in education records may not be disclosed without the student's written consent except to school officials whom DLIC has determined have a legitimate educational interest.

Legitimate Educational Interest means the demonstrated need to know by those officials of an institution who act in the student's educational interest, including faculty, administration, professional staff and other designated staff.

Information that cannot be disclosed without a student's written consent:

- Name of the student in combination with any of the following items,
- Student's parents or other family member,
- Student or family address,
- Student's Social Security number, Personal Identification Number (PIN) or other identifying number,
- Student's schedule,
- List of personal characteristics (such as gender, race, ethnicity or religion),
- Grading or attendance information
- Other information that could make the student's identity easily traceable.

Gramm-Leach-Bliley Act ("GLBA")

The purpose of the GLBA is to afford certain rights to students, faculty members, staff members and alumni concerning their personal and financial information. A focus of GLBA is to control the disclosure of personally identifiable information maintained by DLIC in the necessary course of business. Institutions may not disclose personally identifiable information, without the student's, faculty member's, staff member's or alumni's written consent except to school officials whom the institution has determined to have a legitimate interest.

ACCEPTANCE OF RESPONSIBILITY

I understand that DLIC maintains personally identifiable information for students, prospective students, faculty members, staff members, alumni and customers, disclosure of which is prohibited by the Family Education Rights and Privacy Act and the Gramm-Leach-Bliley Act. I acknowledge that I fully understand that the intentional disclosure by me of this information to any unauthorized person could subject me to criminal and civil penalties imposed by law. I further acknowledge that such willful or unauthorized disclosure of student information also violates DLIC policies and could constitute just cause for disciplinary action including termination of my employment regardless of whether criminal or civil penalties are imposed.

I also understand that I am liable for any unauthorized use of, or access to, information protected by FERPA and GLBA by any other person accessing information via my password due to my own negligence or carelessness.

Name

Signature

Date