College of DuPage

Information Technology

Information Security Plan

May, 2023

TABLE OF CONTENTS

Purpose

This information security plan ("Plan") describes the College of DuPage's ongoing efforts to secure and safeguard *covered data and information / customer information*[1].

The College is required by law, specifically the Gramm-Leach-Bliley Act, to:

1. Designate an information security plan coordinator to oversee the safeguarding of covered data and information.
2. Identify and assess risks to covered data and information.
3. Provides for the design and implementation of safeguards to control the risks the College of DuPage identifies through its risk assessment
4. Regularly monitor and test the effectiveness of the safeguards implemented in this Information Security Plan
5. Provides for the implementation of policies and procedures to ensure that personnel are able to enact the information security program.
6. Oversee service providers and contractors and require them to demonstrate the same safeguards to covered data and information (after May 2004).
7. Periodically monitor, evaluate, improve, and implement changes to this COD Information Security Plan.
8. Design, develop, implement, and maintain an incident response plan that provides a well-defined, organized approach for handling any potential unauthorized access/breach of sensitive data (covered data and information) at the College of DuPage.
9. Designate a qualified Individual to report regularly and at least annually to those with control over the institution regarding the institution's information security program

This COD information security plan ("Plan") also makes good business sense. This plan ensures that the students, employees, etc. are confident that the college is taking adequate steps to protect their information and to minimize loss in the event of a security breach. The plan also serves to deter an increasingly common crime nationwide– identity theft.

[1] *Covered data and information / customer information* for the purpose of this policy includes student personal and financial information required to be protected under the Gramm-Leach-Bliley (GLB) Act and the Family Educational Rights and Privacy Act (FERPA). In addition to educational records and student personal and financial information, the College of DuPage chooses as a matter of policy to also include personal and financial information on faculty members, staff members, alumni, and other donors in the definition of *covered data and information*. When in doubt as to whether a piece of data or information is to be covered, COD 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.

Information Security Plan (ISP) Coordinator(s) (E1)

The Director of Information Technology or his/her designee will be the Information Security Plan (ISP) Coordinator. He/She is responsible for overseeing that the nine (9) list items in the previous section ("Purpose") are carried out and completed.

Identify and assess risks to covered data and information (E2)

The College of DuPage 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
- 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 thru hardcopy files or reports
- Unauthorized transfer of covered data and information thru third parties

The College of DuPage recognizes that this may not be a complete list of the risks associated with the protection of covered data and information. Since technology growth is not static, new risks are created regularly. Accordingly, the Information Security Plan Coordinator will actively participate and monitor industry advisory groups for the identification of new risks.

The College of DuPage believes that the current Information Technology (IT) department safeguards are reasonable and, in light of current IT risk assessments are sufficient to provide security and confidentiality to covered data and information stored and maintained on computer systems. Additionally, these safeguards protect against currently anticipated threats to the integrity of covered data and information stored and maintained on computer systems.

Safeguards to Control the Risks the College of DuPage has Identified through Risk Assessment (E3)

Safeguards have been designed and implemented to control the risks identified through the risk assessment. These safeguards include the following:

1. Implementing and periodically reviewing access controls, including technical and, as appropriate, physical controls to (a) authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information and (b) limit authorized users' access only to customer information that is necessary to perform their duties and functions;
2. Identifying and managing the data, personnel, devices, systems, and facilities that enable the College to achieve its business purposes in accordance with their relative importance to business objectives and risk strategy;
3. Encrypting all covered data and information held or transmitted both in transit over external networks and at rest. If the College determines that the encryption of sensitive information, either in transit over external networks or at rest, is not feasible, then the College may instead secure such customer information using effective alternative compensating controls as reviewed and approved by the Information Technology (IT) dept.;
4. Using secure development practices for in-house developed applications utilized by the College for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications utilized to transmit, access, or store customer information;
5. Implementing multi-factor authentication for all individuals accessing any information system, unless the IT dept. has approved in writing the use of reasonably equivalent or more secure access controls;
6. Following the developed, implemented, and maintained procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained;
7. Periodically reviewing the retention policy to minimize the unnecessary retention of data;
8. Following the College's adopted procedures for change management; and
9. Utilizing the implemented policies, procedures and controls designed to monitor and log the activity of authorized users and detect unauthorized access to, use of, or tampering with customer information by such users.

Additionally each Department Head will be responsible for making sure all employees understand and are committed to practice the following guidelines. Department staff members are responsible for abiding with the following guidelines.

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 and frequently changing passwords to access automated systems that process covered data and information. Also encouraging the use of "strong" passwords (e.g. at least 6 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 employees work area).
4. 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.
5. Shredding and erasing customer information when no longer needed in accordance with Department / College policy.
6. 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.
7. 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.
8. Encouraging employees to report suspicious activity to supervisors and/or the COD Police Department, as appropriate.
9. Encouraging password-activated screen savers and using them when an employee is away from his/her desk.
10. 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.

Appropriate disciplinary measures may result against employees who violate any part of the guidelines set forth in this Information Security Plan, Policy, or Procedure.

Periodically monitor, evaluate, improve, and implement changes to this COD Information Security Plan (E4 / E7)

The Information Security Plan (ISP) Coordinator, working in conjunction with each department, must continually assess the vulnerabilities of their systems. At least annually, the Information Security Plan Coordinator will review the COD Information Security Plan and make all required changes. If changes have to be made, a new copy of the plan will be updated on the IT department webpage. It will be the responsibility of each department to implement changes within their department (if any) to be in compliance with changes to the plan. The ISP Coordinator and the following COD departments are available to assist in assessing the efficacy of their existing safeguards and in proposing improvements. The COD Police Department is available to discuss physical security issues. The COD Information Technology (IT) department is available to provide consulting on cyber-security and other computer related security issues. The director of admission services and/or registrar is available to consult on the privacy of student education records (FERPA). The Information Security Plan Coordinator will assure that the COD Information Security Plan is reflective of those practiced at other community colleges and universities, as measured by industry security advisory groups.

Policies and procedures are implemented to ensure that personnel are able to enact the College's Information Security Plan by: (E5)

1. Utilizing the Office of Information Technology's (OIT) qualified information security personnel to manage the information security risks and to perform or oversee appropriate aspects of the information security program;
2. Providing information security personnel with security updates and training sufficient to address relevant security risks; and
3. Verifying that key information security personnel take steps to maintain current knowledge of changing information, security threats, and countermeasures.
4. Providing employees with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;

EMPLOYEE SECURITY AWARENESS TRAINING INCLUDES:

- Background checks of new employees working in areas that regularly work with covered data and information are done by the Human Resources (HR) department or the hiring department.
- During new employee orientation, each new employee will receive information on the importance of the confidentiality of covered data and information.
- Existing employees will receive information on the importance of the confidentiality of covered data and information.

- Annual awareness and updates will be provided to employees on the importance of the confidentiality of covered data and information (see below).

The awareness program will also include controls and procedures to prevent employees from providing covered data and information to unauthorized individuals, including "pretext calling"[2], and how to properly dispose of documents and electronic records that contain covered data and information. Appendix A can be used to provide awareness and get confirmation that employees understand and intend to practice the safe handling of covered data and information in accordance with this Information Security Plan.

ON-GOING EMPLOYEE SECURITY AWARENESS TRAINING

- The ISP Coordinator will be responsible for making a reasonable effort to distribute annual awareness and updates to all employees that have access to covered data and information and that they understand what is required of them to practice safe handling of covered data and information as outlined in this Information Security Plan.
- Area Administrators responsible for maintaining and safeguarding covered data and information must take reasonable steps, depending on the media form on which covered data and information resides, to protect the information from unauthorized access, destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures.

Oversee Service Providers and Contracts and Require Them to Demonstrate the Same Safeguards to Covered Data and Information (E6)

Due to the specialized expertise needed to design, implement, service, and use new technologies and business tools, vendors may be needed to provide resources that the College of DuPage (COD) chooses not to provide. In the process of choosing a service provider that will maintain or regularly access covered data and information, the evaluation process shall include the ability of the service provider to abide with the safeguards outlined in this COD Information Security Plan. COD Legal Counsel is available to help with such contracts if needed.

[2] "Pretext calling" occurs when an individual improperly obtains covered data and information so as to be able to commit identity theft. It is accomplished by contacting a College of DuPage (COD) employee posing as someone authorized to have access to covered data and information, and through trickery and deceit, convince the COD employee to release the covered data and information to them.

Design, Develop, Implement, and Maintain an Incident Response Plan (E8)

MANAGEMENT OF SYSTEM FAILURES:
The COD IT department has developed written plans and procedures to detect any actual or attempted attacks to COD computer systems and has an Incident Response Policy that outlines procedures for responding to an actual or attempted unauthorized access to covered data and information.

Departments must immediately report significant failures of their safeguarding system to the COD Information Security Plan Coordinator(s) and the COD Police Department, if appropriate. Affected customers may also need to be notified after the Department unit consults with the COD Police Department, the COD Information Security Plan Coordinator(s), and COD Legal Counsel. Examples of significant failures would include a successful IT hacking effort, a burglary, or impersonations leading to unauthorized access to covered data and information.

Designate a Qualified Individual to Regularly Report Information Security Plan Status to the College Administration (E9)

The ISP Coordinator will report in writing, regularly and at least annually, to the College Administration. The report shall include the following information:

1. The overall status of the Information Security Plan and the College's compliance with this ISP; and
2. Material matters related to the Information Security Plan, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the Information Security Plan.

Supplemental Policies & Guidelines

The following policies and procedures and references supplement and help to create a comprehensive information security plan. Referral and adherence to these documents is imperative to the overall protection of covered data and information. The following documents are incorporated by reference into this document.

1. COD Policy Manual of the Board of Trustees, Policy No. 4.02, 4.03, 5.12, 3.50, 3.51, 3.52, 3.53
2. Federal Trade Commission 16 CFR Part 314 “Standards for Safeguarding Customer Information; Final Rule”

APPENDIX A

EMPLOYEE GUIDELINES FOR SECURING COVERED DATA AND INFORMATION:

"*Covered Data and Information*" is defined as educational records, and the personal and financial information of students, faculty members, staff members, alumni, and other donors. When in doubt as to whether a piece of data or information is to be safeguarded as covered data and information, COD 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 COD 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 and frequently changing passwords to access automated systems that process covered data and information. Also encouraging the use of "strong" passwords (e.g. at least 6 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 employees work area).

4 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.

5 Shredding and erasing customer information when no longer needed in accordance with Department / College policy.

6 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.

7 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.

8 Encouraging employees to report suspicious activity to supervisors and/or the COD Police Department, as appropriate.

9 Encouraging password-activated screen savers and using them when an employee is away from his/her desk.

10 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 of the Family Educational Rights and Privacy Act and Gramm-Leach-Bliley Act

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 the Registrar.

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

ACCEPTANCE OF RESPONSIBILITY

I understand that the College of DuPage maintains personally identifiable information for students, faculty members, staff members, alumni and other donors, disclosure of which is prohibited by the Family Education Rights and Privacy Act and the Gramm-Leach-Bliley Act of 2002. 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 COD Policy Manual of the Board of Trustees, Policy No. 20-15: "Student Education Records" 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