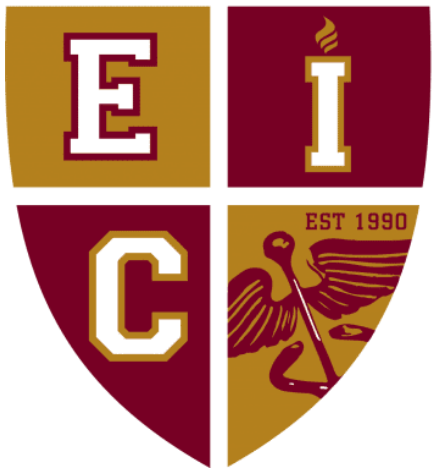

Eastern International College

INFORMATION TECHNOLOGY & CYBERSECURITY POLICIES AND PROCEDURES MANUAL

2023-2024

Table of Content

1 Overview

EIC has policies in place to ensure the data integrity of student information ensuring the following cyber protections are in place as outlined below and required by Federal Funding. Student information is defined as:

- Data stored in the student database, including personal identifying information and financial data;
- Data transmitted by email; and
- Data transmitted over the Internet, including to Department of Education sites by Financial Aid accessing students' information.
- Interaction with Third Party Vendors

2 Handling, management, and transmission of the school's personal identifiable information (PII) in Information Systems

2.1 What is PII?

Personal Identifiable Information (PII) is defined as any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information:

(i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or

(ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online contact of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic, or other media.

2.2 Who is PII gathered on?

- Prospective Students
- Current Students
- Alumni
- Prospective Employees
- Current Employees
- Past Employees

2.3 How is PII stored in Information Systems?

Information Systems means any electronic system that stores, processes or transmits Institutional Data. Institutional Data means any data concerning a natural person that is owned or licensed by the College, with the exception of data that is governed by the College's HIPAA Privacy Policy and HIPAA Security Policy.

EIC keeps digital records on prospective, current and past students and employees housed in two principal databases. The first is our student information system database which is stored in the cloud. It uses credentialed, permission-based access (by user role). Permissions are allocated to staff after undergoing appropriate training use with data access limited to their role following minimum necessary standards. The second database is Google's online cloud storage, as EIC uses Google and its tools for email and digital document storage. Team drives are used by Administrative units to storage appropriate documentation needed for their roles and is protected by login credentials and two factor authentication. On premises storage is used for local Windows administration and Dentrix used by the Dental Hygiene clinic. Certain divisions (Accounting with PayChex and Quickbooks, Financial Aid with HISSA and DOE website) have access to specialty tools that are required of their role and function. Credentials and passwords are used and security in line with College online accessibility.

2.4 Who has access to PII?

EIC implements appropriate technical and organizational measures to ensure that, by default, only Institutional Data that is necessary for its specific purpose is processed in Information Systems. This obligation applies to the amount of Institutional Data collected, the extent of their processing, the period of their storage and their accessibility in particular, and that such measures ensure that by default that Institutional Data is not made accessible to an indefinite number of natural persons.

EIC allocates permissions to the appropriate data access according to job role and when the employee is no longer at EIC, access to data is terminated.

3 What is a breach?

Per Financial Aid/ Title IV/ GLBA, EIC must protect against any unauthorized disclosure, misuse, alteration, destruction, or other compromise of information, such as unauthorized access.

The Department of Education and Federal Student Aid considers each of these a breach. EIC must have in place administrative, technical, and physical safeguards which:

● ensure the security and confidentiality of customer information;

● protect against any anticipated threats or hazards to the security or integrity of such records; and

Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

3.1 Identifying reasonably foreseeable internal and external risks to data security via formal, documented risk assessments of employee training and management New EIC staff are required to take database training before user names are distributed.

EIC provides cybersecurity training to all staff (administrative and faculty) giving ongoing cyber security awareness training. This training allows for monthly cybersecurity training and tips, providing an overview and reminders for completion and the ability to monitor their progression.

This cybersecurity training helps EIC manage the ongoing problem of social engineering with simulated phishing and training platform. Note this training is not meant to be a physical solution in security but the Human Firewall.

3.2 Identifying reasonably foreseeable internal and external risks to data security via formal, documented risk assessments of information systems, including network and software design, as well as information processing, storage, transmission, and disposal.

EIC has staff or students report missing equipment or a data breach to the IT Department as per the following policy outlined in the Faculty Handbook, College Catalog and EIC's website.

All EIC employees must immediately report lost or stolen technology resources to the IT Department (support@eicollege.edu).

EIC staff, administrators, faculty and students should report any suspected data breach to IT either by email (support@eicollege.edu) or phone (201.680.7714). With the help of a network monitoring tool, EIC is able to have insight to our network to identify anomalies in real time that could be potential threats.

We are able to monitor the network activity of users and devices on premises using a monitoring tool based in our server room, ensuring that data across the entire organization is secured.

3.3 Identifying reasonably foreseeable internal and external risks to data security via formal, documented risk assessments on the ability to detect, prevent, and respond to attacks, intrusions, or other systems failures

EIC has in place firewalls that gives EIC network protection and EIC network engineer's ability to detect and prevent unauthorized traffic on our network. EIC also uses antivirus protection on all

EIC issued computers (staff, faculty and computer labs). This allows EIC the ability to monitor and mitigate viruses and malware on university hardware. This is a first line of defense in preventing an attack.

In the event of an attack, intrusion or system failure, our monitoring appliance provides real-time detection and alerting. This technology is ideally suited to detecting attacks in their earliest stages before they become data breaches; even previously unknown threats that are novel or tailored. By identifying anomalies, end-users are able to investigate and respond to compromises as they emerge. The combination of artificial intelligence that sets off the alerts, allows EIC staff to be constantly monitoring and alerted when issues arise, in real time.

4 Control the risks identified by designing and implementing information safeguards and regularly test/monitor their effectiveness

Once a risk is identified and a safeguard is defined as a response, EIC's real-time monitoring and investigation device interface helps ensure that these procedures are strictly enforced. By investigating detailed alerts on user and machine activity, the team can immediately determine an ineffective security policy. For example, if a safeguard is put in place that prevents employees from using certain file storage platforms, EIC can monitor which users comply and which violate policy.

4.1 Oversee service providers by taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the FSA, student, and school (customer) information at issue; and require service providers by contract to implement and maintain such safeguards

Such information is collected from third party providers, including certification standards and audit details.

4.2 Evaluate and adjust your school's data security program in light of the results of the required testing/monitoring, any material changes to operations or business arrangements, and any other circumstances that may have a material impact on EIC's information security program

By leveraging visibility within the network thanks our monitoring efforts, EIC can use the tool to determine effectiveness of security programs and implement necessary changes, even to shape cyber security policies as a whole (when relevant). In addition, the tool helps with making critical security repairs by determining problematic misconfigurations in the first place.

The following was undertaken to reduce our risks:

● Moving data to the cloud- Two-factor authentication and disaster recovery done for Diamond and Google's GSuite: FERPA, HIPAA, and GDPR compliant.

● Updating our website with hosting on BlueHost and using WordPress- increases security and disaster recovery plans.

Title IV schools are subject to the requirements of the Federal Trade Commission Identity Theft Red Flags Rule ("Red Flags Rule") (72 Fed. Reg. 63718) issued Nov. 9, 2007. The Red Flags Rule requires an institution to develop and implement a written identity theft prevention program to detect, prevent, and respond to patterns, practices, or specific activities that may indicate identity theft.

5 How do staff or students report missing equipment or a data breach to IT?

All EIC employees must immediately report lost or stolen technology resources to the IT Department (support@eicollege.edu). EIC staff, administrators, faculty and students should report any suspected data breach to IT either by email (support@eicollege.edu) or phone (201-533-1027).

6 How does IT at EIC report security breaches to students and the Department of Education?

The Student Aid Internet Gateway (SAIG) Agreement requires that as a condition of continued participation in the federal student aid programs, EIC report actual data breaches, as well as suspected data breaches. EIC must report on the day that a data breach is detected or even suspected. The U.S. Department of Education (the Department) has the authority to fine institutions—up to $54,789 per violation per 34 C.F.R. § 36.2—that do not comply with the requirement to self-report data breaches. The Department has reminded all institutions of this requirement through Dear Colleague Letters (GEN 15-18, GEN 16-12), electronic announcements, and the annual FSA Handbook.

7 How does IT report a breach to the Department of Ed?

To report a breach, email cpssaig@ed.gov. Your email should include:

- date of the breach (known or suspected),
- impact of the breach (number of records, number of students, etc.),
- method of the breach (hack, accidental disclosure, etc.),
- information security program point of contact (email address and phone number are required),
- remediation status (complete, in-process, etc. with detail), and
- next steps (as needed).

If you cannot email, call the Department's security operations center (EDSOC) at 202-245-6550 to report the above data. EDSOC operates 24 hours a day, seven days per week.

For more information, please contact:

Call: 201-533-1027

Email: support@eicollege.edu