POLICY # 3358-7-19
Section: Information Technology
Original Policy: # 3358-7-19
Revision Approved: 11/16/2022
Approved by: Board of Trustees

Edison State Community College
Information Technology and Security Policy

PURPOSE

The purpose of the Edison State Community College Information Technology and Security Policy is to recognize the importance of information and data processes and security. The College uses best practices in research, design, development, implementation, and sustainability of information technology in support of the teaching process of faculty, the learning process of students, the management and decision-making processes of administration, and the transactional processing and record management functions of support staff.

POLICY STATEMENT

In order to protect critical information and data, and to comply with Federal Law[1], Edison State Community College's Information Technology Department (IT), proposes certain practices in the College information environment and institutional information security procedures. While these practices mostly affect IT, some of them will impact diverse areas of the College, including but not limited to Business Services, Student Services, the Office of the Registrar, and many third-party contractors, facilities and building service providers. The goal of this document is to define the College's Information Security Program ("Program"), to provide an outline to assure ongoing compliance with federal regulations related to the Program and to position the College for likely future privacy and security regulations. Whenever possible, the College conforms to the State of Ohio IT Policies.

Gramm Leach Bliley (GLB) Requirements

GLB mandates that the College appoint an Information Security Plan Coordinator, conduct a risk assessment of likely security and privacy risks, institute a training program for all employees who have access to covered data and information, oversee service providers and contracts, and evaluate and adjust the Program periodically.

Information Technology Security Plan Coordinator

In order to comply with GLB, IT has designated an Information Technology Security Plan Coordinator. This individual must work closely with the Business Office, the Networking and Security Administrator in Information Technology, other positions in

1 The Financial Services Modernization Act of 1999 (also known as Gramm Leach Bilely (GLB) 15 U.S.C. §6801

Information Technology and Information Systems and Services, as well as all relevant academic and administrative Departments throughout the College. The Coordinator is presently the Chief Information Officer.

The Coordinator must help the relevant offices of the College identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information; evaluate the effectiveness of the current safeguards for controlling these risks; design and implement a safeguards program, and regularly monitor and test the program.

Risk Assessment and Safeguards

The Coordinator must work with all relevant areas of the College to identify potential and actual risks to security and privacy of information. Each Department head, or his/her designee, will conduct an annual data security review, with guidance from the Coordinator. Vice Presidents will be asked to identify any employees in their respective areas that work with covered data and information. In addition, the relevant components of IT will conduct a quarterly review of procedures, incidents, and responses, and will publish all relevant materials except in those cases where publication may likely lead to breaches of security or privacy. Publication of these materials is for the purpose of educating the College community on network security and privacy issues. IT will assure that procedures and responses are appropriately reflective of those widely practiced at other state colleges and community colleges, as measured by four advisory groups: The Educause Security Institute, The Internet2 security working group, the SANS Top Twenty risks list, and the Federal NIST Computer Security Resource Center.

In order to protect the security and integrity of the College network and its data, IT will develop and maintain a registry of all computers attached to the College network. This registry will include, where relevant, IP address or subnet, MAC address, physical location, operating system, intended use (server, personal computer, lab machine, etc.), the person, persons, or department primarily responsible for the machine, and whether the machine has or has special access to any confidential data covered by relevant external laws or regulations.

IT assumes the responsibility of assuring that patches for operating systems or software environments are reasonably up to date, and will keep records of patching activity. IT will review its procedures for patches to operating systems and software and will keep current on potential threats to the network and its data. Risk assessments will be updated quarterly.

IT bears primary responsibility for the identification of internal and external risk assessment, but all members of the College community are involved in risk assessment. IT, working in conjunction with the relevant College offices, will conduct regular risk assessments, including but not limited to the categories listed by GLB.

IT, working in cooperation with relevant College departments, will develop and maintain a data handbook, listing those persons or offices responsible for each covered data field in relevant software systems (financial, student administration, development, etc.). IT and the relevant departments will conduct ongoing (at least biannual) audits of activity, and will report any significant questionable activities.

IT will work with the relevant offices (Business Services, Human Resources, the Registrar, and Student Services among others) to develop and maintain a registry of those members of the College community who have access to covered data and information. IT in cooperation with Human Resources and Business Services will work to keep this registry rigorously up to date.

IT will assure the physical security of all servers and terminals which contain or have access to covered data and information. IT will work with other relevant areas of the College to develop guidelines for physical security of any covered servers in locations outside the central server area. The College will conduct a survey of other physical security risks, including the storage of covered paper records in non-secure environments, and other procedures which may expose the College to risks.

While the College has discontinued usage of social security numbers as student identifiers, one of the largest security risks may be the possible non-standard practices concerning social security numbers, e.g. continued reliance by some College employees on the use of social security numbers. Social security numbers are considered protected information under both GLB and the Family Educational Rights and Privacy Act (FERPA).[2] By necessity, student social security numbers still remain in the College student information system.[3] The College will conduct an assessment to determine who has access to social security numbers, in what systems the numbers are still used, and in what instances students are inappropriately being asked to provide a social security number. This assessment will cover College employees as well as subcontractors.

IT will develop a plan to ensure that all electronic covered information is encrypted in transit and that the central databases are strongly protected from security risks.

It is recommended that relevant offices of the College decide whether more extensive background or reference checks or other forms of confirmation are prudent in the hiring process for certain new employees, for example employees handling confidential financial information.

IT will develop written plans and procedures to detect any actual or attempted attacks on covered systems and will develop incident response procedures for actual or attempted unauthorized access to covered data or information.

---

2 20 U.S.C. § 1232g

3 Social Security Numbers are kept both for historical purposes and due to the requirements of 26 U.S.C. § 6050S, the tuition payment credit reporting requirements.

The Information Security Coordinator will periodically review the College's disaster recovery program and data-retention policies and present a report to the College leadership.

Employee training and education

While directors and supervisors are ultimately responsible for ensuring compliance with information technology and security practices, IT will work in cooperation with Human Resources to develop training and education programs for all employees who have access to covered data. These employees typically fall into three categories: professionals in information technology who have general access to all college data; custodians of data as identified in the data handbook, and those employees who use the data as part of their essential job duties.

Oversight of Service Providers and Contracts

GLB requires the College to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. Business Services will develop and send form letters to all covered contractors requesting assurances of GLB compliance.

Evaluation and Revision of the Information Security Plan

GLB mandates that this Information Security Plan be subject to periodic review and adjustment. The most frequent of these reviews will occur within IT where constantly changing technology and constantly evolving risks indicate the wisdom of quarterly reviews. Processes in other relevant offices of the College such as data access procedures and the training program should undergo regular review. The plan itself as well as the related data retention policy should be reevaluated annually in order to assure ongoing compliance with existing and future laws and regulations.

Definitions

Covered data and information for the purpose of this policy includes student financial information required to be protected under the Gramm Leach Bliley Act (GLB). In addition to this coverage, which is required by federal law, Edison State Community College chooses as a matter of policy to also define *covered data and information* to include any credit card information received during business by the College, whether or not such credit card information is covered by GLB. Covered data and information includes both paper and electronic records.

Student financial information is that information the College has obtained from a student in the process of offering a financial product or service, or such information

provided to the College by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CFR § 225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and social security numbers, in both paper and electronic format.

PERSONS AFFECTED

All Edison State Community College employees and permanent employee's spouse and/or dependent children as defined above.