Cuyahoga Community College (Tri-C) Information Security Program

Purpose

The purpose of the program is to ensure compliance with applicable laws and regulations and to safeguard CSI to protect students, employees, and the College.

Executive Summary

The Information Security Program is designed to safeguard all nonpublic personal information and to comply with regulations related to safeguarding information. This program includes the administrative, technical, and physical safeguards the school uses to access, collection, distribute, dispose of, and handle **"**Confidential/Sensitive Information" or CSI.

This Program applies to any area of Tri-C where CSI, regardless of format, is collected, edited, manipulated, reviewed, reported, disposed of or stored.

It is the responsibility of all members of the Tri-C community to be aware when they are handling CSI and to understand and follow the processes defined in or referenced from this document.

For business processes and systems with CSI, it is the responsibility of each Business Process Owner or System Owner to define the specifics of how the information in their stewardship will be protected, and to ensure anyone using the process or system is familiar with the protection protocol.

Tri-C's general approach to protecting CSI is based on:

- Minimizing the collection and storage of CSI.
- Limiting access only to those who require it by job function.
- Educating staff on how to handle CSI will help better protect it from disclosure or compromise.
- Utilizing secure practices and technologies to protect CSI.

Related Rules and Regulations

In addition to other Ohio laws, handlers of CSI should also be aware of these other laws and regulations regarding personal information:

Family Educational Rights and Privacy Act (FERPA) of 1974

The Family Educational Rights and Privacy Act of 1974 sets forth requirements designed to protect the privacy of student education records. FERPA provides for the right to inspect and review education records, the right to seek to amend those records and to limit disclosure of

information from the records. FERPA applies to all institutions that are the recipients of funds under any program administered by the Secretary of Education.
For more information on the College's FERPA policy, visit http://www.Tri-C.edu/administrative-departments/office-of-legal-services/student-education-records-and-ferpa.html

Payment Credit Industry Data Security Standards (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is a standard for organizations who accept credit cards. It places a number of requirements for security management, policies, procedures, network architecture, software design and other critical protective measures for systems that handle credit card data. Anyone who handles credit card data or transactions must be certain to protect this data.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 sets forth rules regarding Privacy, Security and Breach Notification of individually identifiable health information. Athletic departments and Human Resources handle health information. This must be protected in accordance with the HIPAA rules.

The College HIPAA Privacy policy is posted at http://www.Tri-C.edu/administrative-departments/human-resources/documents/HIPAA%20Privacy%20Policy.pdf

FTC "Red Flag Rules"

The Federal Trade Commission (FTC) Red Flags Rule requires us to implement a written Identity Theft Prevention Program designed to detect the warning signs – or red flags – of identity theft in their day-to-day operations. We have in place procedures for identity verification, reporting suspicious activity, and placing a "hold" on a student's record. The policy is stored on our public web site, 3354:1-20-09 Identity Theft Policy - http://www.Tri-C.edu/policies-and-procedures/documents/identity-theft-policy.pdf

Gramm Leach Bliley Act (GLBA)

An FTC rule aimed at protecting customer information held by "financial institutions", which applies to the College due to financial aid-related activities. The GLBA Safeguards rule requires a comprehensive information security program that adjusts to respond to changing risks.

Ohio Revised Code – Section 1347

3354:1-43-05 Personal Information System Policy - http://www.Tri-C.edu/policies-and-procedures/documents/personal-information-policy.pdf

Roles

Program Oversight

Oversight and maintenance of this Information Security Program is the responsibility of the Vice President, Information Technology Services, the Vice President, Legal Services, and the Director, Office of Safe and Secure Computing.

Business Process Owners

Business Process Owners should have awareness of the relevant regulatory and compliance issues, as well as the responsibility and authority for defining the rights of others to collect, use, or store data during the process execution. To the extent that IT systems are used as part of the process, Business Process Owners will work with System Owners to ensure that appropriate tools and controls are in place to enforce the desired policies.

Business Process Owners may further delegate specific responsibilities; however, in the event of a data incident or questions about policy, the Business Process Owner is accountable for the outcome.

System Owners

Senior IT Managers who have responsibility for the systems supporting business processes involving CSI are expected to designate one or more System Owners.

System Owners should have awareness of IT parameters used to support the regulatory and compliance issues, and the technology used to implement the policies with regard to collecting, using or storing the data during the process execution. System Owners will generally take policy direction from the Business Process Owner.

System Owners are responsible for overall security of the systems and services they manage. This includes but is not limited to security patching and awareness of available security patches, system hardening, and service accounts, using strong authentication, and ensuring the confidentiality and integrity of data.

In the event of a data incident or questions about controls, the System Owner and Senior IT Manager are expected to be part of the discussions.

Department Heads and Other Managers

Department Heads and other Managers have a responsibility for ensuring that the individuals in their areas who are accessing or dealing with business processes involving CSI are aware of the requirements for handling CSI, and to provide them with awareness, training, and education opportunities.

Department Heads and Managers are also expected to provide appropriate technical support such as software tools and fully trained IT support staff to facilitate compliance.

Individuals with Access to CSI

Individuals with access to CSI should be aware of this Program so that they can follow appropriate steps to protect CSI in hard copy, electronic or other forms. Secure practices are particularly important to protect electronic information. Individuals are encouraged to work with the System Owners or technical support staff who can provide security solutions or recommendations.

Compliance and Business Continuity Team (C and BT)

The Compliance and Business Continuity Team is notified when a possible breach of CSI or other sensitive information is suspected. The Compliance and Business Continuity Team will work with the legal team to decide whether to put the insurance carriers on notice and to activate potential IT resources provided by the College's insurance carriers.

Office of Safe and Secure Computing (OSSC)

The Office of Safe and Secure Computing (OSSC) is a team within ITS. OSSC is the first technical team notified in the event of a suspected computer or network intrusion that may involve CSI. OSSC evaluates the technical specifics of each event and notifies the Compliance and Business Continuity team when a breach of CSI is suspected. OSSC will coordinate other incident response activities.

OSSC assesses changes in risk, evaluates and adjusts the security program and controls.

Internal Audit

The Internal Audit department evaluates the effectiveness and adoption level of controls to identify risks, gaps, and non-compliance.

Minimizing CSI Collection and Storage

Understanding Where CSI Is Located

Each Business Process Owner or System Owner is expected to:

- Understand why CSI is needed, and to limit the amount of CSI that is collected to that which is reasonably necessary to accomplish the legitimate purpose for which it is collected.
- Understand where data is stored, used or transmitted.
- Determine appropriate record retention for CSI.
- Ensure that when electronic and hard copy records are redacted, deleted or destroyed, this is done in such a way that CSI cannot be practicably read or reconstructed.
- When a new business requirement for handling CSI develops, Business Process Owners are expected to update processes and protocols as appropriate. Business Process Owners or System Owners may delegate the above responsibilities to one or more individuals who have received training or education in information security and privacy.

Limiting Access to CSI

Each Business Process Owner or System Owner will be responsible for a protocol that defines the rules, processes and/or systems for:

- Limiting access to only authorized and authenticated individuals who need CSI to conduct Tri-C business.
- Removing access when it is no longer needed, such as in the event of employment termination or job change.
- Periodically reviewing who has access to ensure it is in alignment with current business needs, done at least annually.
- Securing electronic and hard copy files when stored or during transmission, as well as understanding that electronic files that contain CSI should not be transmitted over email or the Internet unless properly encrypted and authorized.
- Logging and monitoring access to detect unauthorized attempts to access CSI, as well as inappropriate access by authorized individuals.

Training

Each Business Process Owner or System Owner will take steps to ensure those authorized to access CSI have received training in the specific responsibilities and procedures associated with that area. They will also ensure that one or more individuals in those areas receive training or education in information security and privacy.

Department managers and supervisors will take steps to ensure that individuals in their area who are working with processes involving CSI have appropriate and sufficient training, as well as access to relevant tools and IT support services to enable compliance with this Program. Individuals are expected to be aware when they are part of a process that includes CSI. They are also expected to avail themselves of relevant training and guidance offered by Business Process Owners, System Owners or their department.

Third-Party Vendors

Each Business Process Owner or System Owner must undertake reasonable steps to verify that third-party service providers with access to CSI have the capacity and the commitment to protect such information in accordance with applicable laws and regulations. Service providers should be aware of Tri-C's responsibilities to protect CSI. Contracts must include appropriate clauses that require service providers to implement and maintain appropriate security measures to protect CSI as well as language that ensures the design of secure systems and data handling processes. Tri-C's Office of Legal Services can provide assistance with contract language. Consult the College-Wide Director, Compliance Risk Management to have a risk assessment performed as part of the procurement process.

Protection of Hard Copy Files

In addition to removing CSI from files where they are not required for business processes, recommended protective measures for paper, microfiche, or other non-computerized files include physically locking cabinets, drawers, offices and other areas containing these files. CSI must never disposed of in regular trash or recycling bins – they must be placed in the secured College shredding bins in accordance with the College Record Retention Schedule - http://www.Tri-C.edu/administrative-departments/office-of-legal-services/documents/records-retention-schedule.pdf

Protection of Electronic Files

Tri-C has a set of minimum IT security standards that must be used for the protection of laptop and desktop computers, servers, cloud services, smart phones as well as mobile storage devices such as USB memory sticks that process, store, view, or transmit CSI.

Below are a partial list of procedures and technologies that are used to protect the confidentiality of data:

- Only supported OS and application software allowed
- Firewalls, IPS, ACLs, and other network protections
- Malware and exploit protection
- Unique system account for each person (no shared accounts)
- Full Disk Encryption for Laptops
- File and Transport Encryption
- Principle of least privilege
- Browser and email protections
- Secure destruction of electronic data

Each person with access to CSI is responsible for following secure practices to protect the data. Secure practices include but are not limited to:

- Using strong, unique passwords to access Tri-C services that are not reused at any other service.
- Storing CSI only in approved, secure locations.
- Transmitting CSI only to approved parties in an approved, secure manner.

Monitoring and Enforcement

Each year, Tri-C will review this Program to ensure that it is operating in a manner reasonably calculated to prevent unauthorized access to or use of CSI. Compliance with this Program will be reviewed as part of regularly scheduled operational and IT audits conducted by Tri-C's Internal Audit department.

Tri-C employees whose behavior is inconsistent with this Program will be subject to Tri-C disciplinary action, up to and including termination. See 3354:1-43-03 Corrective Action Policy - http://www.Tri-C.edu/policies-and-procedures/documents/corrective-action-policy.pdf. Enforcement actions relative to Tri-C faculty, students, temporary employees or others who compromise the protection of CSI will be addressed on a case-by-case basis.