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[1] and to comply with regulations related to safeguarding information. This program includes the administrative, technical, and physical safeguards the school uses to access, collect, distribute, dispose of, and handle **"**Confidential/Sensitive Information" or CSI, as defined in this document, to protect against anticipated threats or hazards to this information[2] and against unauthorized access or use of this information that could result in substantial harm or inconvenience to customers[3].

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 and document 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:

[1] 16 CFR §314.3(b)(1)
[2] 16 CFR §314.3(b)(2)
[3] 16 CFR §314.3(b)(3)

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

The Director, Office of Safe and Secure Computing will report to the Management Committee of the Board of Trustees on at least an annual basis[4]. The report must include the following information:

- The overall status of the Information Security program[5]
- Compliance with GLBA[6]
- Material matters related to the information security program[7], addressing issues such as:
    - Risk assessment[8]
    - Risk management and control decisions[9]
    - Service provider arrangements[10]
    - Results of testing[11]
    - Security events or violations and management's responses thereto[12]
    - Recommendations for changes in the information security program[13]

Business Process Owners

Business Process Owners must 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 owners must design and implement safeguards to control risks to CSI identified through the risk assessment.[14] This includes:

- Identify and manage the data, personnel, devices, systems, and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy.[15] This includes:
    - Documenting and approving data flows
    - User and privilege authorization
    - Physical access authorization
    - Authorization to operate devices and systems

[4] 16 CFR §314.4(i)
[5] 16 CFR §314.4(i)(1)
[6] 16 CFR §314.4(i)(1)
[7] 16 CFR §314.4(i)(2)
[8] 16 CFR §314.4(i)(2)
[9] 16 CFR §314.4(i)(2)
[10] 16 CFR §314.4(i)(2)
[11] 16 CFR §314.4(i)(2)
[12] 16 CFR §314.4(i)(2)
[13] 16 CFR §314.4(i)(2)
[14] 15 CFR §314.4(c)
[15] 15 CFR §314.4(c)(2)

- Adopt data retention and disposal practices:
    - Develop, implement, and maintain 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[16], unless any of the following conditions are met:
        - Such information is necessary for business operations or for other legitimate business purposes[17]
        - Is otherwise required to be retained by law or regulation
        - Where targeted disposal is not reasonably feasible due to the manner in which the information is maintained[18]
    - Periodically review the data retention policy to minimize the unnecessary retention of data[19]
- Adopt procedures for change management[20]

Business Process Owners must inform the Director, Office of Safe and Secure Computing, and request evaluation and any necessary adjustment to the Information Security program[21]:

- In light of the results of the testing and monitoring[22]
- When there are material changes to operations or business arrangements[23]
- Based on the results of risk assessments[24]
- Under any other circumstances that may have a material impact on the information security program[25]

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

Business Process Owners who have responsibility for the systems supporting business processes involving CSI are expected to designate one or more System Owners. System Owners selected must be in alignment with required knowledge and qualifications established by job descriptions managed by HR.[26]

System Owners must 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.

[16] 15 CFR §314.4(c)(6)(i)
[17] 15 CFR §314.4(c)(6)(i)
[18] 15 CFR §314.4(c)(6)(i)
[19] 15 CFR §314.4(c)(6)(ii)
[20] 15 CFR §314.4(c)(7)
[21] 16 CFR §314.4(g)
[22] 16 CFR §314.4(g)
[23] 16 CFR §314.4(g)
[24] 16 CFR §314.4(g)
[25] 16 CFR §314.4(g)
[26] 16 CFR §314.4(e)(2)

System Owners are responsible for overall security of the systems and services they manage. This includes security best practices for the type of system or service used.

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 are responsible 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 must 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 Risk Management

The Compliance and Risk Management (Risk.Management@tri-c.edu) team is notified when a possible breach of CSI or other sensitive information is suspected. Compliance & Risk Management will work with the Legal team to determine appropriate notifications to relevant insurance carriers and to activate IT resources provided by the College's insurance carriers, as necessary. Compliance & Risk Management also works with the College's Office of Safe and Secure Computing to conduct risk assessments of College IT services and resources and prior to the procurement of third-party IT products.

Office of Safe and Secure Computing (OSSC)

The Office of Safe and Secure Computing (OSSC) is a team within Information Technology Services (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 Risk Management team when a breach of CSI is suspected. OSSC will coordinate other incident response activities in accordance with the Incident Response Plan[27].

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.

[27] 16 CFR §314.4(h)

Development

The Executive Director, Enterprise Application Services must adopt secure development practices for in-house developed applications utilized for transmitting, accessing, or storing CSI and procedures for evaluating, assessing, or testing the security of externally developed applications utilized to transmit, access, or store CSI[28].

Minimizing CSI Collection and Storage

Understanding Where CSI Is Located

Each Business Process 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 will be responsible for implementation of a protocol, including policies, procedure, and controls, that defines the rules, processes, and/or systems to address risks identified through the risk assessment, including the following safeguards[29]:

- Limiting CSI access to only authorized and authenticated individuals[30] who need access to that CSI to conduct Tri-C business.[31]
- 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.[32]
- Implementing multi-factor authentication for any individual accessing any information system, unless the Director, Office of Safe and Secure Computing has approved in writing the use of reasonably equivalent or more secure access controls.[33]
- Securing electronic and hard copy files when stored or during transmission, including encryption of stored CSI, as well as understanding that electronic files that contain CSI should not be transmitted over email or external networks, including the Internet, unless properly encrypted and authorized.[34]

---

[28] 15 CFR §314.4(c)(4)
[29] 16 CFR §314.4(c)
[30] 16 CFR §314.4(c)(1)(i)
[31] 16 CFR §314.4(c)(1)(ii)
[32] 16 CFR §314.4(c)(1)
[33] 15 CFR §314.4(c)(5)
[34] 16 CFR §314.4(c)(3)

- Logging and monitoring access to detect unauthorized attempts to access or tamper with CSI, as well as inappropriate access by authorized individuals.[35]

To the extent that encryption of customer information, either in transit over external networks or at rest, is infeasible, such customer information may instead be secured using effective alternative compensating controls reviewed and approved by the Director, Office of Safe and Secure Computing.[36]

Training

Each Business Process Owner will ensure:

- Those authorized to access CSI have received training in the specific responsibilities and procedures associated with that area.
- Individuals working with CSI and in Information Security in those areas receive training and updates in information security and privacy sufficient to address relevant risks.[37]
- Verifying Information Security personnel take steps to maintain knowledge of changing threats and countermeasures.[38]

Department managers and supervisors will 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.

Each Business Process Owner will ensure security awareness training is updated to reflect risks identified by risk assessments.[39]

Formal Risk Assessment

A formal risk assessment of business processes and systems handling CSI must be performed and documented on at least an annual basis. The Office of Safe and Secure Computing and Compliance & Risk Management are responsible for performing this task.[40] The Information Security program must be based on this risk assessment.[41]

The formal risk assessment must identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of CSI that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks.[42]

---

[35] 16 CFR §314.4(c)(8)
[36] 16 CFR §314.4(c)(3)
[37] 16 CFR §314.4(e)(3)
[38] 16 CFR §314.4(e)(4)
[39] 16 CFR §314.4(e)(1)
[40] 16 CFR §314.4(b)(2)
[41] 16 CFR §314.4(b)
[42] 16 CFR §314.4(b)

The risk assessment documentation must include:[43]

- Criteria for the evaluation and categorization of identified security risks or threats faced by Tri-C[44]
- Criteria for the assessment of the confidentiality, integrity, and availability of Tri-C information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats[45]
- Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks[46]

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.[47] Service providers must 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.[48] 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 and periodically based on the risk presented by the third-party vendor and the continued adequacy of their safeguards.[49]

Protection of Hard Copy Files

In addition to removing CSI from files where they are not required for business processes, required 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 be 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[50]

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.

---

[43] 16 CFR §314.4(b)(1)
[44] 16 CFR §314.4(b)(1)(i)
[45] 16 CFR §314.4(b)(1)(ii)
[46] 16 CFR §314.4(b)(1)(iii)
[47] 16 CFR §314.4(f)(1)
[48] 16 CFR §314.4(f)(2)
[49] 16 CFR §314.4(f)(3)
[50] 16 CFR §314.4(c)(6)(i)

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 in accordance with the College Record Retention Schedule - http://www.Tri-C.edu/administrative-departments/office-of-legal-services/documents/records-retention-schedule.pdf[51]

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.

The review will include regularly testing or otherwise monitoring the effectiveness of the Information Security safeguards' key controls, systems, and procedures.[52] This review must include:

- Safeguards used to detect actual and attempted attacks on or intrusions into information systems[53]
- Continuous monitoring or periodic penetration testing and vulnerability assessments on information systems[54]
- If continuous monitoring is absent:
    - Annual penetration tests based on relevant risks identified during the risk assessment[55]
    - Vulnerability assessments (scans or reviews) designed to identify publicly known vulnerabilities based on the risk assessment:[56]
        - At least every six (6) months[57]

[51] 16 CFR §314.4(c)(6)(i)
[52] 16 CFR §314.4(d)(1)
[53] 16 CFR §314.4(d)(1)
[54] 16 CFR §314.4(d)(2)
[55] 16 CFR §314.4(d)(2)(i)
[56] 16 CFR §314.4(d)(2)(ii)
[57] 16 CFR §314.4(d)(2)(ii)

- When there are material changes to operations or business arrangements[58]
- Where there are circumstances that may have a material impact on the Information Security program[59]

The Information Security program must be evaluated and adjusted in light of the results of this testing and monitoring.[60]

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.

Definitions

Confidential/Sensitive Information (CSI) – Information that must be protected due to law, regulation, or other responsibility, in order to protect the College and/or the individual(s) whom the information is about.

[58] 16 CFR §314.4(d)(2)(ii)
[59] 16 CFR §314.4(d)(2)(ii)
[60] 16 CFR §314.4(g)