SUMMARY OF INFORMATION SECURITY PROCEDURES

ABSTRACT

Every employee plays a role in securing the College’s data. This document provides a high-level overview of the College’s security-related IT practices, procedures and regulations.

David Mastny
Director, Information Security

Cuyahoga Community College

REVISED JUN. 2024

Contents

Information Security Program

Each employee should be familiar with their role in the Information Security Program, which can be found online:

A brief summary is:

- Minimize the collection and storage of sensitive information
- Limit access to sensitive information to those who require it
- Educate staff on data handling and security awareness
- Utilize secure practices and technologies
- Each person has responsibility for securing data and should be familiar with their role

Electronic College Records

Official College records must only be stored in storage directly controlled by Cuyahoga Community College District. Examples include network drives, KWeb, OnBase, and other College servers. College records should not be stored on personal devices, portable storage devices, or cloud services not managed by the College.

Sensitive Information

Sensitive or confidential information must be protected against unauthorized access or public disclosure. Some examples include but are not limited to: Social Security numbers, passwords, credit card numbers, grades, bank account numbers, health information, biometric data (such as fingerprints) and disability status.

It is the duty of everyone who handles sensitive information to protect against unauthorized disclosure and ensure regulatory compliance regardless of format. 3354:1-50-05 Technology Resources Procedure (E) Training on this topic is available on-demand in the modules Handling Sensitive Information Securely SECUR1063 and Red Flags Rule COMP1002 which are both accessible via the COMPASS system.

Protecting Sensitive Information

Ensure that sensitive information is only disclosed to the people authorized to receive such information. When dealing with the public, you must verify the identity of an individual before making a transaction on their behalf or before disclosing sensitive information. When collecting additional information on a student, student identification numbers (S-Numbers) should be used to link the new information to a student's identity. This prevents unnecessary copies of Social Security numbers from being stored.

Sending and Receiving Sensitive Information

Cuyahoga Community College employees and agents have a responsibility to protect Confidential and Sensitive Information (CSI). Transfer of CSI should only occur under specific circumstances where the transfer is appropriate, authorized, and secure**.**

If you come across a circumstance that requires you to send or receive CSI or PII, **first ensure the data transfer is appropriate**. Consider the following:

- Is the receiving party authorized to receive the information? For example, a FERPA or similar release is on file with the College.
- Does the entity or party receiving the data have a legitimate reason to receive the data?
- Have you sufficiently verified the identity of entity you are working with?
- Are all of the data elements or fields required? If not, reduce the data to only those items required.
- If you do not know the answers, check with your supervisor.

If the data transfer is appropriate, check with your supervisor to determine if your department or organizational unit has an existing process in place. If not, seek guidance from ITS.

Processing Sensitive Information

CSI must not be entered, pasted, uploaded, or otherwise submitted into unapproved externally controlled data processing, transformation, conversion or similar systems, including generative AI systems such as ChatGPT. Another example system is online/cloud document conversion systems, such as PDF converters. These systems may subject CSI to unauthorized disclosure. Full Procedure

Approved Storage of Sensitive Information

Digital/Electronic Information

Sensitive digital information should only be stored on an approved, access-controlled storage location. Some examples include departmental drives ("I: drives"), KWeb sites with restricted membership or other approved, access-controlled storage. These locations have a number of protective controls and hardware redundancies which protect against hardware failure and unauthorized access. Workstation hard drives should not be used to store sensitive information.

Neither removable media (such as DVDs, CDs and flash drives) nor personal computing devices should be used to store sensitive information. The ideal location for data is within an approved application, such as OnBase or BANNER.

Cloud Storage locations not approved by the College should not be used to store sensitive data or College records.

Printed Information

Sensitive documents should be stored in a College-controlled, secured location. If you do not need to access a record but it must be kept, you should contact the College's Records Management department to have the documents stored. When no longer required, and in accordance with records retention policies, dispose of records properly by placing them into secured College shredding bins.

Email Security

Emailing Sensitive Information

Email should not be used to send sensitive information unless the sensitive information is encrypted using an approved solution such as the College's **Secure Message System**.

Risks inherent with using email to transfer sensitive information:

1. Mistyped addresses. It is not uncommon to hear stories about sending email to the wrong person by accident. This is especially the case with the "AutoComplete" feature used by many email clients, including Microsoft Outlook, or by clicking on the wrong address book entry and not noticing it.
2. Mail is sent over the internet unencrypted, or in plain text. Any devices through which it passes have access to read the email along the way.
3. Compromised accounts. If an email account is compromised (by phishing or keylogger, for example), all email contents can be easily stolen by an attacker.
4. Compromised or untrustworthy endpoints. Email can be accessed from mobile devices which can be lost or stolen along with all the data on them. Email can be accessed from personal computers and even public computers like library and hotel PCs, which present an elevated risk profile due to potential malware or keyloggers.

In order to send sensitive information to another authorized individual, you may use the College's secure message system. Instructions can be found on the KWEB ITS Security site.

Phishing

Phishing is one of the most common ways attackers use to steal login information. An email is crafted which constructs a scenario designed to get the recipient to give out his or her username/password or other sensitive information. In some cases, the information is requested via email by impersonating IT support (**ITS and the Helpdesk will NEVER request your password**). In other cases, a link is provided in the email which directs recipients to a fake but realistic-looking login site from which the credentials are harvested.

Some of these phishing emails and sites are very sophisticated. Research and customization are used to target a specific organization which provides a level of trust in the site and email. Phishing email usually creates a sense of urgency to get a person to act quickly. One commonly used scenario states that your account has had unusual activity and needs to be verified. Another impersonates IT systems administrators and requires you to log in and update accounts due to systems maintenance.

Always **Hover to Discover** to see where an email link leads before clicking. You can do this by "hovering" the mouse cursor over a link without clicking. The box that appears will show you where the link leads. This will help you to identify malicious websites before you click.

Should you accidentally respond to a phishing email, immediately change your password and call the Helpdesk at 216-987-4357 (HELP).

If you suspect a message is phishing, report it by using the Phish Alert button or by sending it to phishing@tri-c.edu. Create a new, blank message and add the phishing message as an attachment. This preserves header information for investigation.

The Office of Safe and Secure Computing (OSSC) uses Twitter to alert the College about widespread phishing messages. You can follow us on Twitter or check https://twitter.com/TriCOSSC to see if a suspect phishing message has been reported.

A number of training modules are available on-demand to help you recognize phishing emails. The KnowBe4 Security Awareness Training and Social Engineering Red Flags training modules can help teach you to recognize phishing emails. In addition, the in-person HOVER (SECUR1042) training provides in-depth training and practice to recognize phishing.

The College sends simulated phishing emails as part of a security awareness training program. Be prepared to recognize and report these and real phishing messages via the Phish Alert Button which can be found in Outlook (desktop version), Outlook mobile app, and web Outlook.

Laptops and Mobile Devices

College Laptops

College laptops are configured for full disk encryption. This includes a pre-boot password – a code that must be entered before the device will boot into Windows. The pre-boot password should never be recorded and stored with the laptop. Although full disk encryption provides a strong level of security, there are certain scenarios where this level of protection is insufficient. For example, if the laptop is on when it was lost, the encryption might not be sufficient since the information is decrypted while running. For this reason and to prevent lost data due to hardware failure or device loss, important and sensitive data should be stored in a secure network location, not on the laptop's hard drive. Also, turn the device off when not using it.

Laptops should be stored in a secure, locked location when not in use. When traveling, use the hotel safe if you leave it in your hotel room.

Whenever using a network not controlled by the College, the College VPN should be used. This allows the College's network security measures to protect systems and data.

Mobile Devices

Personally owned mobile devices, such as smart phones and tablets, can be used to connect to the College email systems and to gain remote access via VDI. When connecting to College email, the app used must enforce Microsoft Exchange policies, including the use of a PIN to lock the device after inactivity.

For a full list of mobile device best practices, review the OSSC guide here. An online training module, Mobile Device Security, is available via TEC for additional guidance on mobile device security.

Wi-Fi (Wireless Networks)

College-Provided Wi-Fi for Personal Devices

When configuring personal devices for the College's wireless network, be certain to connect to the College's official wireless network for personal devices which has the SSID or name of **CCC**. The **CCC** network requires login via captive portal, which means that the first time you attempt to visit a non-secure website, you will be redirected to log in to the "captive portal." Employees authenticate using their Tri-C network username and password. Once your device is registered on the network, the registration will be valid for 30 days. Up to 5 devices can be registered per employee.

Using Free Wi-Fi While Traveling

Only connect to trusted wireless networks. Before using wireless networks outside of home or work, such as at a business or hotel, inquire about the official name of the wireless network before connecting. Doing so will reduce the risk of connecting to a malicious network which might attempt to steal information or infect your device.

International Travel

If you intend on accessing College computing resources while traveling abroad, you should contact the Helpdesk to discuss options for securely remote work.

Do not store sensitive data on any internal or external device, including but not limited to hard drives, flash memory cards/sticks, DVDs or CDs. Instead, store data securely on College servers and access it using VDI. If you do not already have VDI permissions, you can request access via the online remote access request form.

When returning to the United States, it is advisable to change any passwords you may have used while traveling. For the full procedure on international travel, please see the International Travel College Computing Resources Procedure.

Lost Laptops/Mobile Devices

Should you lose your laptop or mobile device, promptly report it the local police and notify ITS by contacting the Helpdesk at 216-987-4357 or helpdesk@tri-c.edu.

Remote Access from Personally Owned Devices

VDI can be used as a method of remote access from personal computers or mobile devices, allowing you to access the non-public sections of the College network via a virtual desktop. Access can be requested via the remote access online request form.

Passwords

Your passwords are what protects your accounts from unauthorized access. To protect them:

- Use strong passwords or passphrases. Longer is better.
- Use unique passwords/passphrases. A password used for other accounts is exposed by the other systems.
- Never write down passwords/PINs and store them in your desk, under your keyboard or in any other area.
- Keep your password to yourself. You should never share your password with anyone. **ITS and the Helpdesk will NEVER ask you for your password.**

- Be careful where you type your password. Those attempting to steal your password will try to direct you to a fake login page.
- For guidance on creating strong passwords, an on-demand training module Creating Strong Passwords is available.

Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) requires an extra step to verify you when you login. This can be a phone, text message, code from a mobile app, or notification to a mobile app. If you ever receive unexpected MFA calls, messages, or prompts, someone might be trying to get into your account. Should this occur to you, change your password and notify the information security team immediately.

Single Sign-On (SSO)

Most College web applications use the same login application page. This is called Single Sign-On (SSO). SSO allows you to use the same login information across multiple apps. When you are logged in to SSO, you can switch between College web apps without the need to login more than once. When you log out, you will be logged out of all web apps in order to stay secure and have the expected behavior of being logged out.

Certain web applications such as *my Tri-C space* have automatic timeouts that log you out after a period of inactivity. To avoid unexpected and undesired logouts, close *my Tri-C space* tabs and windows when you are no longer using them.

Security Controls

Do not attempt to circumvent or disable College security controls. Examples to avoid include using proxy servers or third-party VPN services to bypass filtering or using hardware devices or software to prevent workstations from locking due to inactivity.

Reporting Suspicious Activity

Data breaches are all too common in today's world. We must all be vigilant. If you suspect a security incident or see unusual activity, please report it promptly by contacting the Helpdesk at 216-987-4357 (helpdesk@tri-c.edu) or Information Security at 216-987-4171 (information.security@tri-c.edu). You can check for other reported incidents and advisories on our Twitter site: https://twitter.com/TriCOSSC.

Suspicious Phone Calls

Should you receive a suspicious phone call where an unexpected caller asks you to take action on your computer or reveal sensitive information, do not follow their instructions or provide information. This may be a phone scam or a social engineering attack. Instead, report it to your supervisor and the

Helpdesk or Information Security team. See Reporting Security Incidents section above for contact information.

Suspicious Emails

If you receive a suspicious message, do not follow any links or open any attachments. Instead, follow the reporting information in the Phishing section to report the message.

Suspicious SMS/Text Messages

Threat actors will use multiple means to compromise their targets. One method they use is SMS text messages. Since these are outside of the College computer system, the College's security tools are not able to block or other detect these attacks. Should you receive a text message from someone you have not previously, treat it with suspicion. Contacts from unfamiliar phone numbers claiming to be someone from the College, especially positions of authority should be considered highly suspicious. Exercise caution in these situations, as attackers will gather information and send targeted text messages that research the names and positions of authority. If you did not provide your phone number to the claimed sender, there is a good chance the person is not who they claim to be. If you did provide it to the claimed sender but the sending number is different from the number you have for that person, it is likely the sender is not who they claim.

Questions

Should you have a question related to information security, please email information.security@tri-c.edu and we will get back to you.

On-Demand Information Security Awareness Training

Employees can sign up for on-demand information security awareness modules by accessing our COMPASS system via My Tri-C Space.

1. Log in to *My Tri-C Space* (my.tri-c.edu)
2. Find the *Employee Success Center* card
3. Click on the COMPASS logo:
4. Type SECUR in the Search box (this is the Security Awareness Training course code prefix):
    a. Click on the desired training module
    b. Click *Launch*

Personal Anonymizing Services, such as Personal VPN, TOR, etc.

Do not use anonymizing services designed to obscure identity and location. This makes account activity look suspicious and it is difficult to verify account activity as legitimate. Use of these services may prevent access or result in a suboptimal experience, such as unexpected logouts or other undesirable experiences. Examples include anonymizing VPNs like NORD VPN, or other services like TOR or web proxies.

Regulation and Compliance

The College is subject to a number of regulations based on the activities it performs and the information it holds. Each employee must handle data appropriately in order to comply with these regulations.

FERPA

The Family Educational Rights and Privacy Act of 1974 (FERPA) 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 receiving funds under any program administered by the Secretary of Education.

For more information on the College's FERPA policy, visit the Student Education and FERPA page on the Tri-C website.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a standard for organizations that 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 and follow the PCI Data Security procedure. Training on this topic is available via the TEC system in modules *Basics of Credit Card Security SECUR1008* and *PCI Compliance Simplified SECUR1009*.

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) sets forth rules regarding privacy, security and breach notification of individually identifiable health information. The College accepts patients in the dental clinic and the preventative care centers, while athletic departments and Human Resources handle health information. This information must be protected in accordance with HIPAA rules. The College's HIPAA privacy policy is posted here.

FTC Red Flags Rule

The Federal Trade Commission (FTC) Red Flags Rule requires the College to implement a written identity theft prevention program designed to detect the warning signs – or red flags – of identity theft in our day-to-day operations. Procedures are in place for identity verification, reporting suspicious activity and placing a hold on a student's record. Tri-C's identity theft policy is posted on our public website.

To view the 10-minute, self-paced training module, search "Red Flags Rule" in the TEC system.

Sunshine Laws - Ohio Public Records and Open Meetings Laws

Ohio's Public Records and Open Meetings Laws, collectively known as the Sunshine Laws, give Ohioans access to government meetings and records. When handling College records, be certain to follow the Tri-C Records Retention Schedule. Only store records in approved College locations.

Gramm-Leach-Bliley Act (GLBA) Safeguards Rule

The GLBA Safeguards Rule is an FTC rule aimed at protecting customer information held by financial institutions. The rule, which applies to the College due to financial activities such as accepting installment payment plans, requires a comprehensive information security program that adjusts to respond to changing risks.

Ohio Revised Code - Section 1347

ORC section 1347 – Personal Information Systems

Related College Policies

Current policies and procedures can be found on the College's public website at http://www.tri-c.edu/policies-and-procedures/.

Public Records

- 3354:1-11-06 Policy
- 3354:1-11-06 Procedure

Personal Information

- 3354:1-43-05 Policy
- 3354:1-43-05 Procedure

Identity Theft

- 3354:1-20-09 Policy

Knowledge Management

- 3354:1-50-02 Policy

Student Education Records

- 3354:1-30-02.2 Procedure

Technology Resources Policy

- 3354:1-50-05 Policy
- 3354:1-50-05 Procedure

Privacy Policy

- http://www.tri-c.edu/privacy.html

Definitions

Confidential or Sensitive Information (CSI): Data which if disclosed, could cause harm and must be protected from unauthorized disclosure

Encryption: A mathematical process that renders data unreadable by anyone except the person(s) holding the key or passphrase

Information Security Incident: An attempted event which may affect the confidentiality, integrity or availability of computer systems or records

Malware: Undesirable software which may steal or destroy information, spy on and report activities, or perform other unwanted activities

Phishing: A form of fraud using social engineering with email to steal sensitive information such as usernames and passwords

Social Engineering: An act, often involving deceit and social pressure, designed to elicit a specific response from a person that is not in their best interest

Spam: Unsolicited and undesired email messages which are often advertisements, phishing or malware

VDI (Virtual Desktop Infrastructure): A technology that enables remote access to a hosted virtual desktop, sending the display to a remote device or computer over a network

VPN (Virtual Private Network): A solution for securely accessing a remote network over an encrypted tunnel