SUMMARY OF INFORMATION SECURITY PROCEDURES

Cuyahoga Community College

REVISED AUGUST 2016

ABSTRACT

This document provides a high-level overview of the College's security-related IT practices, procedures and regulations.

David Mastny

Manager, Information Security

Contents

Sensitive Information

Sensitive or confidential information should be protected against unauthorized access or public disclosure. Some examples include but are not limited to: Social Security numbers, usernames, 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 Procedure F (10) Training on this topic is available on-demand in the module *Handling Sensitive Information Securely SECUR1006* which accessible via the TEC 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.

Approved Storage of Sensitive Information

Digital/Electronic Information

Sensitive digital information should 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.

Whenever possible, removable media (such as DVDs, CDs and flash drives) should not be used to store sensitive information. In cases where removable media is required to store sensitive information, the information must be encrypted using an approved solution and strong keys or passwords that are not stored with the media. When possible, approved network storage should be used instead.

Printed Information

Sensitive documents should be stored in locked cabinets. If you do not need to access a record but it must be kept, you may 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 and a strong key or passphrase. The key or passphrase should not be sent

over email, but must be communicated using an alternate channel such as instant message, text message or phone call.

Reasons why email is not a good way 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 by 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 is 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.

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 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. Then use the Junk Email reporting tool to aid in blocking similar future messages.

The Office of Safe and Secure Computing (OSSC) uses Twitter to report 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 *Kevin Mitnick Security Awareness Training 2016* *(SECUR1000, SECUR1001, & SECUR1002) and* *KnowBe4 Basic Security Awareness* *(SECUR1003)* training modules can help teach you to recognize phishing emails.

Reporting Spam

Spam messages are bulk messages sent out unsolicited to advertise a product or service. The College attempts to filter undesired spam messages without blocking legitimate messages. Unfortunately, some do get through. You can aid in blocking spam by reporting it using the Junk Email reporting tool in Outlook. You can find the current instructions for reporting spam here.

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 would 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.

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 operated by 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 SECUR1007* is available in for additional guidance on this topic.

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 borrow a loaner laptop that has been wiped of all data. These can be obtained from the Learning Commons library or ITS User Services.

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 or VPN. If you do not already have VDI or VPN 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. Doing so should cut off any unauthorized access in the event that your account was compromised abroad.

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 password is what protects your accounts from unauthorized access. To protect it:

- Use strong passwords or passphrases. Longer is better.
- 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.**

- For guidance on creating strong passwords, an on-demand training module *Strong Passwords SECUR1005* is available.

Reporting Security Incidents

Data breaches are all too common in today's world. We must all be vigilant. If you suspect a possible 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 take 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.

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 TEC system via My Tri-C Space.

1. Log in to My Tri-C Space (www.my.tri-c.edu)
2. Click on the *Employee* tab

3. Click on the TEC logo: TEC Documents

4. Either type SECUR in the Search box or:
5. Highlight *Learning* then select *Browse for Training*
6. Click on *Technology* under the subject
7. Click on *Security* under subject
8. Click on the desired training module
9. Click *Launch*

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

All current policies and procedures can be found on the College's public website.

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

Definitions

Confidential or Sensitive Information: Data that 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