Tompkins Cortland Community College Information Security Protocol

Approved: 6/29/2009 Revised: 7/21/2017

Purpose

- To ensure the safety and confidentiality of personal information
- To protect against any anticipated threats to the security or integrity of such information
- To guard against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any person.
- To comply with all applicable regulations.

Definitions

Personal Information: any record containing nonpublic personal information; whether in paper, electronic, or another form, that is handled or maintained by TC3 or on behalf of TC3 by our affiliates.

Information Security Program: the administrative, technical, or physical safeguards used to access, collect, distribute process, protect, store, transmit, dispose of, or otherwise handle personal information.

Service Provider: any person or entity that receives, maintains, processes, or otherwise is permitted access to personal information through its direct provision of services to the College.

Designated Employees

The following employees of the College are designated to coordinate the information security plan of the College: Chief Information Officer and Registrar along with the appointed members of the Information Security Management Program team.

Risk Assessment

A complete risk assessment of all College departments will be conducted by utilizing the risk assessment form **(Appendix 1)**.

All areas of the College are required to follow this plan. However, areas of high risk will be audited annually for compliance with the provisions of this plan. Areas of medium to low risk will be reviewed and evaluated as deemed necessary.

Employee management and training including student workers, interns, and co-op students who work with personal information

We will incorporate the following employee management and training program practices:

- Check references prior to hiring employees who will have access to personal information. Supervisors will be responsible for training staff in the proper use of confidential information.
- All new employees, as part of the orientation process, will meet with the Registrar or her designee to review FERPA regulations, and will also meet with the Dean of Campus Technology or his designee to review the campus' security policies.
- As part of the Human Resources exit interview, the HR Office will verify the employee is not leaving with any College data/information nor any computer equipment in their possession.
- Every employee and student worker must sign a TC3 Administrative Network/Data Access Form, which discusses FERPA, confidentiality, and security standards for handling personal information on campus.
- Train employees to take basic steps to maintain the security, confidentiality, and integrity of personal information, such as:

    - locking rooms and file cabinets where paper records are kept
    - using strong passwords
    - changing passwords periodically, and not posting passwords near employees' computers
    - encrypting sensitive personal information when it is transmitted electronically over networks or stored online
    - referring calls or other requests for personal information to designated individuals who have safeguards training
    - recognizing any fraudulent attempt to obtain personal information and reporting to appropriate agencies.

- Instruct and regularly remind employees of our policy and the legal requirement to keep personal information secure and confidential.
- Limit access to personal information to employees who have a business reason for seeing it.

Information Systems

- The College will store records in a secure area and make sure only authorized employees have access to the area. For example:

    - paper records will be stored in a room, cabinet, or other container that is locked when unattended
    - storage areas will be protected against destruction or potential damage from physical hazards, such as fire or floods
    - refer to **Appendix 2** for policies concerning electronic data storage.

- The College will provide for secure data transmission when collecting or transmitting personal data. See **Appendix 2** for policies concerning data transmission. The College provides Internet service and computer access to the students on campus and at residence life. Students using these services are

bound by the terms of this protocol. The College also provides student email. See **Appendix 5** for policies concerning this service.

- The College will dispose of personal information in a secure manner. For example:
    - Personal information recorded on paper will be shredded and/or stored in a secure area until an approved service picks it up
    - All data will be erased when disposing of computers, diskettes, magnetic tape, hard drives or any other electronic media that contain personal information
    - The College will promptly dispose of outdated personal information in compliance with state and federal regulations.

- Use appropriate oversight or audit procedures to detect the improper disclosure or theft of personal information.

- The College will keep an up to date inventory of all computers on campus.

Managing System Failures

- Effective security management includes the prevention, detection, and response to attacks, intrusions, or other system failures. See **Appendix 4** for College procedures regarding electronic system failures.

- The College will notify persons promptly if their nonpublic personal information is subject to loss, damage, or unauthorized access.

Oversight of Service Providers and Contracts

All College contracts will be reviewed for the nature and content of the contractual arrangement. Any service providers that we determine have the ability to access personal information will be required to comply with the College non-disclosure agreement. Such language will be added to all contracts, and authorized parties will sign the addendums. Campus Technology will be responsible for maintaining these forms.

Procedures will also be followed to monitor contractor compliance with the provisions of this plan.

Evaluation and Revision of the Information Security Plan

This information security plan will be periodically evaluated and adjusted in light of relevant circumstances, including changes in the College's business arrangements or operations, or as a result of testing and monitoring safeguards.

Appendix 1: Information Security Risk Assessment

Department_____
Date Prepared_____ Preparer_____

Examples of nonpublic information: the fact that a person is a student or employee of the College; the individual's name, address, social security number, or account number; details of an individual's academic or employment record; details of student or College employee payments including banking and credit card information; details of a student's financial aid application, grants, scholarships, and awards.

A. Physical Records	ANSWER	ACTION REQUIRED*
1. Does your department keep paper records containing nonpublic personal, student or employee information? If yes, continue. Otherwise, skip to B.		
2. Are these records properly secured?		

B. Computer Access		
1. Does your department keep electronic records containing nonpublic personal, student or employee information? If yes, continue. Otherwise skip to C.		
2. Are these records properly secured?		

C. Employee Training		
1. Has each employee received a copy of the campus network access form and signed the computer network security/FERPA form?		
2. Have all of your employees had an orientation visit with the Registrar and Dean of Campus Technology?		

D. Information Inquiries		
1. Does your department respond to inquiries for nonpublic personal, student or employee information?		
2. Are there adequate procedures for responding to these inquiries?		

* Attach additional papers as needed for actions required.

Appendix 2: Electronic Systems Security Policy and Procedures

Purpose

Access to computing resources is intended to provide members of the College community support for education, research, and necessary administrative activities. Use of the campus computing resources must be consistent with the purpose and the mission of the College. Campus computer systems are not intended for personal gain, profit or misuse.

Ethical Use of Computers

All users of College computing resources must respect the rights of other computing users, the integrity of the physical facilities and controls, and all pertinent license and contractual agreements. All use of resources shall be consistent with College policies and procedures and with all applicable federal, state, and local laws.

Network Applications

Each user is assigned a unique Campus Network ID. The system requires a strong security method for the use of passwords and IDs. Applications on campus may require additional security measures depending on the application and the data contained in it.

Databases

The Colleges databases are on a private network and are protected by the network user ID, and in many instances also protected by application layer security.

Email Access – Employees

The College will provide email access to employees, retirees (designated by the human resources office), and those that may need to be involved in the business of the College. This access will only be provided if the account is actively used. Accounts that are not used cause an unnecessary increase in load, cost, and the perception the email address is active, when it truly is not. The college will review and develop an archive plan.

Email Access – Students

See Appendix 4

Internet Access

The College provides access via web servers. Much of this information is public information. Information that is private is secured using SSL3 encryption technology. Access is granted via an encrypted ID and password, and all secure information is also sent via this encrypted technology.

FERPA

Anyone who accesses our student data , i.e., faculty, staff, and students, must sign the campus network access form which explains the FERPA rules and regulations.

Firewall

Our network is three physical segments: administrative, academic, and wireless. Any server that has confidential data or needs to be a secured server is maintained on our administrative network behind the firewall. This technology allows us to keep out much of the unwanted or “bad” traffic by closing ports that are not needed for us to conduct business.

Packet Shaping and Network Control

The College will maintain a packet shaping device. This product is used to control the various types of applications/protocols that pass to and from the Internet. It maximizes application throughout across our network infrastructure. Internal threats from worm infections, unsanctioned recreational traffic, and rogue servers can severely affect network capacity and bring down critical applications. The packet shaping device helps identify infected PCs and unsanctioned traffic as well as protects performance of key applications and the network.

ID and Passwords

In order for security on any system to work, it is critical that users understand how important it is to keep their passwords secure. Campus Technology is responsible for the management of this on the administrative systems.

1) Each user will be assigned unique IDs and passwords as needed by the network or application that they must use to perform their job function.
2) The College will maintain a strong password standard and encourages staff to use passwords that do not include family names or birthdates.
3) Many applications ask you to save your password so you do not have to enter it the next time you login. Passwords should not be saved in these instances. This allows other users who use your computer to log in as you.
4) Users are not to share their IDs and passwords with anyone.
5) College employees PCs should have a screen saver password, so that if the PC is left unattended for longer than five minutes it will be locked.
6) Where SSN information must be shared in a public area, a keypad is suggested for input of that number, instead of giving the number out loud.

Network and Systems Performance

It is the intention of the College to provide good Internet and network connectivity for the means described in this document. Users will be sharing the network with others in the College, and therefore must be considerate of their actions and how it may affect others. Academic use by the College and its students is important and will be given a priority over any other use. Any action (intentional or unintentional) that would impair the function of the network or systems is prohibited. This includes actions that affect the overall performance of the network. Any action that would deny or impair network service to another system or user is prohibited.

1. TC3 shall have the right to monitor users' bandwidth consumption at any time and on an ongoing basis, and to limit excessive bandwidth consumption (as determined by TC3) by any means available to TC3, including suspension or termination of service

2. Use of Internet through TC3 for any illegal activities is strictly prohibited. Any receipt, transmission or retransmission of software or data must observe copyright laws, license restrictions, and College policies.

3. All server activity must be approved by the Office of Campus Technology. Operation of any unapproved server

related application is prohibited. This includes, but is not limited to sharing files on your computer, FTP, web server and other systems that serve information.

4. Network service may be interrupted on occasion. TC3 will work to restore service as soon as possible. However, TC3 is not responsible for any losses or damages caused by service interruptions or other failures in College equipment.

Acceptable and Unacceptable Uses of Resources

The following are examples of acceptable and unacceptable uses of computing resources, including, but not limited to, email, all campus networks, systems, and the Internet. This listing is not intended to be inclusive.

Examples of acceptable uses:

- activities promoting educational collaboration and information sharing
- research and collaboration by students and faculty related to course work
- communication with scholars and educators in connection with teaching and research
- grant administration and application
- involvement in professional organizations related to the user's teaching, research, or professional activities

Examples of unacceptable uses:

- users shall not create, display, transmit, or make accessible threatening, racist, sexist, obscene, offensive, harassing language, electronic communications, including broadcasting unsolicited messages, sending unwanted email, or other related uses. Please remember the College’s policies against discrimination and harassment.
- engaging in any illegal activity
- commercial profit-making activities or advertising
- sending chain letters
- engagement in an activity that affects network performance or causes congestion
- malicious use
- Using another user's ID or password, with or without consent
- using electronic communications to forge an academic document
- using electronic communications to steal another individual's work or otherwise misrepresent one's own work
- forging, fraudulently altering, or wilfully falsifying electronic mail headers or electronic information generated as, maintained as, or otherwise identified as College records in support of electronic communications
- intentional introduction of a computer "virus" or other disruptive/destructive program into the system
- promoting partisan political or religious views

- removing personal information as defined in the TC3 Information Security Protocol is prohibited without written approval from the owner of the data and both the Registrar and Dean of Campus Technology.

Data Loss

If the College suspects that College information has been compromised it will use all necessary measures to recover this information. There are many laws, especially in New York state, that describe the process for dealing with lost or stolen data. The College will comply with these laws and its own policies and procedures to safeguard the intellectual property and confidentiality of its data and records. Employees must report the loss of data, as soon as they are aware of the loss, to the Office of Campus Technology.

Laptop, Smartphone, USB and Portable Devices

Data from the administrative databases may not be removed from the network/servers without complying with the proper procedures for encryption and security. Users must obtain permission through Campus Technology. These devices must also be configured with good antivirus and other measures for securing this information.

Note: Users, like faculty, may keep grade book like records on their laptops, personal computers or USB memory devices in order to conduct the business of teaching. Proper password and security standards should be followed. Campus Technology will provide an information sheet on best practices for securing this information. This kind of information is defined by FERPA as sole possession.

Privacy

Each user account is protected from unauthorized access by requiring the use of a unique password to identify the legitimate user. No user will snoop, hack, or be involved in any other actions that interfere with the privacy of others. Users must abide by the system's security mechanisms in a manner that preserves the privacy of themselves and others. The College will make all reasonable attempts to maintain the integrity of the system. However, it shall not be held liable for intentional invasions by others.

Although information passing over the College network or stored in user accounts may be accessed by system personnel for purposes of network management, the content of files and transmissions will not be viewed or monitored on a regular basis, except in those cases where the College has reasonable cause to believe that an account or system is being used by other than an authorized user or is being used in violation of applicable federal, state, or local law or of College procedures, protocols, or policy.

Not withstanding other statements made in this document, the College retains all rights to its systems and information.

Piracy

The copying of copyrighted materials (including incorporation into or attachment to an electronic work product), whether from software, hard copy, or otherwise, is prohibited without the express written consent of the copyright owner. Unlicensed software may not be installed on College equipment.

Local-Regional-Internet Network Use

The College's computer resources include an electronic network of computers that are linked together via a complex system of electronic components, computers, cabling, and information. These systems may also be joined to the outside world via external networks including SUNYNet, Third Party Providers, and the Internet.

Users of these resources are bound by the College's policies and the policies of the aforementioned networks. Copies of applicable use policies will be available in the Office of Campus Technology and the Dr. Lucille S. Baker Learning Commons.

Appendix 3: Network User Accounts and Email Address Change of Employment Procedures

Adopted 7/1/2017

Termination

In the event of a termination, the employee's Network User Account and Email Address will be deactivated no later than their last date of employment.

Resignations

In the event of a resignation, the employee's Network User Account and Email Address will be deactivated at the end of their last date of employment.

Internal Resignation or Transfer

It will be at the discretion of the current supervisor, in consultation with the College's Information Security Officer, to allow an employee to retain their existing username and email address when an employee changes to a new department within the College. The existing network account and email address will be deactivated using the same procedure as a resignation. New credentials will be issued using the same procedure as a new hire.

Retirees

In the event of a retirement, the employee's Network User Account and Email Address will be deactivated at the end of their last date of employment.

The College President may authorize an employee to retain his/her current Tompkins Cortland email address at the time of retirement under the following protocol:

- Human Resources must have written approval from the College President, or designee.
- The Policy on Acceptable Use of Computer Resources must be provided to the retiree.
- The retiree must purge their inbox of all sensitive email related to their former role.
- The retiree must sign a written agreement/form, which includes an attestation that s/he will not hold herself/himself out as an active employee of the College.
- The retiree must forward relevant email to current College staff as appropriate.

All network permissions will be removed other than those required to access email. Any retiree account which has been inactive (not logged into) for more than 180 days will be deleted without prior notification. The display names of retirees will be suffixed with "Retired" (e.g. *Jane Doe – Retired*)

Retention of Deactivated Accounts

Within 30 days of deactivation, email contents will be deleted permanently. The current supervisor may elect that an auto-response message be setup on the email account. The CIO, or designee, may elect to retain a Network User Account in the event that it is required for the proper operation of existing IT systems/services until such time that a transition plan is implemented.

Employees as Students

An employee taking credit classes during their transition from employment will need to create student account. Campus Technology staff will make every effort to ensure the transition to the student account does not cause a disruption of their academic work.

Appendix 4: Disaster Recovery, Backup Procedures, and Security Overview

Purpose/Philosophy

This document focuses on the recovery of the electronic data maintained by the Office of Campus Technology for the administrative systems on Campus. Disaster recovery for the computer systems on campus can mean a file needs to be restored or the entire system and our location has been compromised and we may have to move to another site. The College has taken the view that it must ensure the data and software are backed up in the case of nearly any event that takes place. It has been decided not to have a spare/hot site with new hardware ready to go. The primary consideration for this is the costs to maintain two sets of servers, and the secondary reason is that the equipment we use is readily accessible through many vendors. If there is a major problem with our location, we will be purchasing equipment as quickly as possible, installing our software and loading our data at the new site to be determined by management, focusing on our most critical systems first. Communications are critical to any organization. If an emergency exists and our ability to communicate with our staff and students has diminished, we will work first to reestablish this service.

Backup Procedures

Systems – A complete backup is performed on all servers that contain live data or software. Test systems are not backed up as a rule. Backups are passworded for security purposes.

Storage – Backups are maintained on site and in two off-site locations.

Cycle – We save our backups on a monthly, weekly, and daily basis. The last two monthly backups are maintained. The oldest is saved on campus, and the most current is saved at the First National Bank of Dryden at the Cortland location. The current daily backup is taken off site to the First National Bank of Dryden at the Dryden Branch location. Other daily backups for the past seven days are maintained on campus. Each morning the daily backup from two days ago is returned, so a daily backup is off site at all times. A weekly set of tapes are stored at an alternate building on campus.

Software – In order for us to restore a backup on a new system we must be able to load the current version of the operating system, backup/restore software, application software and all current patches that may apply. Copies of these are maintained on campus and at the two remote sites.

Databases – All of our databases are stored on database servers. Each night a routine is run to backup the databases to disk, then these are copied to our backup tapes.

Security Measures

Antivirus – The College will maintain a network-wide managed anti-virus software runs on every PC and server. Updates are automatically provided to these machines via a server that consistently gets the updates from the Internet. As machines connect to our LAN it looks for and loads any updates that our server has received.

Spyware – The College will maintain a network-wide managed anti- spyware and malware software running on every PC and server. This software monitors for spyware and malware.

Firewalls – We have deployed firewalls that protect each of our internal networks, administrative, academic, and wireless.

Microsoft Active Directory – We use MS-AD for our administrative network. Users are required to use "strong" passwords, and these require changing every 60 days.

Encryption – In the cases where sensitive data is transmitted, Campus Technologywill use encryption standards to protect its data. Passwords are encrypted using Microsoft standards for Active Directory Servers.

SSL3 – Any personally identifiable information passing over the Internet is encrypted with SSL3 using VeriSign as our certificate authority.

Doors – All of our servers and our primary communication equipment are located in our server room and are protected by two locked doors.

Appendix 5 – Student e-mail Protocol

Tompkins Cortland Community College
Student e-mail Protocol and Procedures
March 17, 2008

Introduction

Tompkins Cortland Community College provides electronic mail ("e-mail") for students engaging in activities related to instruction, research, and administrative support. Student e-mail is an official communication mechanism for the College. Students should regularly check e-mail to ensure they are receiving important communications, which will include notices regarding financial aid, grades, faculty contact, and College emergencies.

Each student is issued a mymail.tc3.edu address through Windows Live. This is the account used for College business and official College communications to students. Once a student has registered, the e-mail account username and password will be provided through My.Info and by secure e-mail. It will be sent to the home email address the student supplied during the application process. The College e-mail address will be yourinitials@mymail.tc3.edu (e.g., abc001@mymail.tc3.edu). If a student has not received their account information within a week of registering, they should contact TC3SE@tc3.edu , the Help Desk at Ext. 4270, Room 208, or http://www.tc3.edu/dept/it/.

The College expects students to check their mymail.tc3.edu account regularly for College communications. Students can access their e-mail from anywhere by connecting to mail.live.com. Please be aware, if a student does not log into their mymail.tc3.edu account for 365 days, the mail in their inbox will be deleted.

Accountability

Students are ultimately responsible for any official College communication sent to their mymail.tc3.edu email account. It is in their best interest to make sure their e-mail account is used only by them, and that their password is known only to them. When e-mail is used at a "public" workstation (as in the Learning Commons), students should be careful to log off after using e-mail. The use of e-mail for illegal or unethical purposes, for abusive and harassing activities or other violations of the rights of others, or for purposes inconsistent with College policy or regulation may result in termination of e-mail access, disciplinary action, or dismissal (see Tompkins Cortland Community College Code of Student Conduct).

Security

Security of e-mail is important. The College invests a great deal of time and energy to secure communications to the best of its ability. However, much of the responsibility lies with the user of the system. E-mail sent over the Internet is not encrypted and is substantially less secure than mail sent through the United States Postal Service, or communication through a secure channel on a web site.

For additional information regarding anti-spam and anti-virus software protection through WindowsLive, go to http://get.live.com/edu/mail.

Expectations and appropriate use of student e-mail

Users shall not create, display, transmit, or make accessible threatening, racist, sexist, obscene, offensive, annoying or harassing language, electronic communications, including broadcasting unsolicited messages, sending unwanted e-mail, or impersonating other users. Please see www.tc3.edu/dept/hr/aa_policy.asp for the College's policies regarding discrimination and harassment.

E-mail is not appropriate for transmitting sensitive or confidential information unless an appropriate level of security and access privileges is utilized. All use of e-mail will be consistent with local, state, and federal law, including the Family Educational Rights and Privacy Act of 1974 (FERPA).

System issues will be managed by the Campus Technology Department.

Instructor policies and educational uses of e-mail

Instructors may set policies defining how students use e-mail in their classes, including requiring students to check their e-mail on a regular basis.

Responsible e-mail practice

Please apply common sense and civility to the use of e-mail. Responsible e-mail practice includes:

- Identify yourself clearly and accurately in all electronic communications. Concealing or misrepresenting your name or affiliation to disassociate yourself from your communication is never appropriate.
- Respect and maintain the integrity of the original author(s). Alteration of the source of electronic mail, message, or posting is unethical and possibly illegal. Treat e-mail files and attachments as private and confidential, unless the author(s) make them explicitly available to others.
- Use care that your use of e-mail does not disseminate computer viruses or other programs that may damage or place excessive load on e-mail or other College resources.
- Refrain from sending chain e-mail and SPAM.

Broadcast (bulk) e-mail guidelines

Only individuals specifically authorized may send broadcast e-mail to groups of TC3 students. Under no circumstances may an individual use broadcast -mail for personal purposes.

1) **Broadcast e-mails**

are for general announcements and business-related communications to students. All campus broadcast e-mails are limited to messages approved by one of the deans or a designee. All broadcast e-mail must be signed with the sender's name and/or department.

2) **Surveys**

all surveys conducted using e-mail or other forms of contact need to meet the TC3 Human Subjects guidelines, which generally means approval through the Institutional Research office: http://www.tc3.edu/dept/ir/guidelines.asp. In addition, the guidelines state that any surveys of minors require additional protection (permission from parents) so they are not usually included in surveyed populations. This means in most cases students under the age of 18 should not be surveyed by anyone.

3) "**Emergency Alert" and "Critical Information" e-mails**

are used for situations involving potentially serious disruptions of regular activities or threats to the health and well-being of faculty, staff, or students. This will also be used to advise the TC3 community of situations that may inconvenience them, require some action on their part, or require their increased vigilance for non-violent crime, but which do not involve major disruptions of regular activities. Select individuals in the safety and security office, office of external programs and communication, dean of student life office, residence life, and facilities Management are authorized to initiate "Emergency Alert" and "Critical Information" e-mails.

a) "Emergency Alert" examples include, but are not limited to the following:

- campus closing
- disaster
- campus security warns there is an imminent threat

b) "Critical Information" examples include, but are not limited to the following:

- the Inclement Weather Policy has been invoked.
- a burst water line has required the shutdown of water service to a building
- we will be shutting off power to a building in 45 minutes to replace a failing transformer
- new, dangerous computer virus: delete all e-mails with the subject "whatever"
- several thefts have taken place in a specific location in the past 24 hours
- the individual whose picture is attached is suspected of breaking into cars in a parking lot

All Emergency Alert and Critical Information e-mails must be signed with the senders name and/or department.

Procedure for sending broadcast (bulk) email to students

1. Complete the Request for Authorization to Send Broadcast Email to Students form located at the end of this document. Submit the completed form to your Dean for approval.

    a. Select the appropriate category for broadcast emails:

        i. Routine – these are emails that will be sent to students on a regular basis. Weekly, monthly, etc. This may include newsletter or bulletin board type information. Each area should try to coordinate these so all information can be sent once at the designated time interval to minimize the number of emails sent to students.

        ii. Occasional – these are emails that will be sent for random information on an irregular basis.

2. Upon approval, the Dean designee will send the email to the students either by asking you to sign in to their computer, or by sending from a monitored department email address. The purpose for this is to allow students to respond to the sent emails.

Request for Authorization to Send Broadcast Email to Students

Please complete this form to be given access to student email lists. Email sent to students must be in accordance with the college's Student e-mail Protocol and Procedures listed above.

Staff Member: _____

Frequency ☐ Occasional ☐ Routine
(Please refer to the description of these two categories on the above instructions.)

Please describe the purpose of the email

Target Audience: (eg. all students, commuter students, part-time students, etc.*)

I have read and agree to abide by the Tompkins Cortland Community College
Student e-mail Protocol and Procedures.

_____ _____
Staff Member Signature Date

This form must be signed by your Dean to indicate approval.

_____ _____
Dean or Designee Date

*Please note that your audience list may need to be programmed by Campus Technology and as such will not be immediately available. Campus Technology will provide you with a time estimate for the creation of custom lists.