Tompkins Cortland Community College Information Security Protocol

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

Purpose

Employee management and t

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- The College will promptly dispose of outdated personal information in compliance with state and federal regulations.

Pedure p(a)4(sol befr)-5(ill)-3owced tomio(it)-3(oroc)7o(ntra)5(c)4((oroc54(ompl)-3(anci)-3(e)4(with t)-3(he)4(pro

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 maintainingio3t

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

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

related application is prohibited. This includes, but is not limited to sharing files on your computer, FTP, w

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

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

Adopted 7/1/2017

Termination

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

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.