Cybersecurity

FT_IT_UT_35

Responsible Officer
Rick Snider
Responsible Office
IT
Last Revision
2019-12
Re-evaluation Date
2021

Policy Statement

All users of the CU infrastructure, which includes computers, networks, and data, are to comply with the standards defined below.

Policy Procedures

1. Definition

The use of the term “university” is in reverence to the following organization: Carolina University.

2. Introduction

This Cyber Security Policy is a formal set of rules by which those people who are given access to university technology and information assets must abide.

The Cyber Security Policy serves several purposes. The main purpose is to inform university users: employees, contractors and other authorized users of their obligatory requirements for protecting the technology and information assets of the university. The Cyber Security Policy describes the technology and information assets that we must protect and identifies many of the threats to those assets.

The Cyber Security Policy also describes the user’s responsibilities and privileges. What is considered acceptable use? What are the rules regarding Internet access? The policy answers these questions, describes user limitations and informs users there will be penalties for violation of the policy. This document also contains procedures for responding to incidents that threaten the security of the university computer systems and network.

3. What Are We Protecting

It is the obligation of all users of the university systems to protect the technology and information assets of the university. This information must be protected from unauthorized access, theft and destruction. The technology and information assets of the university are made up of the following components:

- Computer hardware, CPU, disc, Email, web, application servers, PC systems, application software, system software, etc.
- System Software including: operating systems, database management systems, and backup and restore software, communications protocols, and so forth.
- Application Software: used by the various departments within the university. This includes custom written software applications, and commercial off the shelf software packages.
- Communications Network hardware and software including: routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, and associated network management software and tools.

4. Definitions

Externally accessible to the public. The system may be accessed via the Internet by persons outside of the university without a logon id or password. The system may be accessed via dial-up connection without providing a logon id or password. It is possible to “ping” the system from the Internet. The system may or may not be behind a firewall. The CU website (carolinau.edu) is an example of this type of system.

Non-Public, Externally accessible. Users of the system must have a valid logon id and password. The system must have at least one level of firewall protection between its network and the Internet. The system may be accessed via the Internet or a private Intranet. The Jenzabar and Concourse Hosting systems are systems of this type.

Internally accessible only. Users of the system must have a valid logon id and password. The system must have at least two levels of firewall protection between its network and the Internet. The system is not visible to Internet users. It may have a private Internet (non-translated) address and it does not respond to a “ping” from the Internet. A private intranet Web Server is an example of this type of system. CU’s Active Directory (AD) servers are examples of this type of system.

Chief Information Officer. The Chief Information Officer (CIO) serves as the head of IT Technology for the university.

Security Administrator. Either the CIO or an employee of IT shall be designated as the Security Administrator for the university.

5. Threats to Security

5.1 Employees and Students

One of the biggest security threats are users. They may do damage to your systems either by accident or even on purpose. You have to layer your security to compensate for that as well. You mitigate this by doing the following.

- Only give out appropriate rights to systems.
- Don’t share accounts to access systems. Never share your login information with co-workers.
- When employees are separated or disciplined, you remove or limit access to systems.
- Advanced – Keep detailed system logs on all computer activity.
- Physically secure computer assets, so that only staff with appropriate need can access.

5.2 Amateur Hackers and Vandals.

These people are the most common type of attackers on the Internet. The probability of attack is extremely high and there is also likely to be a large number of attacks. These are usually crimes of opportunity. These amateur hackers are scanning the Internet and looking for well known security holes that have not been plugged. Web servers and electronic mail are their favorite targets. Once they find a weakness they will exploit it to plant viruses, Trojan horses, or use the resources of your system for their own means. If they do not find an obvious weakness they are likely to move on to an easier target.

5.3 Criminal Hackers and Saboteurs.

The probability of this increases yearly. The skill of these attackers is medium to high as they are likely to be trained in the use of the latest hacker tools. The attacks are well planned and are based on any weaknesses discovered that will allow a foothold into the network. Email is a primary conduit for malware and ransomware threats, so all users must exercise diligence to ensure they do no indivertibly allow unauthorized access to the CU network.

6. User Responsibilities

This section establishes usage policy for the computer systems, networks and information resources of the office. It pertains to all employees and contractors who use the computer systems, networks, and information resources as business partners, and individuals who are granted access to the network for the business purposes of the university.

6.1 Acceptable Use

User accounts (employees and students) on university computer systems are to be used only for business of the university and not to be used for personal activities. Unauthorized use of the system may be in violation of the law, constitutes theft and can be punishable by law. Therefore, unauthorized use of the university computing systems and facilities may constitute grounds for either civil or criminal prosecution.

Users are personally responsible for protecting all confidential information used and/or stored on their accounts. This includes their login IDs and passwords. Furthermore, they are prohibited from making unauthorized copies of such confidential information and/or distributing it to unauthorized persons outside of the university.

Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to university systems for which they do not have authorization.

Users shall not attach unauthorized devices on their PCs or workstations, unless they have received specific authorization from the employees’ manager and/or the university IT designee.

Users shall not download unauthorized software from the Internet onto their PCs or workstations.

Users are required to report any weaknesses in the university computer security, any incidents of misuse or violation of this policy to their immediate supervisor or the CIO.

6.2 Use of the Internet

The university will provide Internet access to employees, students, and contractors who are connected to the internal network.

The Internet is a business tool for the university. Employees should use it for business-related purposes such as educational purposes, communicating via electronic mail with suppliers and business partners, obtaining useful business information and relevant technical and business topics.

The Internet service may not be used for transmitting, retrieving or storing any communications of a discriminatory or harassing nature or which are derogatory to any individual or group, obscene or pornographic, or defamatory or threatening in nature for “chain letters” or any other purpose which is illegal or for personal gain.

6.3 Monitoring Use of Computer Systems

The university has the right and capability to monitor electronic information created and/or communicated by persons using university computer systems and networks, including email messages and usage of the Internet. It is not the university policy or intent to continuously monitor all computer usage by employees or other users of the university computer systems and network. However, users of the systems should be aware that the university may monitor usage, including, but not limited to, patterns of usage of the Internet (e.g. site accessed, on-line length, time of day access), and employees’ electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with university policy.

7. Access Control

A fundamental component of our Cyber Security Policy is controlling access to the critical information resources that require protection from unauthorized disclosure or modification. The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources. Access controls exist at various layers of the system, including the network. Access control is implemented by logon ID and password. At the application and database level, other access control methods can be implemented to further restrict access. The application and database systems can limit the number of applications and databases available to users based on their job requirements.

7.1 User System and Network Access – Normal User Identification

All users will be required to have a unique login ID and password for access to systems. The user’s password should be kept confidential and MUST NOT be shared with management & supervisory personnel and/or any other employee whatsoever. All users must comply with the following rules regarding the creation and maintenance of passwords:

- Password should not be found in any English or foreign dictionary. That is, do not use any common name, noun, verb, adverb, or adjective. These can be easily cracked using standard “hacker tools”.
- Passwords should not be posted on or near computer terminals or otherwise be readily accessible in the area of the terminal.
- Password must be changed every 90 days.
- User accounts will be frozen after 7 failed logon attempts.
- Employee accounts will be terminated upon the employee’s end of employment.
- Student accounts will be terminated after three semesters of non-registration, or within one month of graduation or when a student withdraws from the university.

Users are not allowed to access password files on any network infrastructure component. Password files on servers will be monitored for access by unauthorized users. Copying, reading, deleting or modifying a password file on any computer system is prohibited.

Non-IT users will not be allowed to logon as a System Administrator. Users who need this level of access to production systems must request such access from the CIO.

Employee Login IDs and passwords will be deactivated as soon as possible if the employee is terminated, fired, suspended, placed on leave, or otherwise leaves the employment of the university office.

Supervisors / Managers shall immediately and directly contact the CIO to report change in employee status that requires terminating or modifying employee login access privileges.

Employees who forget their password must call the IT department to get a new password assigned to their account.

Employees will be responsible for all transactions occurring during Logon sessions initiated by use of the employee’s password and ID. Employees shall not logon to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

7.2 System Administrator Access

System Administrators, network administrators, and security administrators will have administrator access to host systems, routers, hubs, and firewalls as required to fulfill the duties of their job.

All system administrator passwords will be changed immediately after any employee who has access to such passwords is terminated, fired, or otherwise leaves the employment of the university.

7.3 Special Access

Special access accounts are provided to individuals requiring temporary system administrator privileges in order to perform their job. These accounts are subject to monitoring by the university and require the permission of the CIO.

7.4 Connecting to Third-Party Networks

This policy is established to ensure a secure method of connectivity provided between the university and all third-part companies and other entities required to electronically exchange information with university.

“Third-party” refers to vendors, consultants and business partners doing business with university, and other partners that have a need to exchange information with the university. Third-party network connections are to be used only by the employees of the third-party, only for the business purposes of the university. The third-party university will ensure that only authorized users will be allowed to access information on the university network. The third-party will not allow Internet traffic or other private network traffic to flow into the network. Third-party networks must be connected by a branch-to-branch office VPN (always up) or an on-demand VPN.

This policy applies to all third-party connection requests and any existing third-party connections. In cases where the existing third-party network connections do not meet the requirements outlined in this document, they will be re-designed as needed.

All requests for third-party connections must be approved by the CIO.

7.5 Connecting Devices to the Network

Any non-CU computer connected to the university network must have active malware protection. All CU-owned computers must also have active malware protection. Other devices include network infrastructure devices used for network management and monitoring, tablets and smartphones, printers, and student-owned gaming systems.

Users shall not attach to the network: non-university computers that are not authorized, owned and/or controlled by the university. Users are specifically prohibited from attaching non-university routers or Wi-Fi access points to the university network.

7.6 Remote Access

Only authorized persons may remotely access the university network. Remote access is provided to those employees, contractors and business partners of the university that have a legitimate business need to exchange information, copy files or programs, or access computer applications. Authorized connection can be a remote PC connection to the network or a remote network to university network connection. The only acceptable method of remotely connecting into the internal network is using a secure VPN.

7.7 Unauthorized Remote Access

Users may not install personal software designed to provide remote control of the PC or workstation. This type of remote access bypasses the authorized highly secure methods of remote access and poses a threat to the security of the entire network. Remote access is provided by the university through the use of Splashtop, which provides secure remote access. If remote access is necessary or desired, users may request it from the IT department.

8. Penalty for Security Violations

The university takes the issue of security seriously. Those people who use the technology and information resources of the university must be aware that they can be disciplined if they violate this policy. Upon violation of this policy, an employee of the university may be subject to discipline up to and including discharge. The specific discipline imposed will be determined by a case-by-case basis, taking into consideration the nature and severity of the violation of the Cyber Security Policy, prior violations of the policy committed by the individual, state and federal laws and all other relevant information. Discipline which may be taken against an employee shall be administered in accordance with any appropriate rules or policies and the university Policy Manual.

In a case where an accused person is not an employee or student of the university the matter shall be submitted to the CIO. The CIO may refer the information to law enforcement agencies and/or prosecutors for consideration as to whether criminal charges should be filed against the alleged violator(s).

9. Security Incident Handling Procedures

This section provides some policy guidelines and procedures for handling security incidents. The term “security incident” is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of the university network. Some examples of security incidents are:

- Illegal access of a university computer system. For example, a hacker logs onto a production server and copies the password file.
- Damage to a university computer system or network caused by illegal access. Releasing a virus or worm would be an example.
- Denial of service attack against a university web server. For example, a hacker initiates a flood of packets against a Web

server designed to cause the system to crash.
- Malicious use of system resources to launch an attack against other computers outside of the university network. For example, the system administrator notices a connection to an unknown network and a strange process accumulating a lot of server time.

Employees who believe their terminal or computer systems have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to their supervisor or the CIO immediately. The employee shall not turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the security incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem.