

INFORMATION TECHNOLOGY SECURITY POLICY

TABLE OF CONTENTS

1. **Introduction**
2. **Scope of IT Security.**
 1. Definition of Security.
 2. Domains of Security.
3. **Reasons for IT Security.**
4. **Roles and Responsibilities.**
 1. Policy Management.
 2. Policy Implementation.
 3. Custodians.
 4. Individuals.
 5. University Services.
 6. Standards and Guidelines.
5. **Policy Documentation.**
 1. Documents.
 2. Availability.
 3. Changes.
6. **Guidelines on Passwords.**
 1. Password Management.
 2. Password Administration.
 3. Password Construction.
7. **Security Awareness and Training.**
8. **Disaster Recovery.**
 1. Data Backup.
 2. Alternate Data Backup.
 3. Contingency Planning.
9. **Virus Prevention Policy.**
10. **Intrusion Detection Policy.**

1. Introduction

Charleston Southern University acknowledges an obligation to ensure appropriate security for all Information Technology (IT) data, equipment, and processes in its domain of ownership and control. This obligation is shared, to varying degrees, by every member of the university. The principles of academic freedom apply to this policy, and this policy is not intended to limit or restrict those principles. These policies apply to all departments within the university. Each department within the university should apply this policy to meet their information security needs. The policy is written to incorporate current technological advances.

This document will:

1. Enumerate the elements that constitute Information Technology security.
2. Explain the need for IT security.
3. Specify the various categories of IT data, equipment, and processes subject to this policy.
4. Indicate, in broad terms, the IT security responsibilities of the various roles in which each member of the university may function.
5. Indicate appropriate levels of security through standards and guidelines.

2. Scope of IT Security.

1. Definition of Security.

Security can be defined as "the state of being free from unacceptable risk". The risk concerns the following categories of losses:

- Confidentiality of Information.
- Integrity of data.
- Assets.
- Efficient and Appropriate Use.
- System Availability.

Confidentiality refers to the privacy of personal or corporate information . This includes issues of copyright.

Integrity refers to the accuracy of data. Loss of data integrity may be gross and evident, as when a computer disc fails, or subtle, as when a character in a file is altered.

The assets that must be protected include:

- Computer and Peripheral Equipment.

- Communications Equipment.
- Computing and Communications Premises.
- Communications utilities.
- Supplies and Data Storage Media.
- System Computer Programs and Documentation.
- Application Computer Programs and Documentation.

Efficient and Appropriate Use ensures that University IT resources are used for the purposes for which they were intended, in a manner that does not interfere with the rights of others.

Availability is concerned with the full functionality of a system (e.g. finance or payroll) and its components.

The potential causes of these losses are termed "threats". These threats may be human or non-human, natural, accidental, or deliberate.

2. Domains of Security.

This policy will deal with the following domains of security:

- Computer system security: CPU, Peripherals, OS. This includes data security.
- Physical security: The premises occupied by the IT personnel and equipment.
- Operational security: Environment control, power equipment, and operation activities.
- Procedural security by IT, vendor, management personnel, as well as ordinary users.
- Communications security: Communications equipment, personnel, transmission paths, and adjacent areas.

3. Reasons for IT Security.

Confidentiality of information is mandated by common law, formal statute, explicit agreement, or convention. Different classes of information warrant different degrees of confidentiality.

The hardware and software components that constitute the university's IT assets represent a sizable monetary investment that must be protected. The same is true for the information stored in its IT systems, some of which may have taken huge resources to generate, and some of which can never be reproduced.

The use of university IT assets in other than in a manner and for the purpose for which they were intended represents a misallocation of valuable university resources, and possibly a danger to its reputation or a violation of the law.

Finally, proper functionality of IT systems is required for the efficient operation of the university. Some systems, such as the HR, Finance, Student Records, Jenzabar, and Library systems are of paramount importance to the mission of the university. Other systems (e.g. someone's PC) are of less importance.

4. Roles and Responsibilities.

1. Policy Management.

Approval of the IT Security Policy is vested with the Chief Information Officer (CIO), the Executive Technology Committee, the Cabinet and the President of the university.

Formulation and maintenance of the policy is the responsibility of the CIO.

2. Policy Implementation.

- Each member of the university will be responsible for meeting published IT standards of behavior.
- IT security of each system will be the responsibility of its custodian.

3. Security Custodians.

- IT will be the security custodian of all strategic system platforms.
- IT will be the security custodian of the strategic communications systems.
- IT will be the security custodian of all central computing laboratories.
- Offices and departments will be the security custodian of strategic applications under their management control (e.g. Finance, HR, Library).
- Individuals will be the security custodians of desktop systems under their control.

4. Individuals.

All ordinary users of University IT resources:

1. Will operate within the guidelines set forth within the Technology Manual.
2. Are responsible for the proper care and use of IT resources under their direct control.

5. University Services.

It is recognized that various departments of the university provide services that relate to IT security, both directly and indirectly. It is expected that there will be collaboration between these departments and IT in generation of standards and implementation of the policy. Some of these departments and their services are:

- Human Resources: Personnel selection, induction, and exit processing.

- Registrar: Policies concerning confidentiality privacy, and copyright.
- Campus Services: Physical building security.

6. Standards and Guidelines.

Standards (mandatory) and guidelines (suggestions) will be published as attachments to this policy to assist ordinary users and system custodians to meet their IT security responsibilities. These standards and guidelines, though presented as attachments, are an integral part of this university's IT Security Policy and therefore define it in detail.

These Standards and Guidelines will appear under the following classifications:

- Personal behavior.
- Strategic systems.
 1. Computer.
 2. Communications.
- Desktop (personal) systems.
- School-based systems.

5. Policy Documentation.

1. Documents.

This policy is enunciated by twelve documents:

- Campus Computing Policy
- Microcomputer Purchase, Repair and Maintenance Policy
- Copyright Laws and Software License Agreement Policy
- Administrative Computer Policy
- Electronic Communications Policy and Procedures
- Electronic Communications Code of Conduct
- Wireless Network Policy
- Procedures and Protocols under the USA –Patriot Act Policy
- Equipment Disposal Policy
- Remote Access Policy
- Student E-Mail and WEB Policy
- CSU Gramm-Leach-Bliley Act, Information Security Program

2. Availability.

It is intended that this IT Security Policy be publicly accessible in its entirety via the University's World Wide Web Home Page. There is the requirement that all users of University IT resources be familiar with relevant sections of this policy.

3. Changes.

The IT Security Policy is a "living" document that will be altered as required to deal with changes in technology, applications, procedures, legal and social imperatives, perceived dangers, etc.

6. Guidelines on Passwords.

1. Password Management.

- Passwords should be memorized - **never** written down.
- Passwords belong to individuals and must **never** be shared with anyone else.
- Passwords should be changed every 3 months, or immediately if compromised.

2. Password Administration.

- System Custodians should regularly run password cracking software against their password files to identify weak passwords.
- New or changed passwords must be given in writing only to the identified user - never over the telephone or via email.

3. Password Construction.

Password security isn't just a matter of thinking up a nice word and keeping it to yourself. You must choose a password that will be difficult for someone else to guess or crack.

We often have a tendency to forget passwords, so we choose something that has particular relevance to ourselves: the name of a loved one, our favorite car, sport, or ice cream, etc. Anyone knowing a little about us can make a list of these words and easily crack the password. All-digit passwords usually fall into this category - birth dates and phone numbers.

Observe the following guidelines when choosing your password:

- A password should be at least 6 characters long.
- NEVER make your password a name or something familiar, like your pet, your children, or partner. favorite authors and foods are also guessable.
- NEVER, under any circumstances, should your password be the same as your username or your real name.
- DON'T use words that can be associated with you
- Do not have a password consisting of a word from a dictionary. Most basic cracking programs contain over 80000 words, and plenty of variations.
- Try to have a password with a number or mixed case letters. Simple substitutions like a '1' for an 'i', and '0' for an 'O' are easily guessed. Add a '%' or '\$' to the middle of the password.

- Choose something you can remember, that can be typed quickly and accurately and includes characters other than lowercase letters.

Examples:

- Made-up "words" - chok-bel (can be "pronounced", has a punctuation character)
- Personal acronyms - ihc,alt (I Hate Coffee, And Love Tea)
- Invert syllables - sick.sea (instead of 'seasick')

7. Security Awareness and Training.

An effective level of awareness and training is essential to a viable information security program. Employees who are not informed of risks or of management's policies and interest in security are not likely to take steps to prevent the occurrence of violations. As of June 1, 2004, all new employees at CSU must have computer security awareness training provided by the CIO's office. Employees are informed of this when they finish with their initial benefit training and are then sent to Administrative Services to schedule this training. Departments shall also provide an ongoing awareness and training program in information security and in the protection of computer resources for all personnel whose duties bring them into contact with critical or sensitive university computer resources.

Upon termination of a person who occupies a position of special trust or responsibility, or is working in a sensitive area, Administrative Services shall immediately revoke all access authorizations to computer resources.

8. Disaster Recovery.

It is prudent to anticipate and prepare for the loss of information processing capabilities. The plans and actions to recover from losses range from routine backup of data and software in the event of minor losses or temporary outages, to comprehensive disaster recovery planning in the preparation for catastrophic losses of computer resources.

1. Data Backup.

On-site backup is employed to have current data readily available in machine-readable form in the production area in the event operating data is lost, damaged, or corrupted; and to avoid having to reenter the data from source material. Data and software essential to the continued operation of critical department functions must be backed up. The security controls over the backup resources must be as stringent as the protection required of the primary resources.

2. Alternate Data Backup.

The backup procedures on the multi-user computer systems and departmental servers are designed to protect against data losses caused by hardware failures and other disasters. The frequency and timing of these backups may not provide sufficient protection to meet end-user requirements for data backup. Therefore, it is strongly recommended that end-users include a data backup step in their information processing procedures, and not to depend on single backup procedure to provide all protection.

3. Contingency Planning.

Contingency plans, or disaster control plans, specify actions management have approved in advanced to achieve each of three objectives: to identify and respond to disasters; to protect personnel and systems; and to limit damage. The backup plan specifies how to accomplish critical portions of the mission in the absence of a critical resource such as computers. The recovery plan directs recovery of full mission capability.

9. Virus Prevention Policy.

The wilful introduction of computer viruses or disruptive/destructive programs into the University environment is prohibited, and violators may be subject to prosecution.

All desktop systems that connect to the network must be protected with an approved, licensed anti-virus software product that is kept updated according to the vendor's recommendations.

All servers and workstations that connect to the network and that are vulnerable to virus or worm attack must be protected with an approved, licensed anti-virus software product that is kept updated according to the vendor's recommendations.

Headers of all incoming data including electronic mail will be scanned for viruses by the email server where such products exist and are financially feasible to implement. Outgoing electronic mail will be scanned where such capabilities exist.

Where feasible, system or network administrators should inform users when a virus has been detected.

Virus scanning logs must be maintained whenever email is centrally scanned for viruses.

10. Intrusion Detection Policy.

- Intruder detection must be implemented on all servers and workstations containing data classified as high risk.

- Operating system and application software logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems must be enabled.
- Server, firewall, and critical system logs should be reviewed frequently. Where possible, automated review should be enabled and alerts should be transmitted to the administrator when a serious security intrusion is detected.
- Intrusion tools should be installed where appropriate and checked on a regular basis.