

CHARLESTON SOUTHERN UNIVERSITY

INFORMATION SECURITY POLICY FOR ALL UNIVERSITY FACULTY & STAFF COMPUTER NETWORK USERS

I. PURPOSE

The University's information is one of its vital assets. The purpose of the Information Security Policy is to protect this asset by establishing employee responsibility for the security of the University's information. This policy applies to all University full-time, part-time and miscellaneous wage employees.

II. POLICY STATEMENT

It is the policy of the University to protect its information assets and allow the use, access and disclosure of such information only in accordance with University interests and applicable laws and regulations. All University employees providing services or working with the University's information are responsible for protecting it from unauthorized access, modification, destruction or disclosure. "The University's information" is defined as any information within its boundaries, including information which it may not own but which is governed by laws and regulation which the University is held accountable. It includes all student record data, all personnel data, all University financial data, all student life data, all departmental administrative data, all alumni and donor data, and all other data that pertains to, or supports the administration of the University. This data may be facts, records, reports, telephone numbers, addresses, planning assumptions or any information meant only for internal use. This policy encompasses the safekeeping of the University's information in whatever physical form, such as printed, audio, video and electronic.

III. IMPLEMENTATION

Departments shall administer the information security program that protects information under their control. The protection of the University's information must be part of the overall campus plan. Departments are responsible for:

- Establishing personnel access and utilization requirements and provide to Administrative Services the defined criteria for access control
- Maintaining controls necessary to satisfy information retention requirements

- Determining the value of proprietary information to the functioning of the University and defining reasonable requirements for protecting the asset
- Developing a workable plan in conjunction with Administration Services for resuming operations in the event a disaster destroys the information
- Specifying information control and protection requirements to be adhered to by employees processing and using the information
- Monitoring compliance and enforcing the policy
- Reporting violations
- Ensuring compliance with campus technology and technology security policies and procedures

However, since information security measures must cover the entire flow of information in the University, the implementation of the information security policy cannot be delegated to only Departments. All employees are custodians of the University's information. All employees must adhere to established procedures to ensure that they use the University's information only as required by the normal functions of their duties and that they safeguard it properly according to its sensitivity, proprietary and/or critical nature.

In accordance with federal regulations, passwords will now need to be changed every 90 days.

IV. VIOLATIONS OF THIS POLICY

Employees who violate this policy WILL be subject to disciplinary action in accordance with University due process.

I have read the University security policy located at <http://www.csuniv.edu/securitydocuments.html> and will comply with all sections during any computing access to and from the University's network and computing facilities.

PRINT FULL NAME

SIGNATURE

DATE