Information Security Policy

Purpose

The risk to Charleston Southern University, its employees and students from data loss and identity theft is of significant concern to the University and can be reduced only through the combined efforts of every employee and contractor. Charleston Southern University adopts this sensitive information policy to help protect employees, students, contractors and the University from damages related to the loss or misuse of sensitive information.

This policy will:

1. Define sensitive information;
2. Describe the physical security of data when it is printed on paper;
3. Describe the electronic security of data when stored and distributed; and
4. Place the University in compliance with federal law regarding identity theft protection.

This policy enables the University to protect students and employees, reducing risk from identity fraud, and minimize potential damage to the University. The program will help Charleston Southern University:

1. Identify risks that signify potentially fraudulent activity within new or existing covered accounts;
2. Detect risks when they occur in covered accounts;
3. Respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed; and
4. Update the program periodically, including reviewing the accounts that are covered and the identified risks that are part of the program.

Scope

This policy and protection program applies to employees (including student workers), volunteers, contractors, consultants, temporary workers, and other workers at Charleston Southern University, including all personnel affiliated with third parties.

Sensitive Information Policy

Definition of Sensitive Information

"Sensitive Information" refers to the facts, data, or knowledge itself regardless of the medium of its conveyance. Therefore, documents are deemed to convey or contain information and are not considered to be information per se.

Sensitive Information is to be categorized in one of the following classifications:

- Business Sensitive
- Personnel Sensitive
- Attorney-Client Privileged
- Other
For information to be considered "Sensitive Information", the information must have the potential to damage the University’s interests, or an individual’s private interests if disseminated to or obtained by persons who do not need the information to perform their jobs or other University-authorized activities. Information that is available in the public domain is generally not considered to be Sensitive Information.

The following are the categories and examples of Sensitive Information in use at the University.

**Business Sensitive Information**

The following are examples of the potential types of Business Sensitive information in use within the University: Note; this information may be the result of the University’s own business activities; it may have been provided by a vendor or sub-contractor, or a combination thereof:

- Commercial/proprietary information generally concerns information such as trade secrets, business plans, financial or cost data received from a company doing business or contemplating business with the University. Personal statements or documents supplied by contractors in the course of inspections, reviews, site visits, investigations, or audits when such information is received in confidence should also be maintained as Business Sensitive Information.

- Information produced by the University in the performance of work (basic research, Cooperative Research and Development Agreements, etc.) may be considered proprietary by the University, or a vendor or subcontractor to the University and consequently be Business Sensitive Information. Also, privileged information such as the University’s acquisition/evaluation plans, and results of evaluations and audits should be maintained as Business Sensitive Information.

- Intellectual property, contract negotiation information, procurement data, and research and development information considered proprietary are also to be considered Business Sensitive Information. Pre-decisional information involving internal University business communications or plans that have not been published or determined to be final may also be defined as Business Sensitive Information.

**Personnel Sensitive Information**

Personnel Sensitive Information includes personnel and medical files and similar files whose disclosure would constitute a clear unwarranted invasion of privacy. Examples include employee payroll data, tax reports and payments, payments for employee benefit and welfare plans, travel related costs and information, employee performance information and medical records. Note; this information usually falls under the protection of the Privacy Act of 1974. Personally Identifiable Information, such as a date of birth, Social Security Account Number or a driver’s license number, is classified as Personnel Sensitive Information.

**Attorney-Client Privileged Information**

Attorney-client privileged information or working papers prepared by an attorney in contemplation of litigation. Contact the University’s legal counsel for instructions before
creating or accepting any information that may be considered "Attorney-Client Privileged Information."

Other

The University may receive Sensitive Information from other entities, such as vendors, sub-contractors, or other business partners. Staff should always remember that the University is responsible for maintaining the same level of security for Sensitive Information delivered by an external source as is maintained for Sensitive Information developed from within the University. University personnel are encouraged to use common sense judgment in securing confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor.

Hard Copy Distribution

Physical Storage - Store documents and computer media in appropriate receptacles (Department groups should determine the level of protection required for specific documents, i.e., fire proof safes, locked files or desk drawers, etc.). Locking the office alone is not adequate.

Document Destruction - When documents containing sensitive information are discarded they will be placed inside a locked shred bin or immediately shredded using a mechanical cross cut shredding device. University records, however, may only be destroyed in accordance with the University’s records retention policy.

Locked Offices - Offices containing Sensitive Information shall be locked whenever the office is vacated and at the end of each business day.

Visitor Control - Staff should be vigilant to ensure that visitors (including contractors) cannot access Sensitive Information.

Electronic Distribution

Each employee and contractor performing work for Charleston Southern University will comply with the policies set forth in the Information Technology Security Policy and the GLB Security Plan, both of which are posted on the University website at http://www.csuniv.edu/adminservices/docs/.

Additional Identity Theft Prevention Program

Covered accounts
A covered account includes any account that involves or is designed to permit multiple payments or transactions. Every new and existing customer account that meets the following criteria is covered by this program:

1. Accounts for which there is a reasonably foreseeable risk of identity theft; or
2. Accounts for which there is a reasonably foreseeable risk to the safety or soundness of the University from identity theft, including financial, operational, compliance, reputation, or litigation risks.
Red flags

The following red flags are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag, is apparent, it should be investigated for verification.

1. Alerts, notifications or warnings from a consumer reporting agency;
2. A fraud or active duty alert included with a consumer report;
3. A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report; or
4. A notice of address discrepancy from a consumer reporting agency as defined in § 334.82(b) of the Fairness and Accuracy in Credit Transactions Act.
5. Red flags also include consumer reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
   - A recent and significant increase in the volume of inquiries;
   - An unusual number of recently established credit relationships;
   - A material change in the use of credit, especially with respect to recently established credit relationships; or
   - An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.
6. Suspicious documents
   - Documents provided for identification that appears to have been altered or forged.
   - The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification
   - Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification
   - Other information on the identification is not consistent with readily accessible information that is on file with Charleston Southern University
7. Suspicious personal identifying information
   - Personal identifying information provided is inconsistent when compared against external information sources used by Charleston Southern University. For example
     - The address does not match any address in the consumer report
     - The Social Security number (SSN) has not been issued or is listed on the Social Security Administration’s Death Master File; or
     - Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
   - Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by Charleston Southern University. For example, the address on a document submission is the same as the address provided on a fraudulent document.
   - Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by Charleston Southern University. For example:
     - The address on a document is fictitious, a mail drop, or a prison; or
     - The phone number is invalid or is associated with a pager or answering service.
     - The SSN provided is the same as that submitted by another student.
     - The address or telephone number provided is the same as or similar to the address or
telephone number submitted by an unusually large number of other students.

- The student fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
- Personal identifying information provided is not consistent with personal identifying information that is on file with Charleston Southern University.
- When using security questions (mother’s maiden name, pet’s name, etc.), the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

8. Unusual use of, or suspicious activity related to, the covered account

- Shortly following the notice of a change of address for a covered account, Charleston Southern University receives a request for a replacement check.
- A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer’s covered account.
- Charleston Southern University receives notice from students, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the University.

Responding to Red Flags

Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect students and Charleston Southern University from damages and loss.

1. Once potentially fraudulent activity is detected, gather all related documentation and write a description of the situation. Present this information to the designated authority in your area for determination.

2. The designated authority will complete additional authentication, using outside sources such as banks, credit card issuers, etc., where appropriate, to determine whether the attempted transaction was fraudulent or authentic.

If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:

1. Canceling the transaction;
2. Notifying and cooperating with appropriate law enforcement;
3. Determining the extent of liability of Charleston Southern University; and
4. Notifying the actual student that fraud has been attempted.

Periodic Updates To Plan

Annually, program will be re-evaluated by the Vice President for Business and the Chief Information Officer to determine whether all aspects of the program are up to date and applicable in the current business environment. Such reviews will include an assessment of which accounts are covered by the program, listing of red flags, action to take in event of fraudulent activity.
Program Administration

The Information Security Policy warrants the highest level of attention and so adoption of such a policy is the responsibility of the governing body.

Operational responsibility of the program is delegated to the senior administration for their respective areas of authority. Senior administration shall

- maintain a listing of all employees, officials and contractors for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information that may constitute a risk to Charleston Southern University or its students,
- Distribute to such persons a copy of this policy,
- Obtain from each such person a signed statement indicating that they have read, understand and agree to abide by this policy.

Oversight of service provider arrangements

It is the responsibility of Charleston Southern University to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. A service provider that maintains its own identity theft prevention program, consistent with the guidance of the red flag rules and validated by appropriate due diligence, may be considered to be meeting these requirements.

This policy will take effect immediately upon its approval by the University Board of Trustees.