Policy Title:	Data Privacy, Classification and Protection
Policy Number:	UNIV-483
Revision Date:	February 2023
Policies Superseded:	None
Policy Management Area(s):	Information Technology Services

SUMMARY:

Coastal Carolina University (University) uses a variety of data as well as information technology systems in support of its business operation and mission. These data and systems are some of the most valued University resources. The University is committed to protecting the confidentiality, integrity, and availability of its information, regardless of its media format (physical or electronic), as well as to protecting information system resources. In addition, federal and state laws require that Coastal Carolina University must limit access to certain categories of data to protect the privacy of employees, students, and other affiliated individuals and entities. (Please see Related Information and Links section.)

This policy addresses data privacy (e.g., responsible use of information, use and access of information etc.), data classification (e.g., public, internal, confidential and restricted), and data protection (e.g., security controls against damage, theft, loss, unauthorized access, etc.)

POLICY:

I. DEFINITION

University information (or data) includes any item of information that is collected, maintained and used by the University for the purpose of carrying out the business of the University in accomplishing its mission. University data may be stored either digitally or on paper in multiple formats (e.g., text, graphics, sound, etc.).

II. SCOPE

A. This policy applies to all University colleges, departments, administrative units, and affiliated organizations that use University information technology resources to create, access, store or manage University data. The policy also applies to all faculty, staff, students, affiliates, prospective students, contractors, sub-contractors

and any others who are authorized to interact with the University systems and processes.

B. This policy is not intended to replace or supersede other existing University policies and procedures relating to the use or maintenance of sensitive information such as those related to the Family Educational Rights and Privacy Act (FERPA) compliance, the Gramm-Leach-Bliley Act (GLBA) compliance, or human subjects research.

III. ROLES AND RESPONSIBILITIES

A. Responsibility for University data and technology resources is shared by the units that own them, individuals using these resources and system administrators managing the systems. Each department/unit is responsible for implementing, reviewing and monitoring internal policies, practices, etc., to assure compliance with this policy.

B. Violation of this policy may result in similar progressive disciplinary actions as violations of other University policies, including, but not limited to, termination of employment or, in cases where students are involved, reporting of a Student Code of Conduct violation.

C. Others to whom this policy applies who violate this policy are subject to appropriate sanctions, including, but not limited to, termination of the relationship and/or potential criminal prosecution under applicable federal, state and local laws.

IV. DATA PRIVACY

A. The University is committed to respecting the privacy of students, faculty, staff, business partners, and others who provide information to the University; it does so by committing to the responsible use and protection, in accordance with University policies, and federal and state laws, of sensitive information collected from and about these constituents. (Please reference the UNIV-ITS 449 Website Privacy Policy.)

B. Authorized use of sensitive information to support the University's mission; to facilitate and improve access to services, facilities, and information; to support and enhance effective and efficient processes; and to meet legal and regulatory requirements, is limited.

C. Access to sensitive information is limited to authorized individuals or entities (e.g., data owner, authorized University officials or affiliates, legally authorized entities, etc.) with legitimate access needs.

D. The University must provide a confidentiality agreement defining the responsibilities of the University's employees. Such an agreement is created collaboratively by Human Resources and Equal Opportunity, University Counsel and ITS.

E. The University must provide a confidentiality agreement defining the responsibilities of business partners (e.g., contractors, vendors) in maintaining the privacy of electronic information. Such an agreement is created by ITS in conjunction with University Counsel.

V. DATA CLASSIFICATION

A. Security Categorization

1. The University must categorize data in accordance with applicable federal and state laws, executive orders, directives, regulations and information security guidance. The University data must be classified into one of the following categories. (Please see Related Information and Links section, referencing Data Classification Schema and Guidelines as adapted from the State of South Carolina Enterprise Privacy Office.)
    a. Public: Information that is intended, or required, to be shared with the public.
    b. Internal Use: Non-sensitive information that is used in the daily operations of the University.
    c. Confidential: Sensitive information that is used or held in the daily operations of the University.
    d. Restricted: Highly sensitive information that is used or held by the University. Statutory or regulatory penalties, notification provisions, or other mandates could result if the information is accessed, used or disclosed in an unauthorized manner.

B. Labeling Information

1. Information should be labeled and handled based on its classification and security categorization.
2. If multiple data fields with different classifications have been combined, the highest classification of information included must determine the classification of the entire set.

VI. DATA PROTECTION

A. All University data and technology resources should have appropriate security controls established to address risks such as damage, loss, unauthorized access, interruption, misuse, physical and environmental threats, destruction and/or theft.

B. Data Collection and Use
1. University webpages that are used to collect data must include a link to the UNIV-ITS 449 Website Privacy Policy.
2. The collection and use of confidential and restricted information must be limited and authorized.
3. Departments/colleges that collect and/or use confidential and restricted information should report applicable systems to ITS.
4. Social Security numbers (SSNs) may NOT be used to identify members of the University. Other University-issued identifications should be used instead.
5. SSNs must not be used as a username or password.
6. Departments/colleges must not use any proprietary encryption solutions unless approved by ITS.

C. Data Storage or Processing on Server Systems
1. Servers that connect to the University network must comply with minimum security standards. Please reference the UNIV-ITS 450 General Usage - Network and Computing policy.
2. It is NOT permitted to store credit/debit card data on systems. Please reference the UNIV-ITS 480 Payment Card Industry Data Standard Security (PCI DSS) policy.
3. For confidential and restricted data protected by federal or state laws or regulations, the University must use Federal Information Processing Standards and validated technology for encrypting data.
4. Departments and units must not use any proprietary encryption solutions unless approved by ITS.

D. Data Storage or Processing on Laptops, Phones, Desktops, Tablets, etc.
1. Devices that connect to the University network must comply with minimum security standards. Please reference the UNIV-ITS 450 General Usage - Network Computing policy.
2. It is NOT permitted to store credit/debit card data on systems. Please reference the UNIV-ITS 480 Payment Card Industry Data Standard Security (PCI DSS) policy.
3. It is NOT permitted to store confidential or restricted data on personally-owned devices.
4. The University must implement encryption mechanisms on University-owned devices, where applicable, to comply with this policy.

E. Data Storage on Removable Media such as Thumb Drives, DVDs, CDs, Tapes, etc.

1. Confidential data must only be stored on removable media in encrypted formats or within an encrypted volume using encryption standards.
2. It is NOT permitted to store restricted data on removable media unless required by law. If required by law, restricted data stored on removable media must be encrypted, and the media must be stored in a physically secured environment.
3. It is NOT permitted to store restricted or confidential data on personally-owned media.

F. Granting Data Access
1. Reasonable methods must be used to ensure internal data is accessed only by authorized individuals or entities.
2. Access to confidential or restricted data must be limited to authorized University officials or representatives with legitimate requests. All access of confidential or restricted data must be approved by an appropriate responsible unit or supervisor and tracked.
3. Granting access to external third parties requires contractual agreements that outline responsibilities for data security; these agreements must be approved by University Counsel and ITS prior to granting secure data access.

G. Data Disclosure, Posting, Displaying, etc.
1. Reasonable methods must be used to ensure that internal data is only disclosed to authorized individuals or individuals with a legitimate need to know.
2. Unless required by law, the disclosure or public posting of restricted or confidential data is NOT permitted.
3. Confidential and restricted data must only be displayed to authorized and authenticated users of systems.
4. Directory information can be disclosed without consent. However, per FERPA, students can opt out of directory information disclosure. Please reference the Notification of Student Rights Under FERPA University webpage.

H. Data Transmission
1. Confidential data must be transmitted in encrypted file formats and/or over a secure protocol or connection.
2. Any confidential or restricted information transmitted to and from vendors, customers or entities doing business with the University must be encrypted and/or be transmitted through secure protocols and authenticated connections tunnels encrypted by approved technologies such as virtual private networks (VPN) or point-to-point tunnel protocols (PPTP). These types of transmissions must be governed by agreements approved by ITS and University Counsel prior to any data transmissions.

3. Wireless encryption standards and VPN encryption for remote wireless and/or internal network configurations to encrypt wireless transmissions must be used if transmitting confidential or restricted information.
4. The University must utilize encrypted file transfer programs such as Secured File Transfer Protocol (SFTP), File Transfer Pack over Secure Shell (FTP over SSH) or Secure Copy Protocol (SCP) to secure transfer of documents and data over the Internet. Only authorized users will be able to initiate secure transactions.

I. Data Emailing and Electronic Messaging
1. Reasonable methods must be used to ensure internal data is included only in messages to authorized individuals.
2. Messages that may contain confidential data must only be sent to authorized individuals as encrypted and/or over secure protocols.
3. It is NOT permitted to transmit restricted data via email or other electronic messages without express authorization or unless required by law. If authorized, data must only be included in messages within encrypted file format attachments and/or via authorized secure protocols and systems.

J. Exchanging Data with Service Providers, Cloud Services, Third Parties, etc.
1. A contractual agreement (or Memorandum of Understanding – MOU – if with an authorized governmental agency) outlining security responsibilities based on federal and state laws, standards, and policies must be in place and approved by University Counsel and ITS before exchanging any confidential or restricted data with the third party / service provider.
2. Reasonable steps must be followed to ensure that the responsibilities – of service providers, cloud services and third parties who conduct approved business with the University – for confidentiality of internal data are defined and documented.

K. Data Printing, Mailing, Faxing, Etc.
1. Printed material of internal data should only be distributed or available to authorized individuals with legitimate requests.
2. Printed material that includes restricted information or confidential data must only be distributed or available to authorized individuals or to individuals with legitimate requests.
3. Access to areas where printed records with confidential or restricted data are stored must be limited by using controls such as locks, doors, cameras, etc., to prevent unauthorized entry.
4. Social Security numbers (SSNs) must not be printed on any card required to access services.
5. New processes requiring the printing of SSNs on mailed materials must not be established unless required by authorized state or a federal agencies.

L. Data / Equipment Disposal

1. Departments should notify ITS of any electronic equipment to be moved, surplussed or redeployed. Please reference the UNIV-ITS 450 General Usage - Network Computing policy.
2. Physical media (e.g., paper, CD, tape, etc.) should be destroyed and data deleted in compliance with federal and state laws so that data on the media cannot be recovered or reconstructed.
3. The University must employ sanitization mechanisms with the strength and integrity corresponding to the security category or classification of the information.
4. The University must establish control mechanisms and processes for cleansing and disposal of computers, hard drives and fax / printer / scanner devices as stated in the UNIV-ITS 450 General Usage - Network Computing policy.
5. Media sanitization documentation must provide a record of the media sanitized, when and how the media was sanitized, the person who performed the sanitization and the final disposition of the media. The record of action taken must be maintained in a written or electronic format.
6. The University must test media sanitization equipment and procedures at least annually to ensure accurate performance.
7. The University must destroy hard copy media containing internal-use, confidential or restricted information using approved methods prior to disposal.

M. Physical Access and Security

1. Units must develop, approve and maintain a list of personnel with authorized access to the facility where confidential information, restricted data or information systems are physically located.
2. Units must establish a process to review, approve and issue credentials for personnel authorized to have facility access.
3. Units must remove or request the removal (via approved channels) of individuals from the facility access list when access is no longer required.

N. Physical Access Control

1. The University must control entry to / exit from the data center(s) and/or sensitive facilities such as network closets using physical access control devices (e.g., keycards or keys) and / or security guard(s).
2. The University must maintain physical access audit logs for data center(s) and / or sensitive facilities entry / exit points.
3. The University must employ guards and/or alarms 24 hours per day, 7 days per week, to monitor physical access points to the data center(s) where the information system resides.
4. The University must perform security assessments on an annual basis of the physical boundary(ies) of the data center(s) to check for unauthorized exfiltration of information or removal of information system components.

5. The University must establish a process to escort visitors and to monitor their activity within the data center(s) and/or sensitive facilities.
6. The University must change combinations and keys at defined intervals, as well as when keys are lost, combinations are compromised, or individuals are transferred or terminated.
7. The University must control physical access to information system distribution and transmission lines within the data center(s) using physical access control devices (e.g., keycards or keys).
8. The University must control physical access to information system output devices (e.g., printers, copiers, scanners, facsimile machines) to prevent unauthorized individuals from obtaining sensitive data.
9. The University must review physical access logs at a defined frequency and upon occurrence of security incidents.
10. The University must maintain visitor access records to the data center(s) and / or sensitive facilities for a minimum of one year.

VII. ENVIRONMENTAL SECURITY

A. Power Equipment and Cabling

The University must place power equipment and cabling in safe locations prevent environmental and / or man-made damage and destruction.

B. Emergency Shutoff

1. The University must provide the capability of shutting off power to data center(s) during an incident.
2. The University must place emergency shut-off switches or devices at locations which can be safely and easily accessed by personnel during an incident.
3. The University must implement physical and logical controls to protect emergency power shut-off capability from unauthorized activation.

C. Data Center Emergency Power

The University must implement an uninterruptible power supply to facilitate transition to long-term alternate power in the event of a primary power source loss.

D. Data Center Fire Protection

1. The University must install and maintain fire detection and suppression devices that are supported by an independent power source.
2. The University must employ fire detection devices / systems that activate automatically and notify emergency personnel and defined emergency responder(s) in the event of a fire.
3. The University must employ an automatic fire suppression system if / when the data center(s) is not staffed on a continuous basis.

E. Data Center Temperature and Humidity Controls

1. The University must employ automatic temperature and humidity controls in the data center(s) to prevent fluctuations that could be potentially harmful to processing equipment.
2. The University must employ temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

F. Data Center Water Damage Protection

The University must protect processing equipment from damage resulting from water leakage.

Related information and policy links include, but are not limited to:

The Family Educational Rights and Privacy Act (FERPA) – protects a wide range of personal education records and information about current and former students including, but not limited to, grades, university judicial records, and academic records.

The Health Insurance Portability and Accountability Act (HIPAA) – governs the use of protected health information, including information that identifies an individual and relates to the individual's past, present, or future physical or mental health; the provision of health care to the individual; or the past, present or future payment for health care.

The Gramm-Leach-Bliley Act (GLBA) – protects personal financial information.

UNIV-449 Website Privacy Policy
UNIV-480 Payment Card Industry Data Standard Security (PCI DSS) policy
UNIV- 450 General Usage - Network Computing policy
Notification of Student Rights Under FERPA
Data Classification Schema and Guidelines