UNIVERSITY OF CENTRAL FLORIDA

Office of the President

SUBJECT: Data Classification and Protection	**Effective Date:** 6/3/2021	**Policy Number:** 4-008.2
	Supersedes: 4-008.1	**Page Of** 1 11
	Responsible Authority: Associate VP & Chief Information Security Officer Director, Privacy Compliance	

DATE OF INITIAL ADOPTION AND EFFECTIVE DATE 11/5/07

APPLICABILITY/ACCOUNTABILITY

This policy applies to all members of the university community.

POLICY STATEMENT

All members of the university community have a responsibility to protect the data generated, accessed, modified, transmitted, stored, or used by the university. This requirement is irrespective of the medium on which the data resides or the means by which the data may be transmitted. Data is a critical asset of the university and it is the policy of the University of Central Florida to classify types of data in use at the university and to provide the appropriate levels of information security and protection. Members of the university community are responsible for implementing appropriate managerial, operational, physical, and technical controls for access, use, transmission, storage, and disposal of university, state, or federal data in compliance with this policy, as requested by the Information Security Office, University Compliance, Ethics, and Risk, and any applicable laws, regulations or policies.

It is the policy of the university to require all members of the university community to immediately report confirmed or suspected data security incidents to the Security Incident Response Team (SIRT). Data considered to be Highly Restricted Data or Restricted Data may require a heightened response and reporting obligations.

In the event of a suspected information security incident, users should take no action to delete any data or attempt to investigate.

Any violation of this policy and procedures may result in immediate loss of network and computer access privileges, seizure of equipment, loss of research laboratory access, or removal of inappropriate information posted on university-owned computers or university-supported internet sites. In addition to these corrective actions, failure to comply with this policy and procedures may result in disciplinary action up to and including termination or expulsion.

DEFINITIONS

Controlled Unclassified Information (CUI). A type of federal data consisting of unclassified information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

Credentials. A combination of username, password, and possibly additional information or keys such as a personal identification number (PIN), biometric scan, or other unique identifier that together are used to access a computer system or information resource.

Cross-cut Shredder. Cuts paper both lengthwise and crosswise, leaving papers in a rectangular shape.

Data. Alphanumerical or other information represented either in a physical form or digital form suitable for electronic processing or storage.

Diamond-cut Shredder. Cuts paper similar to a cross-cut shredder yet leaves papers in a diamond shape.

Encryption. The encoding of data into a form that cannot be easily decoded by unauthorized parties.

Federal Data. Data that is collected, stored, processed, transmitted, or used on behalf of a federal agency. This applies to all forms of data (electronic, paper, audio, Controlled Unclassified Information [CUI], etc.). Data accessed from a federal database, even if managed by a third party, constitutes the use of federal data. The data will need to be protected at the appropriate level of NIST SP 800-53.

Federal Information System. An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

Highly Restricted Data. Any data that is strictly controlled, and protected by laws, regulations, contracts, or policies. Highly Restricted Data requires the highest level of access control and security protection, both in storage and in transit. The loss of confidentiality, integrity, or availability of Highly Restricted Data could have a significant adverse impact on the university's mission, safety, finances, or reputation. (For an extended definition, characteristics, and examples, see *Data Classification* section below.)

Institutional Data. All data created, collected, maintained, recorded, or managed by the university, its staff and agents working on its behalf, in the course of conducting university business. This includes information that is processed or resides on privately owned devices that are used for university purposes.

Internet Cloud Storage. Data stored in third-party data centers (e.g., CrashPlan, Dropbox, iCloud, Google Drive, OneDrive, Box, etc.).

Mobile Computing Device. Cellular telephones, smartphones, laptop computers, tablets, personal computers, and similar mobile electronic devices that are capable of storing, processing, displaying, and communicating data.

Network identification (NID). A UCF-issued credential or identifier, classified as Restricted Data, that is to be used by university employees and students to access enterprise computing systems and applications.

Restricted Data. Institutional Data not identified as Highly Restricted Data, and data that may be protected by state or federal regulations, such as the Family Educational Rights and Privacy Act (FERPA.) Restricted Data must be protected to ensure that they are not disclosed in public records requests and are only disclosed as required by law and to authorized individuals only. (For an extended definition, characteristics, and examples, see *Data Classification* section below.)

Transport Layer Security (TLS). Internet protocol that ensures privacy between communication applications and their users on the internet.

UCF Employee Identification Number (UCFID). A unique seven-digit numerical identifier, classified as Unrestricted Data, that uniquely identifies each university employee and student in the university's administrative systems.

University Community. All university personnel, students, volunteers, employees, and volunteers of Direct Support Organizations (DSOs), as well as visitors and contractors who conduct business with the university.

Unrestricted Data. Data that is not protected by law or contract, and the disclosure of which is not reasonably expected to cause harm to the university or to the affected parties. (For an extended definition, characteristics, and examples, see *Data Classification* section below.)

DATA CLASSIFICATION

University, state, and federal data falls into three data classifications: Highly Restricted Data, Restricted Data, and Unrestricted Data:

A. Highly Restricted Data

Highly Restricted Data is any data that is strictly controlled, and protected by laws, regulations, contracts, or policies. Highly Restricted Data requires the highest level of access control and security protection, both in storage and in transit. The loss of confidentiality, integrity, or availability of Highly Restricted Data could have a significant adverse impact on the university's mission, safety, finances, or reputation.

Protection of such data may also be subject to additional operating regulations in accordance with vendor or partner agreements, such as the Payment Card Industry (PCI), Data Security Standards (DSS), or Federal contracts.

Unauthorized access to, or disclosure of, highly restricted data will generally require notification to affected parties under the guidelines of state and federal breach notification laws. In addition, unauthorized access, use, disclosure, or loss of Highly Restricted Data may have significant legal consequences, including civil and criminal penalties, loss of funding, inability to continue current research, and inability to obtain future funding or partnerships.

Examples of **Highly Restricted Data**:

1. **Government Identification Numbers.** An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:
    a) social security number (SSN),
    b) driver's license or identification card number,
    c) passport number,
    d) military identification number, or
    e) any other similar number issued on a government document used to verify identity

2. **Financial Account Numbers.** An individual's first name or first initial and last name in combination with financial account numbers.
    a) UCF ID Card ISO numbers fall under this classification when the cardholder has enrolled in Knights Cash or has a Fairwinds bank account using their UCF ID Card

3. **Credentials**. Username (e.g., NID) or email address, in combination with any of the following that would permit access to an online account:
    a) a password,
    b) a security question and answer, or
    c) a one-time code that would verify an identity and permit a password reset or access to an account, such as a password reset code or a Multi-Factor Authentication (MFA) token

4. **Health Information**
    a) **Health Insurance Portability and Accountability Act of 1996 (HIPAA) Protected Health Information (PHI).** Data concerning an individual that is considered "protected health information" (also known as electronic Protected Health information or ePHI when in electronic form) within the meaning of the HIPAA (as amended by the Health Information Technology for Economic and Clinical Health Act), and its implementing regulations.
    b) An individual's first name or first initial and last name in combination with:
        1) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
        2) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

5. **PCI Data.** Includes information in two main categories:
    a) Cardholder data consists of the full Primary Account Number (PAN, commonly known as the Credit Card Number), either on its own or combined with cardholder name, expiration date, and/or service code.
    b) Sensitive Authentication Data is Security-related information (including, but not limited to, card validation codes/values, full track data (from the magnetic stripe or equivalent on a

chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions. PCI Sensitive Authentication Data must never be stored.

6. **Federally Protected Data.** Data protected by applicable federal laws, regulations, or contracts, including but not limited to:
   a) Federal Information System Modernization Act (FISMA) of 2014 Defense Federal Acquisition Regulation Supplement (DFARS), (including CUI as described in DFARS 252.204-7012)
   b) International Traffic In Arms Regulation (ITAR)
   c) Export Administration Regulations (EAR)

7. **Protected University Employee Data.** The home addresses, telephone numbers, social security numbers, and photographs of certain protected or sensitive university employees and their spouses and children as specified in F.S. 119.071 (4). Relevant examples in F.S. 119.071 (4) include
   a) current or former police officers, or
   b) current or former internal audit personnel whose duties include activities that could lead to criminal prosecution or administrative discipline

8. **Gramm-Leach Bliley Act "Nonpublic Personal Information" (NPI).** Consumers' personal financial information held by the university and data concerning an individual that is considered NPI within the meaning of Title V of the Gramm-Leach Bliley Act (Public Law 106-102, 11 Statute 1338 as amended) and its implementing regulations.

B. Restricted Data

Restricted Data includes Institutional Data not identified as Highly Restricted Data, and data that may be protected by state or federal regulations, such as FERPA. Restricted Data must be protected to ensure that they are not disclosed in public records requests and are only disclosed as required by law and to authorized individuals only.

Unauthorized access to or disclosure of certain types of restricted data will generally not require notification of affected parties; however, breach or disclosure of certain restricted data covered by law or regulation may require notification of an appropriate governmental agency. Unauthorized access to or disclosure of restricted data that is the subject of contractual protections will generally require notification to the contracting party.

Examples of **Restricted Data**:

1. **Business sensitive data**

2. **Proprietary intellectual property data**, such as an algorithm or schematic developed on campus that belongs to the university

3. Certain student education records as defined under FERPA:
   a) **Personally Identifiable Information (PII)**
      i. Student ID - UCFID (EmplID in PeopleSoft)
      ii. UCF ID Card ISO Number
      iii. Residency Status
      iv. Gender
      v. Religious Preference

   vi. Race/Ethnicity

b) **Education Records**
   i. Grades/GPA
   ii. Student's Class Schedule
   iii. Test Scores
   iv. Academic Standing
   v. Academic Transcripts

c) **Other FERPA information UCF considers Restricted Data in terms of data protection**
   i. Student Email Address
   ii. Student ID Photos

d) **Directory information.** The following directory information is considered **restricted data when the student has exercised their right to withhold the release of their directory information via myUCF (sometimes called FERPA Opt-Out)**:
   i. Name
   ii. Current mailing address
   iii. Telephone number
   iv. Date of birth
   v. Major
   vi. Dates of attendance
   vii. Enrollment status (full-/part-time)
   viii. Degrees/awards received
   ix. Participation in officially recognized activities and sports
   x. Athletes' height/weight

4. **Network and Systems data**. Sensitive technical information related to UCF systems that is business sensitive. Examples include:
   a) NID (Network Identification): the UCF-issued NID credential, by itself, is considered restricted data
   b) IP addresses, system names, system inventories, configuration information, network diagrams, and vulnerability data

5. Other data protected by law or regulation.

C. <u>Unrestricted Data</u>

Unrestricted Data is data that is not protected by law or contract, and the disclosure of which is not reasonably expected to cause harm to the university or to the affected parties.

Examples of **Unrestricted Data**:

1. Employee names, dates of hire, rate of pay, title, office address, UCFID or phone number.

2. **Directory Information.** The following directory information, as defined under FERPA, is considered unrestricted data, provided the student has not exercised their right to withhold the release of the information via myUCF: student name, current mailing address, telephone number, date of birth, major or field(s) of study, dates of attendance, enrollment status (full-/part-time), degrees and awards received, participation in officially recognized activities and sports, and athletes' height and weight.

3. Certain types of **institutional data** not otherwise restricted by university, state, federal, or contract-related requirements.

LOGICAL DATA PROTECTION

The following establishes minimum standards for the storage, transfer, and access of university, state, or federal data. More specific requirements may exist in certain contracts, such as research agreements with the federal government. To the extent specific requirements are set forth in a contract, or otherwise required by the government, those specific obligations for storage, transfer, and access of restricted data must be followed.

A. Highly Restricted Data

There are several data types contained within the category of Highly Restricted Data as explained above in the Data Classification section. Certain types of Highly Restricted Data must comply with additional policies, standards, and authorizations specific to the data in question. Many types of data mandate their separation from other data sets. Additionally, authorization that a system may store, or process one type of Highly Restricted Data does not imply authorization for all types of Highly Restricted Data. Highly Restricted Data may only be stored on systems intended, configured for, allowed by relevant policies, and authorized for the given type of data. As required, members of the university community must complete training prior to accessing Highly Restricted Data.

The below establishes the appropriate measures for handling Highly Restricted Data and are intended as a baseline requirement that may be superseded by more elevated data-specific security requirements put in place by the university.

Highly Restricted Data:

1. May be stored on UCF servers only when the servers:
   a) are intended for highly restricted data, and at a minimum meet relevant University Security Standards;
   b) employ full-disk encryption (additional file level encryption is required anytime data is exported, saved, or downloaded or copied from these systems); and
   c) are protected by Multi-Factor Authentication.

2. May only be stored in UCF sanctioned internet cloud data storage systems (e.g. OneDrive) when the cloud systems are intended for highly restricted data and meet relevant University Security Standards.

3. Must not be stored in personally owned cloud data storage accounts (see UCF Policy 4-014 for more information).

4. Must be protected by Multi-Factor Authentication when stored on a server, cloud system, or within an application.

5. May only be stored on desktop or laptops if all of the following are true:
   a) There is a legitimate university business reason that the data must be stored on a desktop/laptop, as opposed to within a secured university server or application.
   b) The desktop/laptop is a university-owned and managed device.
   c) The desktop/laptop meets relevant University Security Standards.
   d) The desktop/laptop employs full disk encryption using current industry standards, such as BitLocker or FileVault.
   e) The data must have file-level encryption with access protected by a strong password (in addition to the full disk encryption).

f) Depending on the types of data present, such as CUI, the desktop/laptop will be required to have strong physical security and may additionally require protection by Multi-Factor Authentication.

6. Must never be stored on miscellaneous mobile devices, such as tablets, smartphones, or USB drives, unless there is a legitimate university business reason that the data must be stored on one of these devices, as opposed to within a secured university server or application. Disk-level encryption is required on these devices. Highly Restricted Data on these devices must also be protected with file-level encryption, with access protected by a strong password.

7. Must not be posted on any public website, blog, or other publicly accessible Internet site.

8. Must not be sent via electronic mail, or in an email attachment unless encrypted using current industry cryptographic standards.

9. Must not be sent via instant messaging or other unencrypted applications.

10. Must always be protected by using a secure connection method, such as a VPN and/or a current version of TLS encryption when transmitted through a data network.

11. Must not be disclosed to third parties without explicit management authorization and then only on a need-to-know basis.

12. Must be sent only to a known number when sent via fax.

13. Must be destroyed when no longer needed, subject to the State of Florida General Records Schedule and UCF Policy 2-003 and UCF Policy 4-010.

B. Restricted Data

1. Can be stored on university-owned and managed workstations or mobile computing devices if the devices are protected by a strong password and full disk encryption. File-level encryption is recommended.

2. May be placed only in a UCF-sanctioned internet cloud data storage system (e.g., OneDrive), but not in a personally owned cloud data storage system.

3. May be sent to authorized users who are within a university-provided email system (e.g., UCF Exchange, Knights email, Webcourses@UCF).

4. May be sent to authorized recipients who use external email systems if encrypted using Office 365 Email encryption.

5. Instant messaging of restricted data between faculty, staff, and students must be through a university-provided instant messaging system, (e.g., Microsoft Teams or Skype for Business). Instant messaging may not be used to send restricted data to external systems, using external systems, or using third party systems.

6. Must not be posted on any public website, blog, or other publicly accessible internet site.

7. Must be sent only to a known number when transmitting via fax.

8. Must be destroyed when no longer needed, subject to the State of Florida General Records Schedule and UCF Policy 2-003 and UCF Policy 4-010.

PHYSICAL DATA PROTECTION

To reduce the physical risks to Highly Restricted or Restricted Data, all members of the university community must maintain a "Clean Desk Area." An important aspect of a clean desk policy is the requirement to keep your environment secure when you are away from your desk or office. All forms of media, such as papers, CDs, DVDs, hard drives, USB drives, flash drives, computer screen displays, etc., containing Highly Restricted or Restricted Data are within the scope of this policy. In addition, these measures reinforce the need to protect usernames, passwords, or other data elements that would allow one to access a secure location or an information system. Please adhere to the following measures to physically secure assets where Highly Restricted or Restricted Data may reside:

1. Physically secure electronic media, electronic devices, and information systems.

2. Log off or screen lock computer workstation(s), laptops, tablets, etc., to safeguard the data accessible on those devices(s).

3. Secure Restricted Data when it is not being worked on or processed, when leaving your work area (e.g., for lunch or restroom breaks, end of the day, etc.)

4. Lock desks and cabinet drawers if they contain any Restricted Data.

5. Do not write down (or share) passwords or passphrases and leave them openly accessible at or around your desk area. Users are strongly encouraged to use a commercially available password manager application to enhance password strength and secure all passwords.

6. Check printer trays where Restricted Data may be printed.

7. Check copier trays (make sure documents are not left under the cover).

8. Check in and out trays, either personal trays on desks or departmental pending work trays.

9. Check departmental mailboxes where Restricted Data may be delivered.

10. Thoroughly erase whiteboards where Restricted Data may be present.

11. Use crosscut or diamond-cut shredders to shred printed Restricted Data. Paper recycle and trash bins must never contain legible confidential materials.

12. Check and secure other areas where paper or electronic media containing Restricted Data may be placed.

If you believe Highly Restricted or Restricted Data has been compromised, please notify your supervisor immediately and contact the UCF Security Incident Response Team at SIRT@ucf.edu.

Requests for Data
Court orders, subpoenas, or requests from federal or state agencies for access to university, state, or federal data should be referred to the Office of the General Counsel. All public records requests for university, state, or federal data should be processed according to UCF Policy 2-100 *Florida Public Records Act – Scope and Compliance*.

RELATED DOCUMENTS

UCF Policy 2-003 Records Management
UCF Policy 2-100 Florida Public Records Act—Scope and Compliance
UCF Policy 2-103 Use of Copyrighted Material
UCF Policy 3-206 Credit Card Merchant Policy
UCF Policy 4-002 Use of Information Technologies & Resources
UCF Policy 4-007 Security of Mobile Computing, Data Storage, and Communication Devices
UCF Policy 4-014 - Procurement and Use of Cloud Computing and Data Storage Services
UCF Policy 4-209 - Export Control Policy

UCF Regulation 3.045 Sensitive Information Disclosure

State of Florida General Records Retention Schedule
https://dos.myflorida.com/library-archives/records-management/general-records-schedules/
UCF Security Standards
https://infosec.ucf.edu/standards/

UCF Information Security Awareness Resources
https://infosec.ucf.edu/awareness/

Florida Statute 501.171
http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0500-0599/0501/Sections/0501.171.html

Family Educational Rights & Privacy Act
https://studentprivacy.ed.gov/node/548/

Gramm-Leach-Bliley Act
https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf

Health Insurance Portability and Accountability Act of 1996
https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf

CONTACTS

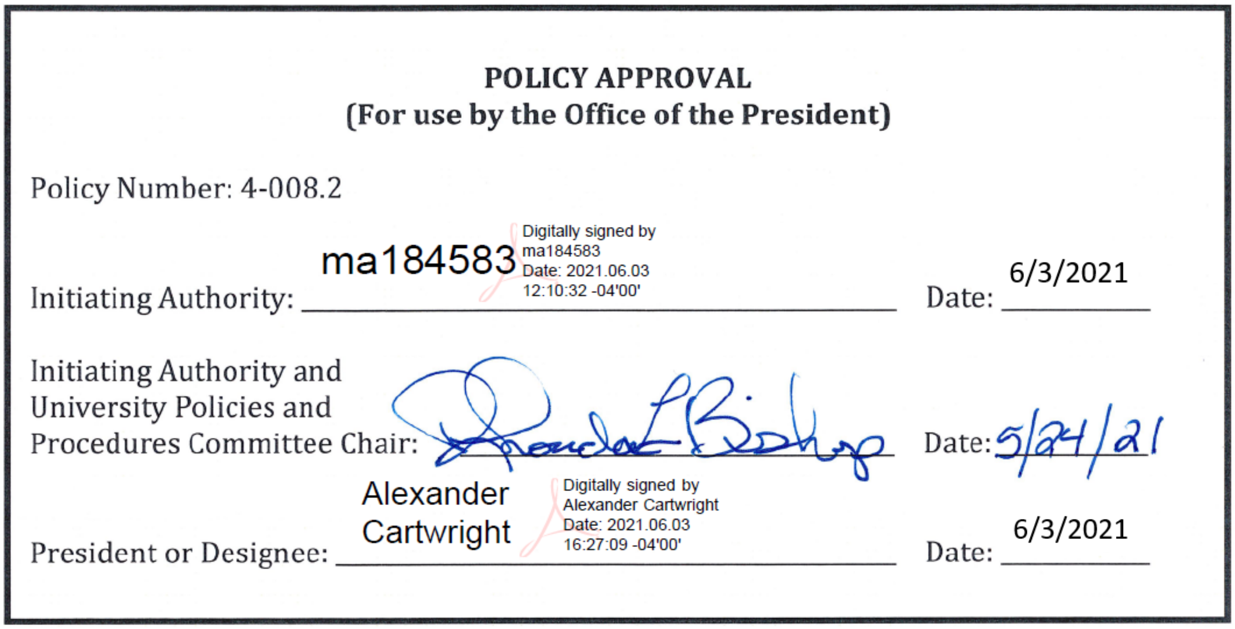
Information Security Office, Chief Information Security Officer, infosec@ucf.edu, 407-823-3863

Information Security Office Security Incident Response Team (SIRT), sirt@ucf.edu

UCF IT Support Center, itsupport@ucf.edu, 407-823-5117

INITIATING AUTHORITIES

Vice President for Information Technology and CIO;
Vice President for Compliance and Risk



POLICY APPROVAL
(For use by the Office of the President)

Policy Number: 4-008.2

Initiating Authority: ma184583 Digitally signed by ma184583 Date: 2021.06.03 12:10:32 -04'00' Date: 6/3/2021

Initiating Authority and University Policies and Procedures Committee Chair: Bishop Date: 5/24/21

President or Designee: Alexander Cartwright Digitally signed by Alexander Cartwright Date: 2021.06.03 16:27:09 -04'00' Date: 6/3/2021

History: 4-008 11/5/07, 4-008.1 8-27-2015