	FGCU POLICY 3.042	Responsible Unit:
	Restricted Data	Information Technology Services

A. POLICY STATEMENT

The purpose of this Policy is to provide direction to University employees and other applicable personnel when handling Restricted Data. The loss or unauthorized disclosure of Restricted Data, such as social security numbers or credit card numbers, would impair the functions of the University, and potentially cause significant financial or reputational loss to the University and those persons whose personal data was lost or disclosed.

B. REASON FOR POLICY

This Policy provides guidance on the handling of, obtaining, and approving access to Restricted Data.

C. APPLICABILITY AND/OR ACCOUNTABILITY

This Policy applies to all University units and members of the University community accessing Restricted Data, as well as University contractors when acting as Data Users.

D. DEFINITION OF TERMS

1. *Cross Departmental Folder*: A folder on the University network located on the R: drive, which can be accessed simultaneously by multiple users that work in different departments within the University. (Folders located on the S: drive (Scratch Drive) are not considered Cross Departmental Folders.)

2. *Data Steward:* A University employee responsible for maintaining the functionality of a system and for ensuring that data within the system stays accurate and up to date. The Data Steward is responsible for determining computing needs and applicable systems and software in their respective functional area of responsibility. All Data Stewards must adhere to the standards, policies, and procedures set by the University Data & Information Strategy Council for use of Restricted Data.

3. *Data User*: Any University unit, employee, or contractor who has been provided specific privileges to view, copy, edit, store, update, or transfer Restricted Data that originates from a University system.

4. *Departmental Share Folder*: A folder on the University network located on the P: drive that can be accessed simultaneously by multiple users that work in the same department.

5. *Encryption*: The process by which a message or a file is encoded in such a way as to prevent unauthorized users from reading the data in the message or file. A key or password is required to decrypt a file to make it readable by the recipient. Instructions for encrypting data or devices can be found on the Information Technology Services (ITS) webpage.

6. *Mobile Computing Devices*: An electronic device, which is easily transportable, is intended primarily for access to, or processing of, data, and provides persistent media storage. New products with these characteristics appear frequently. Current examples include, but are not limited to, the following:

    a) Portable computers (laptops, notebooks, netbook, or any comparable hybrid);

    b) Smartphones; and

    c) Tablets.

7. *Mobile Storage Devices*: An electronic device, which is easily transportable and which provides persistent media storage. New products with these characteristics appear frequently. Current examples include, but are not limited to, the following:

    a) Memory storage devices such as USB-sticks, thumb drives, flash drives, jump drives, and memory cards (SD, CompactFlash, and Memory Stick);

    b) Portable devices that make non-volatile storage available for user data like digital cameras, MP3 and other digital music players, digital audio recorders, smart watches, cell phones, and tablets;

    c) Magnetic storage devices (diskettes, tapes, USB hard drives); and

    d) Optical storage devices (CDs, DVDs).

8. *Restricted Data*: Any data which may be considered confidential or personal that is protected by law or policy, and that requires the highest level of access control and security protections whether in storage or in transit.

9. *Secure Sockets Layer (SSL)*: Cryptographic protocols designed to provide communications security over a computer network.

10. *Secure Transfer Protocol*: A method of transferring data from one computer to another by a method that is secure, such as Secure File Transfer Protocol (SFTP) or Secure Copy Protocol (SCP).

11. *Virtual Private Network (VPN)*: Software which extends a private network across a public network and enables users to send and receive data across shared or public

networks as if their computing devices were directly connected to the private network.

E. PROCEDURES

1. Restricted Data

   a. A list of Restricted Data types is posted on the ITS website or may be found through a search for "Restricted Data" on the University website. Please note that this list is not all-inclusive and if there is uncertainty whether data is restricted, please contact the ITS Help Desk at 239-590-1188.

   b. Data Not Expressly Defined or Categorized

      If data is in use that is not expressly identified as Restricted Data as discussed in this document, treat the data as restricted until a determination of the data's security status can be made by ITS. Additionally, Records Management should be contacted for the proper data storage, security, retention, and destruction methods.

      Regardless of the category of data, always consider the privacy implications and impact of the data you are working with and err on the side of caution.

   c. Contact the ITS Help Desk at 239-590-1188 before any media, service, or device to store Restricted Data are used.

2. Use of Restricted Data

   Restricted Data must be used consistent with the following:

   a. Restricted Data that is in electronic or digital format may be stored on a University Departmental Share Folder or Cross Departmental Folder in an unencrypted state. Physical copies of Restricted Data must be stored in a secure environment with limited access.

   b. Restricted Data must be encrypted on Mobile Computing or Mobile Storage Devices. Instructions on Encryption can be found on the ITS website.

   c. Once the Restricted Data is no longer needed, it must be disposed of in accordance with FGCU Policy 3.032, Records Management.

   d. No Restricted Data may be taken out of the country on any Mobile Computing Device or Mobile Storage Device. Please contact the Office of Research and Graduate Studies about the federal export control regulations and their application to Restricted Data.

3. Access to Restricted Data

Access to Restricted Data is approved by the responsible Data Steward. The Data Steward shall grant access in compliance with all relevant regulations (e.g. FERPA, HIPAA, and GLBA). Data Stewards shall grant access only to those Data Users that need the access to perform their job duties. A complete listing of Data Stewards and authorized designees is maintained on the ITS website. In the case that a Data Steward is not designated, the Dean or Director of the University unit that originates the data will be responsible for authorizing access to the Restricted Data.

4. Procedures for Requesting, Approving, and Revoking Access

   Data Stewards shall establish procedures for:

   a. Requesting and approving access to Restricted Data;

   b. Regular auditing access to Restricted Data;

   c. Revoking access to Restricted Data when it is no longer needed or authorized;

   d. Ensuring that the location of all reports, printouts, and files containing Restricted Data is included in the Unit's Restricted Data inventory; and

   e. Tracking of requests, approvals, and revocations of access to Restricted Data in case of audit. Please contact ITS for assistance in developing tracking procedures.

5. Transmission of Restricted Data

   There are restrictions on transmitting Restricted Data inside and outside the University network.

   a. Restricted Data shall not be shared with unauthorized individuals or entities.

   b. Restricted Data sent over the Internet must be encrypted and a Secure Transfer Protocol must be used. Please contact the ITS Help Desk to obtain instructions for these procedures.

   c. Do not email Restricted Data in unencrypted format. Email only when Restricted Data is encrypted. Please contact ITS for information on how to encrypt Restricted Data for delivery by email.

   d. Restricted Data must be shared with other authorized Data Users by using the Departmental Share Folder or the Cross Departmental Folders.

   e. Faxing Restricted Data

1) Restricted Data may not be faxed. Notwithstanding, Student Health Services and Counseling and Psychological Services may fax Restricted Data as permitted by law and in accordance with HIPAA regulations.

2) Restricted Data may be received via fax from an individual or entity through the University fax server. Restricted Data may be received by fax provided the recipient is standing by the fax machine waiting for the fax or the fax machine is located in an area that has limited access.

f. Only Secure Transfer Protocols may be used to transmit Restricted Data.

6. Printing or Copying Restricted Data

a. If Restricted Data is printed, the Restricted Data must be immediately retrieved from the printer.

b. Do not use an outside copy service to copy Restricted Data.

c. The Data User is responsible for all copies of the Restricted Data and must ensure the copies are secured or destroyed when no longer useful.

7. Storing Restricted Data

a. Physical Storage of Restricted Data

1) If Restricted Data needs to be printed and retained, it must be stored in a secure environment with limited access, such as a locked file cabinet.

2) "Keep a clean desk." All Restricted Data should be removed from a Data User's work space and stored in an appropriate location after use.

b. Prohibited Physical Storage Methods

Certain devices and services are not permitted to store, transport, or backup Restricted Data because of security or control over Restricted Data. The following services, Mobile Storage Devices, and Mobile Computing Devices may not be used to store, transport, or backup Restricted Data:

1) Cloud-based file storage services such as Microsoft OneDrive, Dropbox, Google Drive/Docs, etc.;

2) Unencrypted static memory storage devices such as USB-sticks, thumb drives, flash drives, jump drives and memory cards (SD, CompactFlash and Memory Stick);

3) Personal or University Email;

4) Personal or University smart phones; or

5) CD's, DVD's, or other optical storage methods.

c. Authorized Physical Storage Methods

The following devices are authorized to store, transport, or backup Restricted Data if the Restricted Data is encrypted on the device:

1) Encrypted personal or University desktop computers;

2) Encrypted personal or University laptops;

3) Encrypted personal or University tablets or smart phones; or

4) Encrypted USB-sticks.

8. Loss of Restricted Data

If you have Restricted Data in a printed or electronic format and it is lost or stolen, you must immediately report the missing data to the ITS Help Desk at 239-590-1188. The ITS Help Desk will initiate the process to address the loss of the Restricted Data.

9. Disposal

a. Disposal of Restricted Data must be done in accordance with FGCU Policy 3.032, Records Management.

b. Electronic copies stored on mobile devices must be deleted. Please contact ITS for instruction on how to clean a mobile device of Restricted Data.

c. Disposal of Devices Used to Store Restricted Data

1) Disposal of computing and storage devices must comply with surplus equipment disposal requirements. The device memory must be properly cleaned of all University data or destroyed to prevent any Restricted Data or any other data or records of the University from remaining on the device memory.

2) All University-owned devices capable of storing data must be returned to the ITS Help Desk for proper cleaning and disposal if the devices are no longer being used or an employee is separating from the University.

d. Mobile Storage Devices

All Mobile Storage Devices with Restricted Data must be disposed of through Records Management to insure proper data destruction.

e. Physical Copies

Physical copies of Restricted Data must be shredded in a crosscut shredder to ensure complete destruction. Printed Restricted Data must be destroyed consistent with procedures described within this Policy and in accordance with FGCU Policy 3.032, Records Management, when the data in this format is no longer needed.

f. Electronic copies stored on shared drives may be deleted when no longer needed as long as retention policies are being followed.

10. Accessing Restricted Data Remotely

a. Restricted Data may be accessed while at home, or in another remote location, using the University Virtual Private Network system. Certain Restricted Data may be accessed without using the VPN if the system is maintained or contracted by FGCU (such as Gulfline or the University's learning management system), where the system requires a Secure Sockets Layer connection and user authentication to gain access to the Restricted Data.

b. Any Restricted Data downloaded to a computing device must be encrypted immediately after downloading. Instructions for encrypting data or devices can be found on the ITS website.

c. It is the responsibility of the Data User to ensure that the data is deleted from the computer or tablet when the data is no longer needed and in accordance with FGCU Policy 3.032, Records Management.

11. Inventory of Restricted Data

Once a year, each department will perform an inventory of Restricted Data in accordance with the procedure 'Restricted Data Inventory Process' and submit this inventory to ITS.

12. Adherence to University Technology Resource Security Procedures

Users shall comply with all University Technology Resource security procedures. Users shall also comply with all requirements for notifying ITS of breaches or violations of University Technology Resource security procedures.

13. Acquiring Services to Store Data

All software or online software services that access Restricted Data must be officially licensed software. All software or online software services that access Restricted Data

must be reviewed by ITS for data and network security prior to use. No User may install any software or online software services that access any Restricted Data on the University's computer or network, by any means of transmission, unless authorized. All vendor contracts and license agreements for software or online software services must be submitted to Procurement for review and execution prior to use.

Related Information

Chapter 119, Florida Statute
1B-26.003 Florida Administrative Code Rule 1B-26.003
Board of Governors Regulation 3.0075, Security of Data and Related Information Technology Resources
FGCU Policy 3.006, Education Records
FGCU Policy 3.017, Departmental Employee Files
FGCU Policy 3.019, Identity Theft Prevention Program
FGCU Policy 3.022, Technology Acceptable Use
FGCU Policy 3.024, Notification of Social Security Number Collection and Usage
FGCU Policy 3.032, Records Management Policy

Authority

34 CFR PART 99 (FERPA)

History of Policy

New 01/09/15; Amended 02/28/22

APPROVED

*s/Michael V. Martin	February 28, 2022
Michael V. Martin, President	Date