DRAFT DATE 10/15/13 Please use TRACK Changes in this document	**Florida Gulf Coast University** Policy Manual	Policy: **Number to be assigned in the General Counsel's Office**
	Title: Restricted Data Policy _____	**Responsible Executive**: Vice President for Administrative Services and Finance_____ **Responsible Office**: Business Technology Services_____

POLICY STATEMENT

Establish standards for the use, storage, access, printing, and transmission of restricted data.

REASON FOR POLICY

The purpose of this policy is to notify and educate employees that they are responsible for the restricted data they come in contact with while working at FGCU. This policy will help guide employees on how to handle restricted data.

APPLICABILITY AND/OR ACCOUNTABILITY

This policy applies to all employees of FGCU and all service providers under contract with FGCU, as well as all FGCU volunteers.

DEFINITION OF TERMS

Mobile Computing Devices
Electronic devices intended primarily for access to or processing of data, which can be easily carried by a person and which provides persistent storage. New products with these characteristics appear frequently. Current examples include, but are not limited to, the following:

- laptops
- netbooks
- notebooks
- smartphones
- tablets

Mobile Storage Devices
Media that can be easily carried by a person and which provides persistent storage. New products with these characteristics appear frequently. Current examples include, but are not limited to, the following:

- magnetic storage devices (diskettes, tapes, USB hard drives)
- optical storage devices (CDs, DVDs)
- memory storage devices (SD cards, thumb drives, flash drives, etc.)
- portable devices that make nonvolatile storage available for user files (cameras, MP3 and other music players, audio recorders, smart watches, cell phones, tablets)

Restricted Data
Data in any format: Collected, developed, maintained or managed by or on behalf of the University, or within the scope of University activities that are subject to specific protections under federal or state law or regulations or under applicable contracts, and whose loss or unauthorized disclosure would impair the functions of the University, cause significant financial or reputational loss, or lead to potential legal liability. A list of restricted data types will be posted on the Business Technology Services website.

Secure FTP
Secure FTP or Secure File Transfer Protocol is a method of transferring files from one computer system to another in a secure method.

Encryption
Encryption is the process of encoding a message or a file 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.

Florida Gulf Coast University
The colleges, institutes, centers and administrative units that make up the University, along with support organizations whose sole purpose is to provide services to or on behalf of the University.

Florida Gulf Coast University Constituency
The university constituency is made up of the faculty, staff, students, contractors, volunteers, and other persons whose conduct, in the performance of work at Florida Gulf Coast University requires access to Florida Gulf Coast University data.

Office of Records Management
The Office of Records Management is a unit of professionals within FGCU that aid the university constituents with training, records inventory, and compliance with state and federal laws governing document management, security, retention and destruction.

PROCEDURES

Use of Restricted Data in Your Daily Job

(If applicable)

It is understood that your position at FGCU may require you to work with restricted data, and during your required interaction with that data, you may need to store this data.

- Restricted data may be stored on a departmental share folder in an unencrypted state.
- If you must store restricted data on a FGCU desktop or laptop computer, the data must be encrypted.
- Instructions for encrypting data or devices can be found on the Business Technology Services website
- It is your responsibility to ensure that the data is encrypted and deleted from your computer once the data is no longer needed and meets Florida retention schedules. Please see FGCU Policy 3.032 Records Management Policy for more information on retention schedules.

Accessing Restricted Data Remotely

- If your job requires you to access restricted data while not at work, you must use the university virtual private network (VPN) system to do so. You may access restricted data without using the VPN if you are accessing systems that are maintained or contracted by FGCU (such as Gulfline or the university's learning management system), where the system requires a secure connection (SSL) and user authentication to gain access to the data.
- You are strongly advised *not* to download restricted data to your computing device (university provided or not).
- If you must download restricted data to your computing device, the data must be encrypted immediately after downloading.
- It is your responsibility to ensure that the data is encrypted and deleted from your computer once the data is no longer needed and meets Florida retention schedules. Please see FGCU Policy 3.032 Records Management Policy for more information on retention schedules. Instructions for encrypting data or devices can be found on the Business Technology Services website.

Transmission of Restricted Data

- Restricted data should *never* be sent to another person or agency via

email regardless of who provides the email system.

- If you need to share restricted data with other FGCU employees, you must use the departmental share folder or the cross departmental folders.
- If you are required to send restricted data over the Internet to an outside person or agency, the data must be encrypted, and a secure transfer protocol must be used.
- If you are unable to send the data via a secure transfer protocol, then a non-secure protocol can be used only if the data is encrypted.

Printing or Copying Restricted Data

- If you must print restricted data, you must immediately retrieve the printed pages from the printer.
- If you must make copies of restricted data, then you must be present at the time of the copy and may not use an outside service to copy the data. You are responsible for all copies of the restricted data and must make sure they are destroyed or secured when not in use.

Physical storage of Restricted Data

- 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.
- Printed restricted data must be shredded in a cross cut shredder approved by Records Management when the data in this format is no longer needed and has met Florida retention schedules.
  Please consult the Office of Records Management with any questions you may have regarding storage, document management, security, retention and destruction.

Faxing Restricted Data

- You may *not* fax restricted data.
- You may receive restricted data from an individual or entity as long as you use the university fax server, are by the fax machine waiting for the fax or have the fax machine in a secure room.

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 FGCU Helpdesk at 239-590-1188.

These Following Devices Are *Not* Permitted Storage Devices for Restricted Data

The following devices mobile storage and mobile computing devices **should *not*** be used to store, transport, or backup restricted data.

- CD's or DVD's
- cloud-based file storage services (such as DropBox, Google Docs, Sky Drive, etc.)
- personal or university owned flash drives, external hard drives, external storage devices of any kind
- personal or university E-mail
- personal or university phones

These Following Devices Are Permitted if Encryption is Used to Store Restricted Data

- personal or university desktop computers
- personal or university laptops
- personal or university tablets

If you are unsure of the device, or if you are unsure of the type of data you wish to store, contact the FGCU Helpdesk at 239-590-1188 before you use the media or device to store such data.

Disposal of Devices Used to Store Restricted Data

Disposal of computing and storage devices must be in compliance with the university policy on equipment disposal. Even if the device was not used to store restricted data, the device should be properly scrubbed or destroyed to prevent any FGCU data from leaving the university.

The following university owned devices must be returned to the FGCU Helpdesk for proper disposal:

- desktop computers
- laptop computers
- mobile/smart phones
- printers

- tablets

We have attempted to define all devices that currently exist, however, new devices not expressly defined in this document, may need to be returned to the FGCU Helpdesk for proper scrubbing.

The following devices with data must be disposed of through Records Management to insure proper data destruction.

- magnetic storage devices (diskettes, tapes, USB hard drives)
- optical storage devices (CDs, DVDs)
- memory storage devices (SD cards, thumb drives, flash drives, etc.)
- portable devices that make nonvolatile storage available for user files (cameras, MP3 and other music players, audio recorders, smart watches, cell phones, tablets)

Data not expressly defined or categorized

Every attempt has been made to define restricted data; However, if you should encounter data that is not explicitly discussed in this document, treat the data as restricted until a determination can be made. Contact the Office of Records Management for clarification of the proper data storage, security, retention, and destruction methods.

RELATED INFORMATION

Chapter 119, F.S.
Chapter 1B-26.003 State Rule
FGCU Policy 3.006 Education records
FGCU Policy 3.017 Department Employee Files
FGCU Identify Theft Program April 21,2009
FGCU Policy 3.024 Notification of Social Security Number Collection and Usage
FGCU Policy 3.022 Technology Acceptable Use
FGCU Policy 3.032 Records Management Policy

HISTORY

New 01/30/13

APPENDICES

There are no appendices

DRAFT DATE 10/15/13 **Please use TRACK Changes in this document**	**Florida Gulf Coast University** Policy Manual	Policy: **Number to *be assigned in the General Counsel's Office***
	Title: Restricted Data Policy _____	**Responsible Executive**: Vice President for Administrative Services and Finance_____ **Responsible Office**: Business Technology Services_____

APPROVED

_____ _____

President Date