Florida Gulf Coast University

Security Plan

BOG Reg 3.0075

Information Technology Services
8-27-2019

Table of Contents

Introduction (Purpose and Intent)

The IT Security Plan defines the information security standards and procedures for ensuring the confidentiality, integrity, and availability of all information systems and resources under the control of Information Technology Services (ITS).

The FGCU ITS Security Plan supplements the Official Security Policies, Standards, and Procedures that have been established for FGCU. This security plan is intended to comply with the regulations and policies set down by the State of Florida, 3.075 Security of Data and Related Information Technology Resources

Scope

The standards and procedures set down in the FGCU ITS Security Plan apply to all information systems and resources connecting to the FGCU network.

Risk Management

FGCU ITS will manage risk by identifying, evaluating, controlling, and mitigating vulnerabilities that are a potential threat to the data and information systems under its control; it will execute its defined risk management process on an ongoing basis, periodically assessing risks and implementing new controls in response to changes in its information systems as well as to changes to federal, state, and FGCU regulations and policies.

ITS assesses its systems using the confidentiality, integrity and availability triad. Systems that contain restricted or confidential data rank high in confidentiality etc. These rankings are compiled in the ITS application list and serve as a guideline for how to secure the system.

✓	Title		Company	Confidentiality	Integrity	Availability ↑
	Active Directory	•••	Microsoft	1 - High	1 - High	1 - High

Sample Application List Entry

As part of its information security program, FGCU also provides security awareness training for faculty, staff, and students.

Federal/State Laws and Regulations

Acceptable Use Policy

Policy outlining acceptable use of the University computing resources. This is a general policy that specifies and gives examples of what is considered misuse of resources and the actions that can be taken in case of misuse.

Restricted Data Policy

This policy outlines a data classification standard that identifies certain data (like social security numbers, or credit card numbers) as restricted data. The policy guides users on how to handle and use this data in their day to day job and outlines safe practices for the use of this type of data.

FGCU also follows FERPA and HIPAA guidelines

Information Security Roles and Responsibilities

This list identifies groups of users or individuals who have been designated as holding responsibility to assist with the safeguarding of the FGCU's systems and data that is stored in these systems.

Executive Sponsor

Executive Sponsor is the Vice President of Administrative Services and Finance and responsible for ensuring security posture aligns with University's goals, objectives, and strategic vision.

Chief Information Officer

The Chief Information Officer is the highest-ranking IT officer. The Chief Information officer is responsible for providing technology management, development, planning, procurement, security, and implementation activities related to the delivery of quality information services and products for FGCU

Information Security Manager

The Information Security Manager is responsible for administering the information security program/policies/procedures at FGCU, as directed under FLBOG regulation 3.0075 and is the primary security contact reported to the Board of Governors Director of Information Resource Management. Currently, the ISM at FGCU is the Senior Director ITS Infrastructure, Operations and Security

Incident Response Team

The Incident Response Team is responsible for handling incidents as defined in Information Technology Services incident management procedure. The incident management procedure outlines the steps to take in the event of a technology incident.

Information Assurance Council (IAC)

The Information Assurance Council is the steering committee for FGCU's Information Assurance Program. The IAC is responsible for assessing the effective use of current information technology and information systems in support of the University's mission and strategic plan. It reviews the status of existing technologies, systems, and networks, and prepares recommendations for their continuous improvement.

Data & Information Strategy Council

The Data & Information Strategy Council is the governing body of Data Stewards charged with data quality standards, reporting, analytics and decision support. The Data & Information Strategy Council creates data policies and procedures that ensure privacy and security of the data in FGCU information systems.

Data Stewards

Data Stewards have the ultimate organizational responsibility for functionality of a system, and the data in that system. They are responsible for determining data and information needs in their respective functional area of responsibility. Data Stewards adhere to the standards, policies and procedures set by the Data & Information Strategy Council.

Management

Managers oversee information for their respective areas of responsibility and ensure compliance with all applicable federal, state laws and Regulations as well as FGCU Information Security Policies.

Department Information Assurance Liaisons

The Department Information Assurance Liaisons are employees designated by each department. They may be the Department Head or an Office Manage

All Users

A User is any person who accesses data via a computing system to accomplish work tasks at FGCU. Users have access to only the data they need to perform their work tasks.

Inventory of Restricted data

ITS works with all FGCU departments to compile an inventory of restricted data. Once a year, each department is asked to update its restricted data inventory, in which they indicate:

- What type of restricted data is used in their department
- Where this data is stored (physically or electronic)
- Who has access to the data
- Who the owner of the data is
- The business purpose of the data

In addition, ITS deployed monitoring software that assists with locating and inventorying electronic restricted data.

Access Control and Transmission of Restricted Data

The restricted data policy outlines how to handle transmission of restricted data and emphasizes that any data transferred to a non-approved storage location must be encrypted. Access to these locations is provided on an as needed basis and reviewed during the annual network access audit performed by ITS.

Reporting and Handling Security Violations and Consequences

ITS has created an incident response plan that specifically outlines what to do in instances where a security breach, or loss of restricted data is suspected. Please see the ITS Incident Response plan for additional information.

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

All violations of the security plan as well as any other technology security procedures will follow Florida Gulf Coast Universities Disciplinary Actions as stated in Regulation: FGCU-PR5.016 (Disciplinary Action). This policy outlines the consequences for not complying with university policies and other inappropriate behavior at work.

Methods for Ensuring Laws Regulations, Guidelines and Policies are Distributed Regularly

Users may find all FGCU policies on the FGCU General Counsel website located at: https://www.fgcu.edu/generalcounsel/policies/

Verifying Adherence to FGCU's Security Plan

ITS has a variety of processes that it uses to monitor compliance with the processes outlined about:

- Annual network access audits
- Review of rights inside of the financial/HR/student system
- Annual restricted data inventory