FLORIDA	**OFFICIAL**
POLYTECHNIC	**TECHNOLOGY SERVICES**
UNIVERSITY	**PLAN**

Subject/Title: Information Security Plan
Date Last Revised: 2020.01.28
Responsible Division/Department: Technology Services
Initiating Authority: Ben Beachy, Chief Information Officer

PURPOSE AND SCOPE

The Florida Polytechnic University Information Security Plan ('Plan') summarizes the University's policies and controls for managing risks to the confidentiality, integrity, and availability of University information technology systems.

The Plan is reviewed and updated annually in compliance with the Florida State University System Board of Governors regulation 3.0075 – Security of Data and Related Information Technology Resources.

The Plan supplements University policies and Technology Services standards and procedures.

ROLES AND RESPONSIBILITIES

PLAN

University Policies

FPU-11.00111P – Data Security Plan

Establishes policy requirements around user responsibilities for safe computing, user account management, and password controls.

Supported by:

- FPU-TS – Account Management Standard
- FPU-TS – Risk Management Standard
- FPU-TS – Data Security Standard
- FPU-TS – Mobile Device Management Standard
- FPU-TS – Access Management Standard

FPU-11.0018P – Appropriate Use of IT Resources

Establishes policy requirements for users of University information technology resources and consequences for policy violations; and establishes a limited expectation of privacy and outlines University monitoring and audit principles.

Supported by:

- FPU-TS – Data Security Standard

- FPU-TS – Mobile Device Management Standard
- FPU-TS – Access Management Standard

FPU-11.0017P – Electronic Communications and Data Transmission

Establishes policy requirements for electronic communication within the University.

Supported by:

- FPU-TS – Data Security Standard

FPU-11.001P – Mandatory Information Security Training-Employees

Establishes the policy requirement for annual information security training of all employees.

FPU-11.00115P – Virus and Spyware Protection on Computing Devices

Establishes the policy requirement for installed and updated anti-virus software on all devices connected to University networks.

Supported by:

- FPU-TS – Patch Management Standard

FPU-11.0014P – Use of IT Resources when Traveling Abroad

Establishes policy requirements for use of University information technology systems while traveling outside the United States of America.

Supported by:

- FPU-TS – Data Security Standard

Technology Services Standards and Procedures

FPU-TS – Risk Management Standard

Establishes standards for risk management of University information technology systems.

FPU-TS – Change Management Standard

Establishes standards for change and configuration management processes for University information technology systems.

FPU-TS – Logging and Monitoring Standard

Establishes standards for logging and monitoring on University information technology systems.

FPU-TS – Patch Management Standard

Establishes standards for patching University information technology systems.

FPU-TS – Data Security Standard

Establishes standards for data security on University information technology systems.

FPU-TS – Mobile Device Management Standard

Establishes standards for managing mobile devices that connect to University information technology systems.

FPU-TS – Access Management Standard

Establishes standards for managing accounts with access to University information technology systems.

FPU-TS – Obsolete System Standard

Establishes standards for support of obsolete University information technology systems.

CHANGES

2020.01.02 Ben Beachy. Initial 2020 draft.

2020.01.28 Ben Beachy. Updated with mention of Obsolete System Standard. Other adjustments to supporting standards.