

FLORIDA	OFFICIAL
POLYTECHNIC	UNIVERSITY
UNIVERSITY	POLICY

Subject/Title: Virus and Spyware Protection on Computing Devices
FPU Policy Number: FPU-11.00115P
<input checked="" type="checkbox"/> New Policy <input type="checkbox"/> Major Revision of Policy <input type="checkbox"/> Minor Technical Revision of Policy
Date First Adopted: March 18, 2016
Date Revised:
Responsible Division/Department: Information Technology Services
Initiating Authority: Tom Hull, Vice President and Chief Information Officer

A. APPLICABILITY/ACCOUNTABILITY:

This policy applies to Users connecting to the Florida Polytechnic University (the "University") network including employees, students, vendors and guests. Users include all individuals who utilize, possess or have access to University Information Technology ("IT") Resources whether through University IT Resources or through an individual's personal device or through computers accessing and transmitting information via University IT Resources. University IT Resources include University computers, mobile computing devices, telecommunications systems, lab equipment, networks, printers, software, data, database systems and all other University-owned or leased ("University- owned") IT resources involved in the processing, storage, accessing and transmission of information.

B. POLICY STATEMENT:

- University-owned computing devices. All University-owned computing devices must have antivirus/antispyware software installed. IT is responsible for managing the installation and updating of University-owned devices with antivirus/antispyware software.
- User-owned computing devices. A User connecting a User-owned computing device to the University network must ensure that the computing device has antivirus and antispyware software that is the latest version.
- Consequences of policy violation. A User who is an employee and fails to comply with this policy may face disciplinary action up to and including termination. A User who is a student and fails to comply with this policy may face discipline under the Student Code of Conduct.
- IT reserves the right to disconnect any computing device from the University network if the computing device is found to be or is suspected of being infected with a computer virus/spyware/malware.

POLICY APPROVAL	
Policy No. FPU-11.00115P	
 Initiating Authority	<u>3-18-16</u> Date
 Policies & Procedures Review Committee Chair	<u>3-18-16</u> Date
 President/Designee	<u>3/18/16</u> Date
Approved by FPU BOT, if required	 Date