

**IT Asset and Computer Purchasing Policy # 1910.002**

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY
TBD	TBD	Division of Information Technology

**POLICY STATEMENT**

The purpose of this policy is to outline guidelines for the purchase, management and disposal of Information Technology (IT) assets and computer systems owned by Florida International University (FIU).

**1. Procurement**

- Vendor Selection
  - All IT assets and computer systems need to meet the standards set by the Division of IT which meets hardware standards and aligns with security and compliance requirements. The university's preferred vendor is the FIU Panther TECH store as all systems meet these standards and computers purchased through FIU Panther TECH will already be imaged with standard configurations.
- Hardware Selection
  - Devices need to meet the recommended [hardware standards](#)
- Purchase Authorization
  - All IT asset and computer system purchases need to be pre-approved by the appropriate department head or designated authority. The Division of IT will review all purchase requests to ensure compliance with this policy.

**2. Inventory Management**

All purchased IT assets need to be logged in to the FIU's IT Asset Management System. The College IT Administrator or designee is responsible for maintaining an accurate inventory of all IT assets and ensuring proper tracking and accountability.

**Assets purchased through the FIU Panther TECH store will be automatically logged into the asset management system by the store and documented accordingly.**

All computers purchased with university funds remain the property of the University until disposed of through the University's Surplus Program.

**3. Standard Configuration Compliance**

All purchased computer systems, such as but not limited to desktops, laptops, and servers, need to adhere to the established [standard configurations](#) set by the Division of Information Technology. These configurations ensure compatibility with existing infrastructure and help maintain a secure and efficient computing environment. The standard configurations will include:

- Management Tool Configuration
  - Joined to FIU's Active Directory
  - Installation of required enterprise management agents
  - Configuration for remote monitoring and support
  - Compliance with institutional security protocols
- Operating system specifications
- Software applications
- Security software configuration and settings
- Recommended hardware specifications

#### 4. Refresh Rate

The following refresh cycle has been established to ensure that systems are up-to-date, secure, and supported by the vendor:

- IT Assets and computer systems should be refreshed when:
  - Desktops/Laptops reach a predetermined age
  - They no longer meet performance requirements.
  - They are no longer supported by the manufacturer.
  - They are too expensive to repair or maintain.
  - They have been subject to critical vulnerabilities.
- Departments need to follow end of support schedules set up by manufacturers. When the end of support date is published, they should begin planning a replacement prior to the end of support.
- Refresh Schedule:
  - **Desktop and Laptop Computers:**
    - **3-5 Year Cycle**
      - These devices typically undergo a refresh every 3 to 5 years based on performance, manufacturer support, and operational requirements.
  - **Servers:**
    - **5-7 Year Cycle**
      - Servers generally have a longer life cycle, but they should still be refreshed every 5 to 7 years.
  - **Networking Equipment (Switches, Routers, Firewalls, etc.):**
    - **5-7 Year Cycle**
      - Network hardware will be refreshed according to the manufacturer's recommended lifespan, and if support becomes inadequate, a refresh may be necessary.
  - **Printers and Peripherals:**
    - **5-7 Year Cycle**

- These devices should be evaluated for performance at least every 5 to 7 years.

#### **5. Disposal**

IT Assets should be surplusd following the property control surplus process and media sanitization guidelines.

- IT assets that have reached the end of their life cycle cannot be repurposed and joined onto the FIU network.
- IT assets which do not meet FIU's minimum hardware standards cannot be repurposed or joined onto the FIU network.
- IT assets

#### **6. Exceptions**

Any exceptions to this policy need to be documented and submitted to the IT Security Office for review and approval. Exceptions will be considered on a case-by-case basis and may require additional justification.

#### **7. Enforcement**

Hardware or software that is not purchased following this policy and meeting the standard will not be supported.

### **SCOPE**

This policy applies to all faculty, staff, and departments involved in the procurement, management and disposal of IT assets and computer systems at FIU when using university and grant funds for IT assets and computers purchases.

### **REASON FOR POLICY**

This policy aims to minimize risks, ensure compliance with standard configurations, and facilitate the effective management of IT resources.

### **DEFINITIONS**

<b>TERM</b>	<b>DEFINITIONS</b>
Information Technology Asset	Any hardware, software, or digital information that an organization utilizes in its daily operations. These assets can include physical devices like computers, printers, and servers.
PantherTech	Campus technology store, located in the Graham Center.

Management Agents	Active Directory/Intune for windows systems. Addigy for MacOS devices.
Surplus	Surplus technology refers to outdated or unsupported technology assets.

### ROLES AND RESPONSIBILITIES

#### Division of Information Technology:

- Update configuration standard and hardware requirements
- Provide guidance and support to IT Administrators
- Manage the Enterprise IT Asset Inventory Application

#### Panther Tech:

- Work with IT Administrators on their IT Asset purchases to make sure they meet the requirements.
- Provide guidance, compare/demo equipment, and report inconsistencies
- Verify purchase includes standard image configuration
- Responsible for registering equipment in Asset Management and other tools as applicable (i.e. Apple School Manager)

#### College/Department/Unit IT Administrators or designee:

- Review hardware specs for their units to ensure that they meet the requirements.
- Manage IT Asset inventory
- Manage IT Assets following the Standard Configuration Plan
- Follow supplier end of support announcements

### RELATED RESOURCES

Configuration Standard: <https://security.fiu.edu/governance#standards>

IT Security: System and Application Management Policy

<https://policies.fiu.edu/files/562.pdf>

Procurement Manual: <https://controller.fiu.edu/wp-content/uploads/2021/05/ProcurementManual.pdf>

PantherTech: <https://panthertech.fiu.edu/departments>

Supported Hardware: [https://fiu.service-now.com/sp?id=kb\\_article\\_view&sysparm\\_article=KB0010712](https://fiu.service-now.com/sp?id=kb_article_view&sysparm_article=KB0010712)

Supported Operating Systems: [https://fiu.servicenow.com/sp?id=kb\\_article&sysparm\\_article=KB0011768](https://fiu.servicenow.com/sp?id=kb_article&sysparm_article=KB0011768)

Media Sanitization: [https://fiu.servicenow.com/sp?id=kb\\_article&sysparm\\_article=KB0010893](https://fiu.servicenow.com/sp?id=kb_article&sysparm_article=KB0010893)

Surplus: <https://controller.fiu.edu/departments/accounting-reporting/asset-management/surplus/>

## CONTACTS

Division of Information Technology  
IT Security Office  
11200 SW 8 ST, PC534a  
Miami, FL 33199  
305-348-1366  
[security@fiu.edu](mailto:security@fiu.edu)  
<https://security.fiu.edu>

## HISTORY

Initial Effective Date: TBD

Review Dates (review performed, no updates): N/A

Revision Dates (updates made to document): TBD