FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Applications Software Resources: Purchasing, Licensing, & Use
1930.005

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
October 2007	May 17, 2024	Division of Information Technology/ IT Security Office

POLICY STATEMENT

In order to ensure compliance with university-wide information security policies and to ensure proper purchase, licensing, and use of applications at Florida International University, only legally owned software can be used on university-owned computers, servers, devices, or networks. This can be software that is available from Division of Information Technology, PantherTech, for which there is a university-wide license, user or department-purchased software, or shareware that has been obtained appropriately through PantherTech or proper purchasing procedures.

Software as a service (SaaS) applications must also have appropriate licensing and contract agreements in place.

SCOPE

The scope of this policy encompasses the university community, including faculty, staff, persons of interest, and students, as well as and authorized asers of university IT Resources (such as consultants, vendors, etc.).

REASON FOR POLICY

The purpose of this policy is to safeguard the integrity and security of FIU's information technology environment. By strictly regulating the procurement, licensing, and utilization of software applications, this policy aims to minimize the risk of unauthorized software usage, potential security breaches, and legal liabilities. Additionally, by delineating clear guidelines for the University Community and Authorized Users, this policy promotes accountability, transparency, and responsible stewardship of university data and resources.

DEFINITIONS	
TERM	**DEFINITIONS**

Software as a Service (SaaS)	Is a way of delivering applications over the internet as a service. Instead of installing and maintaining software, it is accessed via the Internet.
PantherTech	Is your one-stop shop for your software and hardware needs. Panther TECH provides the FIU community with software for personal use, software for FIU-owned computers, and repairs and upgrades.
Application	Is an end-user program
HECVAT	Higher Education Community Vendor Assessment Toolkit. A HECVAT is a standardized assessment framework designed specifically for higher education institutions to evaluate the security and privacy practices of third-party vendors who provide services or products to the institution.
Vendor Risk Management Program	Is the program that involves assessing the operations, IT and security controls employed at the vendor

ROLES AND RESPONSIBILITIES

Departments/Users:

Follow the proper purchasing and licensing procedures when purchasing software and applications.

For applications or software that handle sensitive data (such as FERPA, HIPAA, ePHI, GLBA, CUI, etc.) the university's Technology Evaluation Group (TEG) will be tasked with evaluating the vendor's cybersecurity and accessibility controls through a HECVAT questionnaire requested from the vendor.

- IT Security specialist is responsible for entering the vendor’s HECVAT data into the enterprise's Vendor Risk Management Program.
- TEG will assess the controls outlined in the HECVAT and provide recommendations.

PantherTech:

- Obtain enterprise licensing for software and applications. Sell software and hardware.

RELATED RESOURCES

Procurement Manual:
http://finance.fiu.edu/purchasing/Docs/ProcurementManual.pdf

Vendor Risk Management:
https://security.fiu.edu/vendor_risk_management

Technology Evaluation Group (TEG):
https://it.fiu.edu/teg/

Software at FIU
https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB0011775

CONTACTS

Division of Information Technology
IT Security Office
11200 SW 8 Street, PC534A
Miami, FL 33181
Telephone Number: (305) 348-3712

HISTORY

Initial Effective Date: October 2007
Review Dates (*review performed, no updates*): N/A
Revision Dates (*updates made to document*): May 27, 2021; May 17, 2024

FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY PROCEDURE

Applications Software Resources: Purchasing, Licensing, & Use
1930.005a

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
October 2007	May 17, 2024	Division of Information Technology/ IT Security Office

PROCEDURE STATEMENT

This procedure outlines the steps to be followed when purchasing software and applications at FIU, particularly for those handling sensitive data. The TEG process ensures that all applications undergo thorough cybersecurity and accessibility control evaluation to mitigate risks and maintain compliance with relevant regulations.

1. Determine Software/Applications Scope:
Identify the need for software or applications within your department or user group. Determine if the software or application will handle sensitive data such as FERPA, HIPAA, ePHI, GLBA, CUI, etc.

2. Submit Request to TEG:
If the software or application is identified to handle sensitive data, submit a request to the university's Technology Evaluation Group (TEG) for cybersecurity and accessibility control evaluation. Include details about the software/application, its intended use, and any pertinent information regarding data sensitivity. (NOTE: all this can be done through the TEG process. See: https://it.fiu.edu/teg/)

3. TEG Evaluation:
Upon receiving the request, TEG will initiate the evaluation process.
This involves:

a. Requesting a filled-out HECVAT (Higher Education Community Vendor Assessment Toolkit) from the vendor.
b. Reviewing the submitted HECVAT to assess the vendor's security and privacy practices, as well as the controls implemented within the software/application.
c. Conducting cybersecurity and accessibility control evaluation based on the information provided in the HECVAT and any additional documentation or communication with the vendor.

4. Vendor Risk Management:

TEG will input the information gathered from the HECVAT into the enterprise's Vendor Risk Management Program. The controls outlined in the HECVAT will be evaluated by TEG cybersecurity risk specialists to determine their effectiveness in mitigating risks associated with the software/application.

5. Approval and Procurement:
Based on the results of the TEG evaluation, a recommendation will be made regarding the software/application for use within the institution. If approved, proceed with the procurement process following the proper purchasing and licensing procedures.

NOTE: Division of IT and IT System Administrators shall not (re)install application software on any University-owned device (computer, server, or network) unless it can be shown that the software is properly licensed.