Campus Acquisition of Information Technology Policy

Effective Date:	September 1, 2025
Supersedes:	N/A
Policy Review Date:	To be reviewed every 3 years from effective date
Issuing Authority:	Research Foundation President
Policy Owner:	Vice President of Sponsored Programs and Regulatory Affairs
Contact Information:	RFCOSponsoredPrograms@rfsuny.org

Reason for Policy

Research Foundation funds may be used to purchase Information Technology to assist with sponsored research and other campus activities. In order to protect all campus-based resources from the threat of cyber-attack it is important that Information Technology purchased with RF funds is compatible with and integrated into the campus's information security environment.

Statement of Policy

Operating Locations must have processes in place to provide reasonable assurance that Information Technology purchased with RF funds is compatible with and integrated into the Operating Location's information security environment. These processes must adhere to the following minimal standards when purchasing Information Technology using RF funds:

1) The process must require either a) **approval** by the Operating Location's CISO, CIO, or designee of all Information Technology purchased with RF funds prior to purchase; or b) **notification** of the Operating Location's CISO, CIO, or designee of all Information Technology purchased with RF funds along with the establishment of a **reasonable waiting period** following that notification before the Information Technology may be deployed into the campus computing environment.

2) Based on their local risk evaluation and tolerance, Operating Locations may choose to adopt a definition of "Information Technology" subject to their local processes that is different than the Definition that appears below. Operating Locations may also include in their local processes Information Technology that is not purchased but which is used in RF activities (e.g. free software and/or personally-owned devices).

The Research Foundation Operations Manager or designee must work with the local CIO or CISO or their designee to develop a local process that complies with this policy or to incorporate RF procurement of Information Technology into existing campus security processes. The local process must outline the specific approval or notification requirement and the definition of Information Technology that will apply as outlined in 1) and 2) above, including the applicable waiting period if notification is used.

If an Operating Location uses an all-funds approach to Information Technology procurement where a review of information technology occurs, and this incorporates RF purchases, that process will automatically satisfy the requirements of this policy as long as the location continues to use that process for Information Technology purchased with RF funds.

This policy is in addition to any relevant RF or SUNY procurement policies and any other local campus or SUNY policies governing information technology.

Responsibilities

The following table outlines the responsibilities for compliance with this Policy:

Responsible Party	Responsibility
PIs, Project Directors, and RF Employees and Representatives	Follow the applicable local process for any purchases of Information Technology using RF funds.
Operations Manager or designee	Work with the local CIO or CISO or their designee to develop a local process that complies with this policy or to incorporate RF procurement of Information Technology into existing campus security processes.

Definitions

Cloud Platform Services – A set of computing resources, tools, and services offered by a cloud provider over the internet to help organizations build, deploy, and manage their applications and computing infrastructure. Examples include Amazon AWS, Microsoft Azure, Google Cloud Platform, Alibaba Cloud, Oracle Cloud, IBM Cloud, and Linode.

Cloud Storage – A type of cloud computing service that enables users to store and access their files and data over the internet from anywhere and on any device. Examples include Dropbox, Google Drive, OneDrive, iCloud, Box, and Carbonite.

Computers – Includes desktops, laptops, servers, and tablets.

Information Technology – Includes Computers, Operating Systems, any Software deployed in a local network (excludes Software as a Service, Cloud Storage, Cloud Platform Services and any other third-party web-based Software), Networking Equipment, and Other Equipment as defined in this policy.

Networking Equipment – Includes switches, routers, Wi-Fi access points, firewalls, VPN gateways, modems.

Operating Location – An RF office located at a SUNY campus location or other SUNY location supporting the RF mission and SUNY operations overseen by an Operations Manager.

Computer Operating Systems – Software that manages and controls computer hardware and software resources, enabling other applications to run on a computer. Examples include Windows, MacOS, Linux, iOS, and Android.

Other Equipment – Any device that connects to a local network.

Software – A set of instructions, data or programs used to operate Computers and execute specific tasks.

Software as a Service (SaaS) – A cloud computing model in which software applications are delivered over the internet by a provider and accessed by users through a web browser or mobile application. Examples include Office 365, Salesforce, DocuSign, and Google Workspace.

Related Information
None

Forms
None

Document History

Date	Summary of Change
September 1, 2025	New Policy.

Feedback
Was this document clear and easy to follow? Please send your feedback to webfeedback@rfsuny.org.