UCF

UCFIT
University of Central Florida
Information Technology

Title: **UCF IT Client Endpoint Services Design Package**	**Effective: 9/19/18** **Revised: N/A**
Approved By: Michael Sink, Associate VP & COO, UCF IT	**Page 1 of 43**

TABLE OF CONTENTS

I. SUMMARY, OUTCOMES AND OBJECTIVES 3
II. DEFINITIONS 4
III. METHODS OF SUPPORT 7
IV. DESKTOP AND MOBILE DEVICES 8
DEVICE LIFE CYCLE OVERVIEW 8
METHODS OF SUPPORT PER CATEGORIZATION 9
DEVICE LIFE CYCLE 11
V. PERIPHERALS AND ACCESSORIES 12
METHODS OF SUPPORT PER CATEGORY 12
VI. CLIENT DESKTOP SOFTWARE 14
SOFTWARE LIFECYCLE OVERVIEW 14
METHODS OF SUPPORT PER CATEGORY 14
SOFTWARE LIFECYCLE 17
SOFTWARE EVALUATION CRITERIA 19
SUPPORTED OPERATING SYSTEMS 19
SOFTWARE DELIVERY METHODS 20
SOFTWARE DELIVERY METHOD USE-CASES 21
AUTOMATED SOFTWARE DEPLOYMENT CRITERIA 21
VII. ELEVATED ACCESS 22
ACCESS NEED VERIFICATION 22
ACCESS LEVEL ASSESSMENT 22
ACCESS FULLFILMENT 23
BUSINESS CASE BY DEVICE CATEGORY 23
ELEVATED ACCESS AGREEMENT LIFECYCLE 25
VIII. ACQUISITION 26
TECHNICAL CONSULTATION 28

PROCUREMENT 29
UCF IT PRODUCT CATALOG 32
EQUIPMENT LOAN 34
IX. FILE, PRINT, SCAN AND NETWORK ACCESS 35
FILE ACCESS 36
PRINT & SCAN ACCESS 41
NETWORK ACCESS 42
X. REFERENCES AND ADDITIONAL CONSIDERATIONS 42
UCF IT PRODUCT CATALOG 42
UCF IT SERVICE CATALOG 42
ADDITIONAL CONSIDERATIONS 42

I. SUMMARY, OUTCOMES AND OBJECTIVES

This Client Endpoint Services Design Package articulates the endpoint computing services commonly requested and consumed by students, faculty and staff at the university. For years at UCF, these services were provided by distributed IT units across campus. Because there were no common standards or guidelines on how these services should be provided, service levels, processes and client expectations varied among these distributed IT units. This design package attempts to align endpoint computing services both within the units currently serviced by UCF IT and serve as guidelines for remaining distributed units as they prepare to become a part of UCF IT. Services currently covered in this design package include:

- Desktop and mobile devices support
- Peripherals and accessories support
- Client desktop software support
- Elevated access to endpoints
- Acquisition of information technology, including devices, peripherals, and software
- File, print, and network access

The tenets in designing the Client Endpoint Services Design Package include:

- **Collaboration**: Leveraging the university community to understand the broad range of diverse needs of our institution, and to design service offerings that deliver value to all members of the community.
- **Best practices**: Consolidating the best existing practices and adopting new practices across the institution that:
  - Deliver our services faster and at higher quality
  - Resolve incidents faster
  - Provide excellent customer service
  - Streamline the processes for our clients and IT staff
  - Comply with information security, university, and other governing policies and regulations
- **Ongoing review and improvement**: Considering the evolving requirements of our clients by reaching out through feedback, relationships, and adjusting our services accordingly.

The sections below define common terms and methods of support provided, and detail the procedures for client services offered by UCF IT.

II. DEFINITIONS

These definitions provide a common reference and terminology for terms used within UCF IT.

Accessory Device	Any ancillary device that attaches to an end-user computer, tablet, or laptop that does not communicate with the host operating system. Examples include surge protectors, uninterruptible power supplies, analog loudspeakers, power strips, etc. Please Note: Peripherals are a separate classification of device, see definition below.
BYOD	Bring Your Own Device; any non-university-owned device that is asked to be serviced by UCF IT Support Center in any capacity.
BYOS	Bring Your Own Software; Software in physical or digital form not owned or approved for use by the university.
Basic Software Support	Support will be limited to software troubleshooting in which the operating system does not have to be upgraded, reinstalled, or otherwise "refreshed" to make the computer functional. Installed and approved applications will be supported as long as the existing equipment meets the minimum system requirements for the application that requires troubleshooting.
Business Case	Documented scenario, providing justification for UCF IT approved standards and deviations from the Client Endpoint Services Design Package.
Device Category	Computing devices grouped by type and function. Examples include laptop, desktop, mobile, managed, and unmanaged.
Device Lifecycle	The amount of time a device receives full support. The standard device lifecycle is 5 years from date of purchase. When possible or financially feasible, the device warranty length should be made to match the 5-year lifecycle window. Lifecycle windows will be reviewed periodically.
Display Device	Any peripheral that connects to a computer and conveys visual information to the user.
Elevated Access Agreement	UCF IT-provided list of terms a client must agree to in order to request and receive elevated access to fulfill the need of an approved business case.
Elevated Access	Access to elevate the security access for a computer process that a standard user account does not have permissions to run on managed or unmanaged university-owned equipment.
End-of-Life	A university-owned device that has been determined is no longer effectively usable by UCF IT or has become nonfunctional beyond repair. At this point, the device will need to be prepared and requested to be sent to surplus for proper processing.
Freeware	No-cost or Open-source software that has passed evaluation by UCF IT.
Grandfathered-in Devices	A broad selection of currently supported devices that will receive additional support outside of the standard device support lifecycle for

	a predetermined amount of time. Grandfathered-in (GFI) window is three years from adoption.
Grandfathered-in Software	Software application(s) that meets any of the minimum support criteria and was previously supported by existing support areas of UCF IT as of July 1, 2017. The recommended support window is three years from adoption. Grandfathered-in software is subject to the evaluation step of the Software Support Lifecycle. Any software purchased beyond the start of the support window will be subject to all lifecycle and support classification standards.
In-House Software	University-developed or significantly customized software, which receives Internal Software Support.
Input Device	Any peripheral that transmits data into a host computer.
Internal Software Support	Software Support lifecycle phase that includes freeware, internally developed software, or other custom software that would only receive support from UCF IT.
In-Warranty Device	University-owned devices with a valid warranty as of the date in which service or support was reported and/or requested.
Legacy	University-owned software in production that is determined through the evaluation process to receive the same or better support than it was receiving when it transitioned to the support model in the Client Endpoint Services Design Package.
Licensed with Vendor Support	University-owned software under a valid license with a vendor-side support agreement. Support will be provided by UCF IT and the vendor as necessary.
Licensed without Vendor Support	University-owned software under a valid license that does not have a vendor-side support agreement. Support will only be provided by UCF IT.
Managed Device	Any university-owned device that is actively managed via any available centralized system such as SCCM, AirWatch, Intune, etc. This type includes but it is not limited to devices joined to a domain.
Obsolete Device	Any peripheral that isn't compatible with a supported operating system, or any device that is Out-of-Warranty and has been diagnosed as beyond repair by UCF IT.
Out-of-Lifecycle Device	University-owned device in which both the warranty and service-window has lapsed. The service-window is typically a maximum of five years from the date of purchase.
Out-of-Warranty Device	University-owned devices with an expired warranty or service contract; typically provided by the vendor or other 3rd party entity.
Peripheral	Any ancillary device that attaches to or communicates with a device that requires an operating system to function. Please Note: Accessories are a sepereate classification of device, see definition above.
Primary Device	Desktop device directly assigned to an individual or laptop device used over 50% of the time by the assigned individual as confirmed by the individual's supervisor.

Printing Device	Any peripheral that connects to a computer and conveys information via paper, ink, or toner.
Recommended Product Lines	The existing supported product lines as negotiated by the university. The Recommended Product Lines will be reviewed and updated as our campus agreements and business requirements change over time. The recommended product lines include but are not limited exclusively to the ones detailed[1] in this document. The UCF IT Product Catalog will be the definitive source on currently supported product lines. Recommended Product Lines do not include infrastructure and networking device support (servers, storage, wireless access points, etc.)..
Specialty Devices	A device that communicates via the network or a computer that requires non-IT expertise for full-functionality verification. Examples include network-attached pianos, network-attached x-ray scanners, digital microscopes, etc.
Support Exceptions Audiences	Group(s) of stakeholders that may require support beyond our support and lifecycle standards that should be provided by staff with specialized training and/or in a specified method. The support level may need to be reviewed on a case-by-case basis.
UCF IT-Approved Item	A peripheral, part, or supply that has been vetted by UCF IT and has been designated to receive full support. A UCF IT-Approved Item shall be listed on the UCF IT Recommended Peripherals List.
University-owned Device	Any device within or outside specified support criteria that was purchased or acquired using university-owned funding.
University-owned Non-Compliant Devices	Devices that have not met any of the grandfathered-in, lifecycle, warranty, or support minimum requirements. These devices will receive BYOD level of support with referrals to other university services if necessary.
Unmanaged Device	Any university-owned device that is not actively managed by any available system.
Unsupported	Software application(s) that do not meet any of the minimum support criteria. This includes software that has lapsed its "Grandfathered-in" status, Retired Software, and software that did not pass evaluation.

III. METHODS OF SUPPORT

Support for information technology will be delivered in a variety of methods. The support methods offered vary depending on ownership and lifecycle stage of the technology.

Methods of Support	Notes
Over-the-Phone	Automated or human guidance providing as much direct support or guidance as possible through the phone to other resources and/or self-service troubleshooting steps.
Email	Providing as much direct support or guidance as possible through email to other resources and/or self-service troubleshooting steps.
Online Chat	Providing as much direct support or guidance as possible through chat to other resources and/or self-service troubleshooting steps.
Remote Assistance	Guidance to other resources and/or interactive troubleshooting steps conducted via standard remote access tools that is within the device support level.
In-Person Dispatch	Technical staff physically dispatched to device or user on university-managed or university-leased properties only.
Self-Service	UCF IT Knowledge Base or other self-service resource.
Walk-Up	Available at designated locations, guided on-site troubleshooting and triage which may result in drop-off service or referral.
Drop Off	Repair or request scenario with university-owned equipment only.Non-university owned devices can be taken to the Student Support Desk located at the Technology Product Center.
Warranty Services	Repair scenario in which the device will be replaced or repaired in part or fully by the manufacturer or vendor.
Service Provider Referral	Technology Product Center, Student Support Desk, Faculty Multimedia Center, etc.
Procurement Consulting	Identify business requirements and/or software minimum requirements and provide recommendation of standard equipment as defined if possible. Additional consultation will be redirected to appropriate entity.
Deployment Services	The use of manual or automated tools to install, configure, manage and maintain devices.
Workaround Services	The implementation of temporary solutions aimed at reducing or eliminating the impact of known errors for which a full resolution is not yet available.
Installation Services	The performance of technician-related tasks and software configuration tasks to cause a device to provide intended services.

Elevated Access	UCF IT providing a process for a client/individual to obtain elevated access on managed or unmanaged university-owned equipment with an approved business case.
Manual Software Installation	Manual installation of a single or multiple applications on a university-owned device.
Automatic Software Delivery	Automatic installation of a single or multiple applications on a university-owned device. This can be initiated by IT or the end-user via self-service tools.
BYOD Software Delivery	Self-Service software tool(s) that can be used on non-university owned devices.
Software Training	One-on-one or group training session that assists the user with a specific piece or suite of software. Self-service and internal training documentation will be required.
Software Project Support	Upgrade, patch, installation, removal, change, or environment migration of one or multiple applications on a university-owned device(s) within Device Support Lifecycle.
Technical Consultation	Preliminary information gathering of a user's business needs for the request of equipment and/or software.
Supplies Installation	Installation of consumable supplies listed in the Product Catalog.

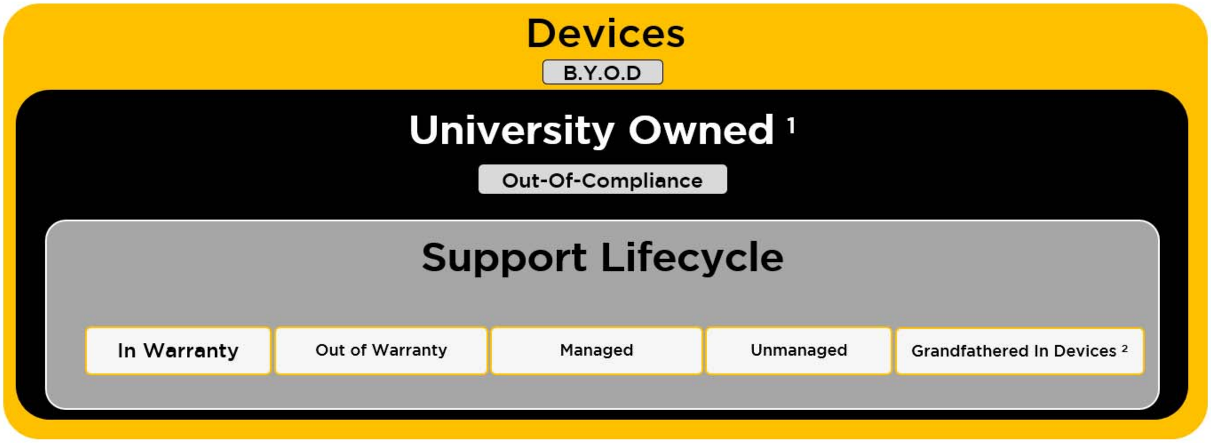
IV. DESKTOP AND MOBILE DEVICES

Below are detailed service and support level descriptions that should be referenced when attempting to identify where in the lifecycle (if applicable) the client's device, peripheral, or other supported technology item is at the time in which the incident or request has been submitted.

DEVICE LIFE CYCLE OVERVIEW

The Device Life Cycle Overview is a graphical representation of the different categories that a device can be a member of throughout the life of the device. Please note that a device can be in either "*Managed*" or "*Unmanaged*" and be part of *"In-Warranty"* and *"Out-of-Warranty"* while still being within the Support Lifecycle. *"Grandfathered-In"* devices will remain in the Support Lifecycle regardless of warranty or management status until the GFI window has lapsed.

Figure 4.1



[1] ***Including Direct Support Organizations***[2] *Hardware that is grandfathered-in will only be accepted during the adoption window and may no longer receive support after 3 years from adoption.*

METHODS OF SUPPORT PER CATEGORIZATION

Desktops and devices can be part of multiple device categories depending on its place within the support lifecycle. Below is a description of the support methods eligible to each of the possible device categories.

Managed Devices

University-owned managed devices are eligible for the following methods of support:

Over-the-Phone	Email	Online Chat
Remote Assistance	In-Person Dispatch	Walk-Up
Drop-Off	Warranty Services	Service Provider Referral
Technology Consult	Self-Service	

In-Person Dispatch will be available if the device is on UCF property. Walk-Up service will be at a designated location(s) for mobile devices. Warranty Services will be provided when applicable, and referral to other UCF services, if necessary, will also be available.

Unmanaged Devices

University-owned unmanaged devices are eligible for the following methods of support:

Over-the-Phone	Email	Online Chat
Drop-Off	In-Person Dispatch	Walk-Up
Technology Consult	Warranty Services	Service Provider Referral
Self-Service		

In-Person Dispatch will be available if the device is on university-managed or university-leased properties for critical incidents only. Walk-Up service will be at a designated location(s) for mobile devices. Warranty Services will be provided when applicable, and redirection to other UCF Group/Service Provider if necessary will also be available. Unmanaged Devices cannot reliably or effectively receive remote support. No university-owned devices will receive support less than BYOD categorized devices.

In-Warranty

Devices will receive the appropriate support and support methods as dictated by the warranty provided. Managed or Unmanaged classification will need to be determined.

Out-of-Warranty and in Lifecycle

Devices will receive support under managed or unmanaged classification.Hardware repair should be performed with new parts. UCF IT should not store or stockpile spare parts or components for use on repair.. University resources should be the primary vendor in conjunction with the UCF IT Product Catalog.

Out-of-Lifecycle and *Out-of-Warranty*

All Out-of-Lifecycle hardware repair will be referred to university-provided or other pay-for-support area(s).

Out-of-Lifecycle and Functional

University-owned, out-of-lifecycle devices are eligible for the following methods of support if still functional:

Over-the-Phone	**Email**	**Online Chat**
Self-Service	In-Person Dispatch	Walk-Up
Technology Consult	Service Provider Referral	

In this device category, several of the available support methods should have the following limitations in place:

- All hardware repair will be via Service Provider Referral at a cost for parts and labor.
- UCF IT will not provide operating system level support which would result in or is caused due to an operating system re-image, operating system upgrade, or ’Blue Screen’ failure.
- Software Application support will be dependent on the software specific minimum requirements.

University-Owned Non-Compliant Devices

Noncompliant or unsupported devices will receive at best BYOD level of support with referral to other university services for hardware and advanced software support.

DEVICE LIFE CYCLE

The Device Life Cycle consists of several steps from procurement to device surplus. These steps occur in order through the life of the device. The Support Life Cycle is within the Device Life Cycle, and is five years. Please note that there can be a scenario in which the maximum length of warranty available to the university-owned supported device is shorter than the established Support Life Cycle. In this case, a machine can become *"Out-of-Warranty"* before becoming "*Out-of-Compliance"*. However, a machine will never go "*Out-of-Compliance"* without also becoming *"Out-of-Warranty"*. Both can occur simultaneously on the same date.

1. **Acquisition**
   A device is acquired via an approved method using university funds.

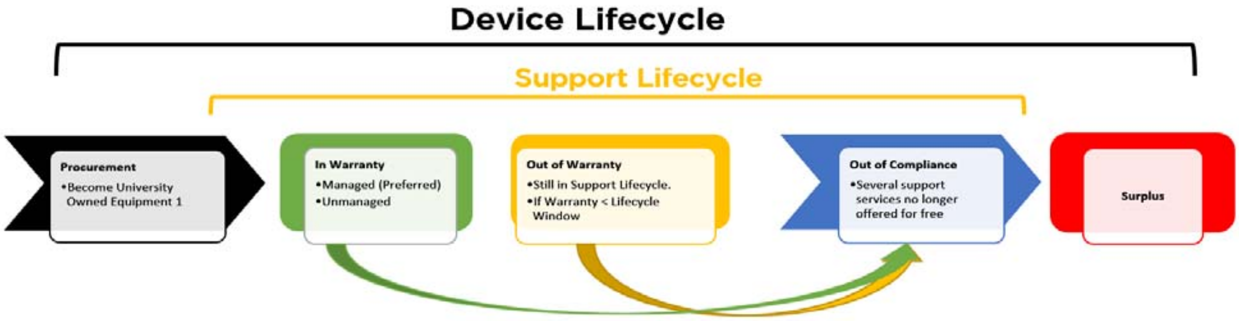
2. **Grandfathered-in**
   A device can also be *"Grandfathered-in"* if it meets the proper GFI criteria and is within the GFI window. This will be an additional entry point into the *Support Lifecycle.*

3. **Start of the Support Lifecycle**
   a. **In-Warranty:** Device begins as an "*In-Warranty"* device and can be in either a *Managed* or *Unmanaged* state. *In-Warranty* and *Managed* is the preferred configuration.
   b. **Out-of-Warranty:** The device can still be within the *Support Lifecycle* window and lapse its maximum available warranty. The only case in which a device can be in this category is if the maximum length of the available warranty is less than the current support window.

4. **Out of Compliance**
   The end of the *Support Lifecycle Window* is reached when a device becomes *Out of Compliance.* The device will receive a slightly reduced level of support for the remaining life of the device. A machine still within warranty cannot become out-of-compliance until the warranty on the device has lapsed.

5. **Surplus**
   The device has reached *End-of-Life* and is no longer deemed valuable by the institution. At this point, the device will be prepared and sent to surplus for proper processing.

Figure 4.2


Device Lifecycle
Support Lifecycle
Procurement
•Become University Owned Equipment 1
In Warranty
•Managed (Preferred)
•Unmanaged
Out of Warranty
•Still in Support Lifecycle.
•If Warranty < Lifecycle Window
Out of Compliance
•Several support services no longer offered for free
Surplus

[1] *Including Direct Support Organizations*

V. PERIPHERALS AND ACCESSORIES

Support services offered for peripherals depend on the following factors: Ownership of the peripheral, ownership of the computer to which the peripheral is attached, operating system of the computer to which the peripheral is attached, lifecycle state of the peripheral, warranty state of the peripheral, category of the peripheral, location of the peripheral, and the process by which the peripheral was procured.

METHODS OF SUPPORT PER CATEGORY

University-owned computer, approved university-owned peripheral:

The peripheral will be fully supported and is eligible to receive the following Methods of Support:

Self-service	Email	Over-the-Phone
Remote Assistance	Online Chat	Walk-Up
In-person Dispatch	Warranty Assistance	Provider Referral
Procurement Consultation	Deployment	Workaround
Installation	Repair	Supplies Installation
Drop-off		

University-owned computer, unapproved university-owned peripheral:

The peripheral is eligible to receive the following Methods of Support:

Self-service	Email	Over-the-Phone
Remote Assistance	Online Chat	Walk-Up
In-person Dispatch	Warranty Assistance	Provider Referral
Procurement Consultation	Installation	Drop-off

University-owned computer, BYOD peripheral:

The peripheral is eligible to receive the following Methods of Support:

Self-service	Procurement Consultation	Email
Phone	Online chat	

University-owned computer or university-operated network connection, university-owned specialty device:

The Specialty Device is eligible to receive the following Methods of Support:

Self-service	Email	Over-the-Phone
Remote Assistance	Online Chat	
In-person Dispatch	Procurement Consultation	

BYOD computer, approved university-owned peripheral:

The peripheral is eligible to receive the following Methods of Support:

Self-service	Email	Over-the-Phone
In-person Dispatch	Online Chat	Walk-Up
Procurement Consultation	Warranty Assistance	Provider Referral
Drop-off	Repair	Supplies Installation

Please Note: The BYOD computer is subject to device support procedures outlined in Section IV.

BYOD computer, unapproved university-owned peripheral, or Specialty device:

The peripheral is eligible to receive the following Methods of Support:

Self-service	Email	Over-the-Phone
In-person Dispatch	Procurement Consultation	

BYOD computer, BYOD peripheral:

The peripheral is eligible to receive the following Methods of Support:

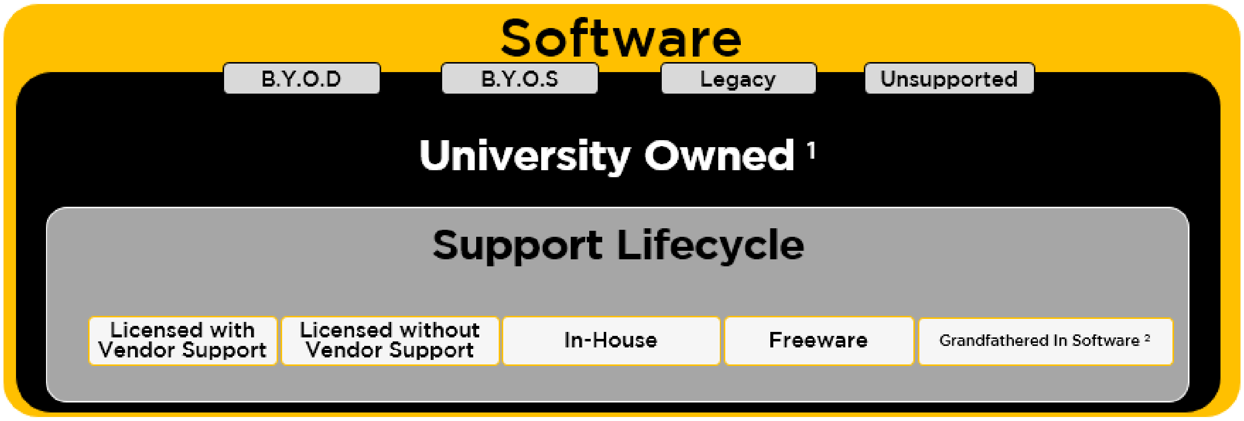
Self-service

VI. CLIENT DESKTOP SOFTWARE

SOFTWARE LIFECYCLE OVERVIEW

The Software Lifecycle Overview is a graphical representation of the different categories that software can be a member of throughout the life of the application. All software will be subject to licensing terms and conditions. “Software” in the section only refers to client desktop software.

Figure 6.1



[1] ***Including Direct Support Organizations***
[2] *Software that is grandfathered-in will only be accepted during the adoption window and may no longer receive support after 3 years from adoption.*

METHODS OF SUPPORT PER CATEGORY

Software can be part of several different categories depending on its place within the support lifecycle. Below is a description of the support methods eligible to each of the possible software categories.

Licensed with Vendor Support

Licensed software with vendor support will be provided the following methods of support:

Over-the-Phone	Email	Online Chat
Remote Assistance	In-Person Dispatch	Walk-Up
Self-service	Software Installation	Software Delivery
Software Training	Software Project Support	Technology Consult
Service Provider Referral		

Vendor support in some cases can be initiated by the end-user directly or by UCF IT on the user’s behalf. The methods of support provided by vendor(s) may vary.

Licensed without Vendor Support

Licensed software without vendor support will be provided the following methods of support:

Over-the-Phone	Email	Online Chat
Remote Assistance	In-Person Dispatch	Walk-Up
Self-service	Software Installation	Software Delivery
Software Training	Software Project Support	Technology Consult
Service Provider Referral		

In-House

In-House software will be provided the following methods of support:

Over-the-Phone	Email	Online Chat
Remote Assistance	In-Person Dispatch	Walk-Up
Self-service	Software Installation	Software Delivery
Software Training	Software Project Support	Technology Consult
Service Provider Referral		

Freeware

Freeware software that is currently supported and approved will be provided the following methods of support:

Over-the-Phone	Email	Online Chat
Remote Assistance	In-Person Dispatch	Walk-Up
Self-service	Software Installation	Software Delivery
Technology Consult	Service Provider Referral	

Freeware will not receive Software Training or Software Project Support.

Grandfathered-in Software

Grandfathered-in software will be provided the following methods of support by UCF IT until it does not pass Evaluation or three (3) years from adoption, whichever occurs first:

Over-the-Phone	Email	Online Chat
Remote Assistance	In-Person Dispatch	Walk-Up
Self-service	Software Installation	Software Delivery
Software Training	Software Project Support	Technology Consult
Service Provider Referral		

Bring your own Device (BYOD)

In the case where a user needs assistance with university-owned software on a personal device, the UCF IT Support Center will provide the following methods of support:

Self-service	Email	Over-the-Phone
Online Chat	Walk-Up	In-person Dispatch*
Software Training	BYOD Software Delivery	Service Provider Referral
Technology Consult		

*In-person dispatch will be for critical incidents only. Remote Support, Software Installation, Managed Software Delivery and Software Project support will not be provided. Software installation in this scenario can only occur via self-service method.

Legacy

All Legacy Software support should begin with a recommendation to use an alternative solution that is within the Software Support Lifecycle. If an alternative is not available or business case exception has been identified, support will be limited to the following methods of support:

Over-the-Phone	Email	Online Chat
Remote Assistance	In-Person Dispatch	Walk-Up
Self-service		

Legacy Software will not receive Software Installation, Delivery, and Training, or Project support. Subject to approved exceptions and use-cases.

Bring Your Own Software (BYOS)

BYOS will not be supported; however, software can be submitted for evaluation and possible adoption into the Software Support Lifecycle. Freeware is not included in this category and will be addressed in a separate category Above.

Unsupported

Software that will not be supported or is no longer supported; it does not receive any services.

SOFTWARE LIFECYCLE

The Software Lifecycle consists of several steps from Acquisition to Retirement. These steps can occur in order through the life of the software, but can be modified by the evaluation phase at any time. All software not acquired by pre-approved methods or the UCF IT Product catalog will require evaluation before it can enter the Software Lifecycle. Legacy software can be re-evaluated and placed back in one of the supported categories. Software will not be required to be uninstalled from production equipment until it reaches a Retired state. The evaluation step can occur at any time during the lifecycle process as well as occurring multiple times throughout the life of a software product.

1. **Acquisition**
   Software is purchased or acquired via an approved method using university-approved funding.

   a. **Grandfathered-in**
      Software can also be *"Grandfathered-in"* if it meets the proper criteria and is identified prior to the start of the support window. This will be an additional entry point into the Software *Support Lifecycle.*

2. **Start of the Software Support Lifecycle**
   The categories inside of the Software Support lifecycle can be applied in any order. The method that the software was acquired, licensed and supported by the vendor are all factors in the determination of which lifecycle category it is a part of at any given time.

   a. **Licensed with Vendor Support:**
      Software evaluated as acquired properly, licensed, and includes a valid vendor-side agreement for direct support to the university will be placed in this category. UCF IT will provide knowledge articles for support of software in this category.

   b. **Licensed without Vendor Support:**
      Software evaluated as acquired properly and licensed will be placed in this category. It will be the exclusive responsibility of UCF IT to provide support throughout the lifecycle of the software. UCF IT will provide knowledge articles for support of software in this category.

   c. **Internal Support:**
      Software evaluated as Freeware or has been developed by the university will be placed in this category. UCF IT will provide knowledge articles for support of software in this category.

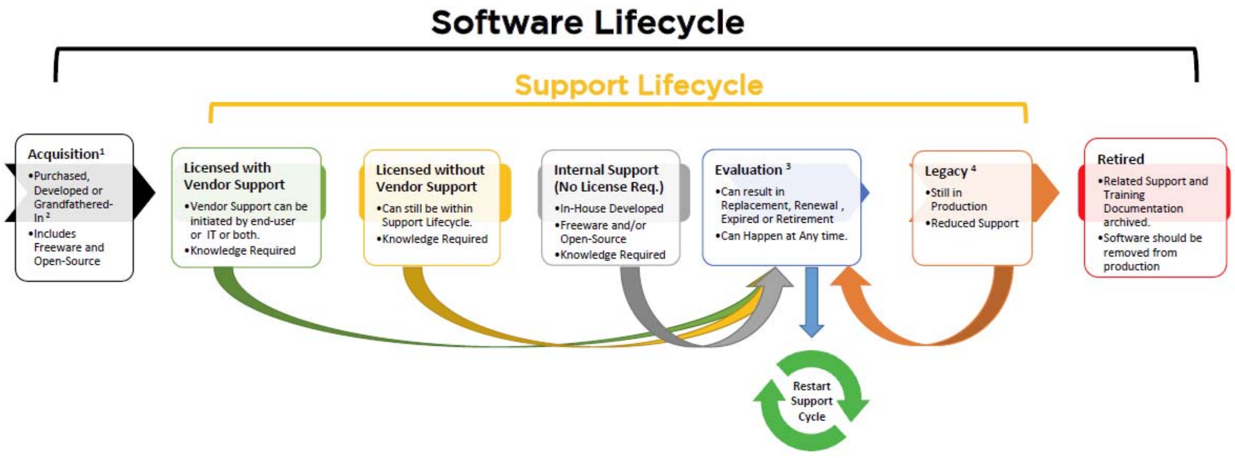
3. **Evaluation**
   The evaluation step of the support lifecycle can occur at any time between acquisition and retirement of a software package. This step is expected to occur at

least twice during the life of a software package, during acquisition prior to procurement and before retirement. However, it will more than likely be the case that the evaluation phase will happen multiple times during the life of a software package as the variables around that software package and the minimum support criteria are modified over time. The evaluation step can result in the placement of software in any of the following categories: *Licensed with Vendor Support, Licensed without Vendor Support, Internal Support, Legacy, or Retired.*

4. **Legacy**
   Software evaluated as not meeting at least one of the minimum evaluation criteria (*Security, Versioning, Age, Application Minimum Requirements, and Business Justification*) or has been deemed for retirement but does not yet have a replacement becomes a Legacy software package. Legacy software is not required to be uninstalled from the production environment. Legacy software may receive a reduced level of support when compared to the other phases of the *Software Support Lifecycle*.

5. **Retired**
   Software evaluated as having been superseded, replaced, no longer valuable to or licensed by the university, or poses a security risk, will be considered for Retirement. All retired software will require uninstallation from the production environment and all related documentation and knowledge be retired as appropriate.

Figure 6.2


Software Lifecycle
Support Lifecycle
Acquisition[1]
•Purchased, Developed or Grandfathered-In [2]
•Includes Freeware and Open-Source
Licensed with Vendor Support
•Vendor Support can be initiated by end-user or IT or both.
•Knowledge Required
Licensed without Vendor Support
•Can still be within Support Lifecycle.
•Knowledge Required
Internal Support (No License Req.)
•In-House Developed
•Freeware and/or Open-Source
•Knowledge Required
Evaluation [3]
•Can result in Replacement, Renewal , Expired or Retirement
•Can Happen at Any time.
Legacy [4]
•Still in Production
•Reduced Support
Retired
•Related Support and Training Documentation archived.
•Software should be removed from production
Restart Support Cycle

SOFTWARE EVALUATION CRITERIA

Below is a list of criteria that should be considered with every software package in which the evaluation phase of the lifecycle is being applied. Failure to satisfy any of the following criteria would make the software package eligible for Legacy or Retirement classification. Inability to satisfy the *Security* criteria without the possibility of remediation should result in immediate Retirement of the software package being evaluated. Software accessibility should be evaluated to match federal regulations and standards. Operating systems are subject to a separate review.

Security	Software that does not pose a known and/or active security exploit or threat to the university's technology or data.
Versioning	Software that is within the two most recently stable version builds unless business case requirement.
Age	Software that is still being supported by the vendor or developer when applicable. A Software Evaluation is required after any software product has been in production for five years.
Application Specific Requirements	Software that meets the requirements as provided by the vendor or developer and is aligned with the device lifecycle.
Business Case	Software that has been identified as meeting a need or business requirement in which no alternative or substitute is available.

SUPPORTED OPERATING SYSTEMS

Below is a list of currently supported operating systems. This list will need to be evaluated and updated on a regular basis. Please note that this will include operating systems that may be grandfathered-in to support.

Windows	Windows 10 within two most recent current branch for business versions or newer, Windows 8.1 and Windows 7 SP1 until no longer supported by Microsoft. Unless there is a legitimate business case, only the most current version of Windows 10 will be deployed or refreshed.
macOS	macOS 10.10 Yosemite or newer. Only macOS 10.11 or newer will be deployed or refreshed unless there is a legitimate business case or technical limitation.
Linux[1]	Any currently supported version of Ubuntu within Long Term Support (LTS) or any currently supported version of Red Hat that is actively licensed. LTS with Hardware enablement will be required for active deployment when applicable. [1] *For the operating system to be applicable for installation, a business case or research purpose needs to be approved by UCF IT.*
iOS	iOS 9 or newer. Mobile devices should be updated to the latest available OS when hardware permitting.

Android	Android OS 5.0 (Lollipop) or newer. Mobile devices should be updated to the latest available OS when hardware permitting.

SOFTWARE DELIVERY METHODS

Software can be provided to students, faculty and staff in a variety of ways. The UCF IT Support Center will provide some level of support for the following methods:

Self-Service Manual	Installation is performed by the user with physical or digital install media as provided by UCF IT or acquired using university funds.
Self-Service Automated	Installation is performed by a managed system (SCCM Application catalog, AirWatch, etc.) and is triggered or initiated by the user. In some cases, approval for the automated install will be required before it is initiated. Administrative Access to the device is not required.
Manual Installation	Installation is performed in-person by a member of UCF IT using physical or digital install media.
Remote Manual Installation	Installation is performed remotely by a member of UCF IT using physical or digital install media.
Virtual Application	Software is provided in a virtual environment by UCF IT. (UCF Apps, RemoteApp, etc.) Software using this delivery method will not require installation of the software package itself but may require a pre-requisite of a platform specific client for a fully-featured experience. Software via this method will require the user(s) to be granted access to the application(s) before consumption.
Managed Deployment	Installation is performed by a managed system (SCCM Application catalog, AirWatch, etc.) and is initiated or scheduled by a member of UCF IT. In some cases, Change Advisory Board requests will need to be submitted and approved before large-scale deployments can occur.
Software-as-a-Service	Software-as-a-Service (SaaS) is provided in a centrally-hosted, platform-agnostic environment in which no local-device installation would need to occur. Most Web-based applications and services would be delivered in this method.

SOFTWARE DELIVERY METHOD USE-CASES

On Premises – Managed

Software-as-a-Service	Self-Service Manual	Self-Service Automated
Managed Deployment	Remote Manual Installation	Manual Installation
Virtual Application		

Off Premises – Managed

Software-as-a-Service	Self-Service Manual	Self-Service Automated
Managed Deployment	Remote Manual Installation	Manual Installation*
Virtual Application		

**Manual Install available if UCF IT is housed at remote location.*

On Premises – Unmanaged

Software-as-a-Service	Self-Service Manual	Manual Installation
Virtual Application	Remote Manual Installation	

Off Premises – Unmanaged

Software-as-a-Service	Self-Service Manual	Manual Installation*
Virtual Application	Remote Manual Installation	

**Manual Install available if UCF IT is housed at remote location.*

BYOD

Software-as-a-Service	Self-Service Manual	Virtual Application

AUTOMATED SOFTWARE DEPLOYMENT CRITERIA

When determining if software should or should not be distributed or made available in an automated way the following set of standard criteria should be used.

Device Impact	20 devices or above.
Priority	Not any of the following: Critical Incident, High Priority Request, or VIP
Licensing	Does not breach licensing agreement or exceed number of allowed installations.
Technical Limitation	Not restricted by specific application installation media or would result in undesired outcome as determined by UCF IT.
Evaluation	Predetermined delivery method or required for desired outcome.

VII. ELEVATED ACCESS

UCF IT recommends and encourages that all administrative functions on the endpoints be performed by UCF IT technical staff. Standard access will still allow you to make customization and other user-specific changes but will require IT staff when installing new software or hardware to the endpoint.

UCF IT acknowledges the need for a process in order for a client to obtain elevated access to perform critical job functions outlined in an approved business case. Any client who needs elevated access to perform functions of their job role must request access through this process.

ACCESS NEED VERIFICATION

UCF IT will document a client's request to obtain elevated access on managed or unmanaged university-owned equipment. Clients must provide:

- First and last name
- NID
- Email address
- Phone number
- Supervisor name, supervisor email, and supervisor phone number
- Business case
- Acknowledgement of access to restricted or highly restricted data
- Data contracts with outside entities
- List of devices involving elevated access
- Timeframe access is desired for up to 1 year

Client must acknowledge and agree with the terms outlined on UCF IT Elevated Access agreement. Client's supervisor must approve of the elevated access requested and verify the information provided. UCF IT support center will evaluate each business case against the required criteria for each device category.

If a client's business case for elevated access is approved the client, client's supervisor, and unit representative will be notified. This will complete the access need verification, and the client's request moves to access level assessment.

If a client's business case for elevated access is denied the client, client's supervisor, and the unit representative will be notified and provided an opportunity to discuss the request to resolution. If no resolution can be reached between all involved parties, the Information Security Office (ISO) will be consulted for final decision.

ACCESS LEVEL ASSESSMENT

UCF IT will determine the minimum level of access required to satisfy the needs of the approved business case. UCF IT will use all available tools/resources to properly outline the level of access to be provided and communicate with the client to confirm all needs of the approved business case are met. Once the plan is outlined and the client agrees, access level assessment is complete; the request moves on to access fulfillment.

ACCESS FULLFILMENT

UCF IT will configure the changes outlined during the access assessment on managed or unmanaged university-owned equipment. This equipment must be the equipment identified and approved during access requirement verification. Once changes are applied, UCF IT will confirm the access provided is functioning properly and the business case has been adequately addressed.

ELEVATED ACCESS AGREEMENT

The Elevated Access Agreement is a UCF IT provided list of terms a client must agree to in order to request and be provided with elevated access to fulfill the need of a business case. These terms include but are not limited to:

- Local UCF IT administrative account cannot be deleted or modified.
- Local user accounts cannot be created by the client.
- Client must adhere to all UCF technology and communication policies, located at http://policies.ucf.edu/
- Elevated access is subject to review in all incidents involving computer viruses, malware, or compromised data.
- Elevated access is subject to review in cases requiring technician support due to issues caused by client's elevated access.
- Not adhering to terms can result in removal of elevated access.
- Supervisor is responsible for contacting UCF IT to remove elevated access for the requested client that falls in between yearly review periods.

BUSINESS CASE BY DEVICE CATEGORY

Business cases provided by the user during access requirement verification will be evaluated for approval based upon the criteria required for each device category.The following statement applies to all of the endpoint related business cases:

> *"Job role requires use of unmanaged, non-standard programs that require elevation on a reoccurring basis, and/or job role requires use and management of peripherals that require elevation on a reoccurring basis"*

UCF Owned and Managed Desktop

Examples include

- Software required for job role that requires elevated access to run
- Research lab equipment that requires elevated access to use or maintain.

UCF Owned and Managed Laptop

- Examples include:Frequent travel without access to IT support verified by supervisor.
- Travel for research, multiple conferences, sabbatical, etc.

UCF Owned and Managed Laptop, Primary Device

Example Include:

- Laptop is user's primary device.
- Travel without access to IT support verified by supervisor.
- Specific travel and return dates must be provided. Examples include travel for research, multiple conferences, sabbatical, etc.

UCF Owned and Managed Mobile OS Device

Example Include:

- Software required for job role requires elevated access to run
- Research lab equipment requires elevated access to use or maintain.

UCF Owned Unmanaged Device

Example Include:

- Software required for job role requires elevated access to run
- Research lab equipment requires elevated access to use or maintain.
- Research lab equipment managed by outside vendor.

At this time, Non-Network attached unmanaged devices do not need to be reviewed for elevated access concerns. Examples include a research lab computerized device offline and not connected to any UCF resources.

UCF Owned Printers

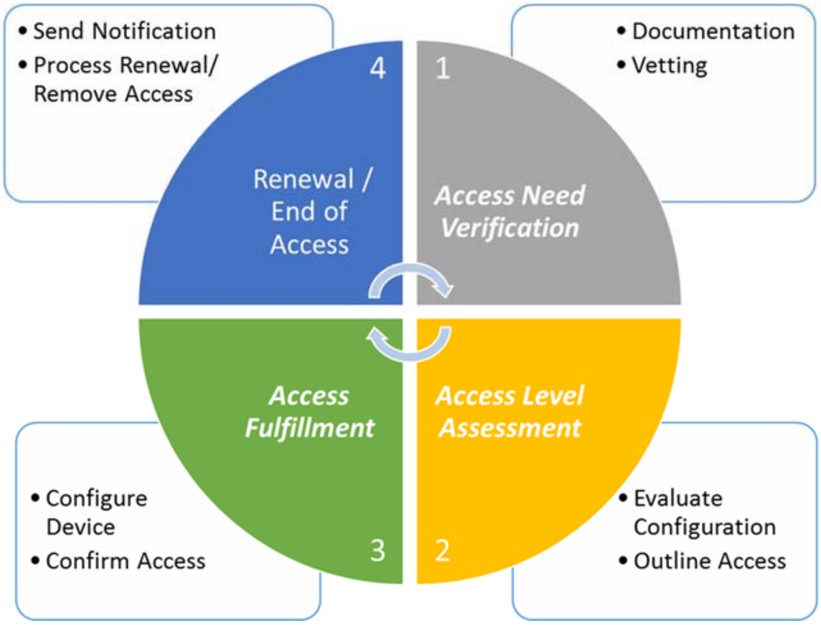
Printing devices connected to the UCF network will not be provided elevated access. Clients must use appropriate support channel to gain access to restricted functions. Ex: Print Management, Address Book Management, User Roles

Non-network attached printing devices do not need to be reviewed for elevated access.

ELEVATED ACCESS AGREEMENT LIFECYCLE

Elevated access granted will be provided for a period up to one (1) year at a time. UCF IT will notify the listed client 30 days prior to access expiration date. A client with elevated access must submit a renewal request and begin access requirement verification prior to elevated access end date to maintain continuous access. Events requiring review of elevated access prior to one (1) year include but are not limited to transfer of access to a new device, operating system refresh, job role change, virus/malware incidence, data compromise, and incidents requiring technician support due to issues caused by client's elevated access.

Figure 7.1
Elevated Access Agreement Lifecycle



IT units have up to one (1) year from UCF IT policy adoption to transition existing clients with elevated access to the UCF IT elevated access policy. If a client with existing elevated access is provided a new device, reassigned an existing device or device requires an operating refresh, the new policy goes into effect at that time.

TECHNICAL SUPPORT STAFF

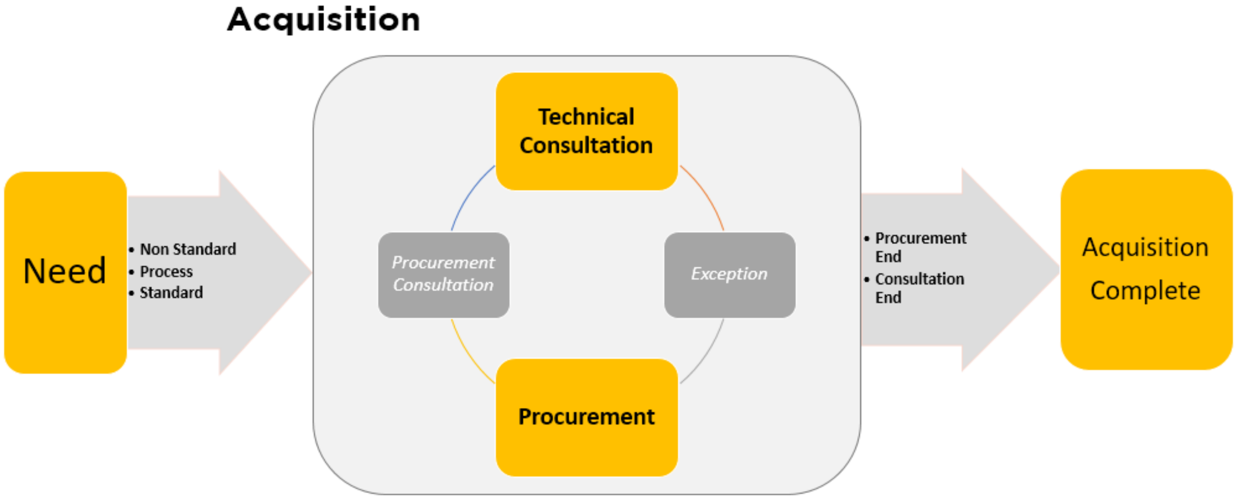
UCF IT technical support staff will need elevated access on all managed or unmanaged university-owned equipment in order to perform the functions defined by their job role. Accounts with elevated access will be separate from their NID account. A training period must be established for all new hires by their supervisor and completed before any elevated access can be provided. Length of time varies upon position hired. Specialized training and certifications will be required before elevated access is provided to technical support staff on specialized systems containing restricted or highly restricted data. Examples include HIPAA, FERPA, CJIS, PCI, etc. UCF IT staff must sign and agree to all terms on the UCF Confidentiality Agreement as part of the hiring process. All university-owned equipment must require a BIOS password or equivalent set by UCF IT.

VIII. ACQUISITION

Standardization of Acquisition processes across UCF IT ensures efficiency and scalability while reducing costs, promoting hardware and software standards, allowing for improved business intelligence, security, service and support. For these reasons, UCF IT should be the central and primary channel for all university information technology purchases.

Acquisition includes two major processes: Consultation and Procurement. A sub-process to Consultation is the Exception request process that considers purchases of non-standard items. Additional consultation processes are required to support Procurement.

Figure 8.1

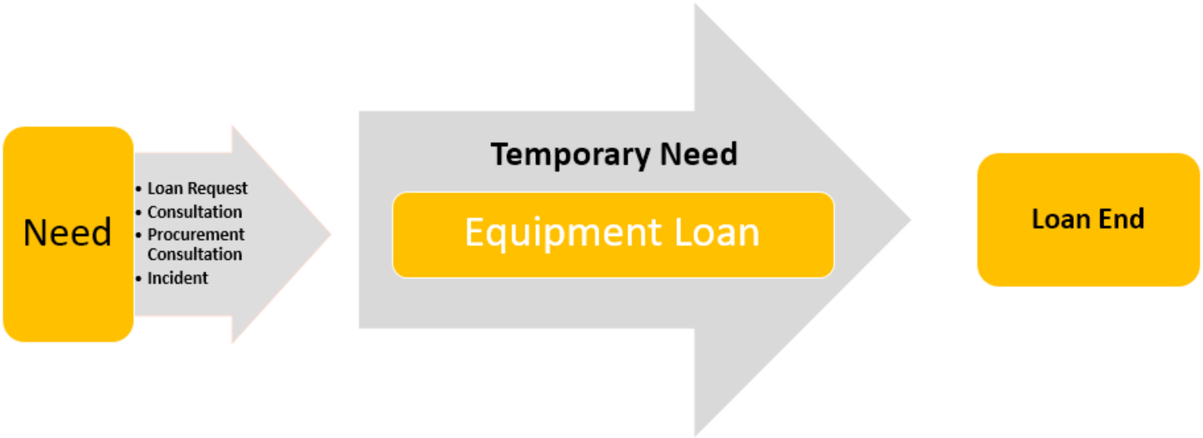


In addition to Consultation and Procurement, two Supporting Processes must be further developed and continually updated: Equipment Loan and UCF IT Product Catalog.

Temporary needs, identified through consultations, requests and incidents, may be satisfied by loaning equipment.

Figure 8.2

Loan Equipment



TECHNICAL CONSULTATION

Technical Consultation is the process by which requirements are gathered, needs are clearly defined and specific information about technology solutions are identified. Technical Consultation happens before Procurement can begin.

Technical Consultation not only happens before Procurement, but also in parallel, receiving continual reassessment as needed. Consultation may be averted when IT needs can be satisfied by the selection of UCF IT Product Catalog items. UCF IT consultants provide Technical Consultations; UCF IT consultants are familiar with the distinct needs of the clients and are subject matter experts in helping to identify them.

Technical Consultation differs from Procurement Consultation, which the Procurement section outlines.

- To initiate a Technical Consultation, the client requests a Technical Consultation from UCF IT Consultants through a tracked workflow process when the clients cannot define their IT needs or need help selecting appropriate solutions. The request may be initiated through self-service, email, phone call, or chat. The request results in a consultation ticket regardless of initiation method.

- The outcome of Technical Consultation is a Procurement Request that is considered to have Technical Approval and, if needed, Exception Request Approval. Technical Consultations may also result in a redirection for selection from the UCF IT Product Catalog, an Exception Request, a Loan Equipment recommendation, or a cancelation.

Consultation Supporting Processes

Exception Requests: these are submitted when there is client demand or perceived need for items outside of the UCF IT Product Catalog, but could be met with standard catalog items. Exception requests are submitted by a consultant and are reviewed and approved by designated personnel in UCF IT. The client accepts that the level of support from UCF IT may vary depending on the nature of the Exception Request. Support levels are addressed in sections II, III, and IV. Exception Requests include:

- Desired items or services (costs, configurations, and technical information)
- Identification of stakeholders and requirements.
- Comparison (cost and specifications) to standard and approved items.
- Justification.
    - Merit of justification is reviewed and granted on a case-by-case basis. Reasons of merit include:
        - It is determined that need cannot be met by UCF IT Product Catalog Items
        - Project or audience requirements can only be met with non-standard items

Review of Standard Catalog Product Requests: In the case of a selection from the UCF IT Product Catalog, a Technical Consultation is not needed. However, the requests shall be monitored to ensure the product selected meets the client's use case. Before Procurement Requests for Standard Catalog items can be fulfilled, indication of UCF IT approval is captured through a workflow.

Data Gathering and Procurement Request: Data gathered through Technical Consultations is captured and entered into a Procurement Request by the IT Consultant when the need for a purchase is identified. See procurement section for required data.

Exception Data Review: Data relating to already approved or denied Exception Requests is available for reference and is reviewed by IT Consultants. Such data may present alternative solutions or indicate need for modification of the UCF IT Product Catalog.

Technical Consultation Closure: Consultations are considered fulfilled when Procurement Requests are fulfilled. Procurement Staff and IT consultants should not close Technical Consultation tickets prior to fulfillment of the Procurement Request.

PROCUREMENT

Procurement includes the transactional and supporting processes to purchase IT products and services that meet the specific requirements defined by consultation or to acquire products from the UCF IT Product Catalog. IT Procurement staff work closely with IT

Consultants and clients by way of Procurement Consultation processes throughout the cycle of a purchase. Procurement includes post-fulfillment support. Examples of post-fulfillment support include purchase history, returns, exchanges, refunds, etc. UCF IT Procurement will manage the fulfillment and post-fulfillment support, eliminating the need for units to continue doing so.

Procurement Consultation, a sub-process of Procurement, addresses basic client and UCF IT Consultant questions. Procurement Consultation is provided by Procurement personnel and is primarily focused on supporting the UCF IT Product Catalog and the procurement processes, including order status, documentation requests, etc.

Procurement Requests

Procurement Requests are submitted by clients for UCF IT Product Catalog items and are reviewed by IT Consultants. Non-standard items will require Consultation and potential Exception Request approval. For non-standard hardware and software acquisitions, the UCF IT Consultant submits the Procurement Request. All Procurement Requests are captured through a request ticket. Procurement Request tickets are initiated only via electronic workflow to ensure that required approvals are captured.

Required Data

Procurement requests contain specific item information and all information necessary for purchasing, approval, and funding.

- Item Data
  - Price, vendor, quantity, model, manufacturer, specifications, configuration, descriptive data (color, size, etc.), and quotations.
- Funding Data
  - Source: Department, Project, or Grant ID/AR/External
  - Billing address
  - Authorized persons to spend (must be on Finance's DAL list)
  - Billing contacts (DDC, RFO, AXA, etc.)
- Logistics Data
  - Delivery address(es)
    - Deliveries are to be delivered to the appropriate UCF IT Support Center zone.
  - Delivery urgency
    - May incur additional shipping handling fees
  - Recipients / Delivery contacts
- Approvals
  - Technical approvals (see Technical Consultation) are granted after final order configuration is determined. Changes required after initial approval

require a new technical approval. Technical approvals are required for non-standard items. Technical approvals indicate fitness for purpose and fitness for use. When a Technical Consultant submits a Purchase Request, it is considered technically approved.

- Financial Approvals follow Technical Approval. They may be granted or denied only after final cost and funding source is determined. Financial Approvals are a requirement for Procurement to proceed and may be obtained through Procurement Request workflow. Provided there are no changes to the technical configuration, increases to costs during procurement require new financial approval. Decreases in cost do not require approval, but notification will be provided to the submitter (designated point of contact, client, or technical consultant).

- Special financial approval processes are needed for certain funding sources. Funding source does not circumvent UCF IT standards for hardware and software supported by UCF IT. Special financial approval may be obtained through Procurement Request workflow. Such approvals include:

    - Foundation
    - Research Foundation
    - External Funding
    - Procurement Card (P-Card)
    - Leasing

- Administrative approvals should be obtained before Procurement begins. Administrative approvals are coordinated by both the Technical Consultant and the Procurement Consultant and are captured by Procurement and may be obtained through Procurement Request workflow. Such Administrative approvals can include:

    - VP Signature indicating approval
    - Information Resource Request (IRR) approval
    - Telecom approval
    - Information Security approval
    - Accessibility approval
    - Facilities approval
    - Exception Request approval
    - General Counsel approval
    - Purchasing officer approval

- Supporting documentation should be included in the purchase request. Supporting documents include:

        - Quotations
        - Administrative forms
        - Lease documents
        - Contract documents

Notification

Procurement notifies billing, consultants, and logistics contacts with order confirmations, changes to orders (require approval), and order completion (invoicing).

Procurement Review

Procurement reviews the Procurement Request and checks necessary data and documentation is in place. It is recommended that procurement staff and consultants review and complete a checklist for non-standard requests. In addition, procurement reviews:

- Product availability
- Vendor price comparison
- Existing resources
    - Check for in-stock items that may meet needs
    - Check for software license availability

Procurement requests are completed when the goods or services are accepted by the designated recipient. Procurement maintains purchase data and documentation for later access and review. Procurement is a key component in asset management processes.

UCF IT PRODUCT CATALOG

The UCF IT Product Catalog is a collection of items that fulfill client needs and are standardized to streamline support service. Clients can request items from the UCF IT Product Catalog without consultation. Requests for UCF IT Product Catalog items receive oversight by IT consultants in lieu of Technical Consultation. The standard catalog is developed and maintained by a UCF IT Product Catalog working group. This working group is made up of consultants and procurement staff and perform the following functions: Reviewing, Negotiating, Publishing, Promoting, and Reporting on UCF IT Product Catalog:

Review

- Review of previous purchases and Exception Requests to determine new or replacement items to fit need.
- Review of marketplace data outside of UCF.
- Review of technology changes to make sure equipment is supportable.

- Updating the UCF IT Product Catalog items when necessary due to technology changes, obsolescence, purchasing cycles, or other market factors such as price changes.
- Review funded or approved information technology projects such as Technology Fee.
- Identification of manufacturer, vendor, model, specifications and configurations.
- Identify products that will satisfy most client needs, will minimize Exception Requests, and will satisfy technical concerns of the university.
- Secure equipment for evaluation and demonstration (vendor loans, try-and-buy, seed units)
    - The equipment in this evaluation pool is available for loan to allow for independent evaluation by UCF IT staff. Availability is first-come-first-serve.
    - The evaluation pool loans are demonstrated, monitored, managed, stored, and returned to vendors centrally.
    - The evaluation pool is separate from the Loaner Equipment program.

Negotiate

- Forecasting university need for each item identified for the UCF IT Product Catalog
- Negotiation with vendors to secure the best pricing on identified equipment.

Publish

- Maintenance of the UCF IT Product Catalog and publishing to media (Web, print, portal) accessible to the UCF community.
- Presenting UCF IT Product Catalog items so that clients can see the high-level specifications and configuration of items and recommended use cases.

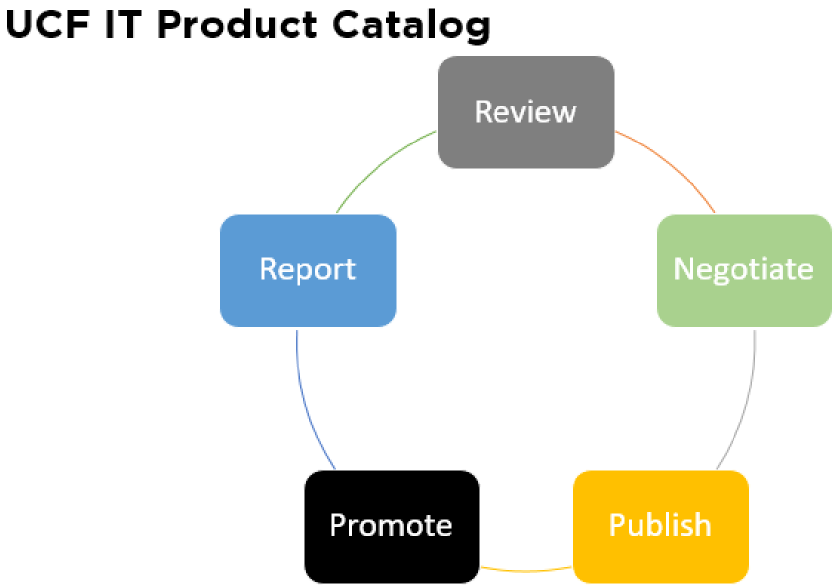
Promote

- Communication and marketing about the availability of standard catalog items to IT and the UCF community.

Report

- Maintain reports showing how much was purchased of each item, and how much savings or efficiencies were achieved.

Figure 8.3



EQUIPMENT LOAN

Equipment Loan processes can satisfy temporary need of clients. Processes to accommodate loaner equipment will help to reduce unnecessary spending, provide clients with incident work-around (hot-swap), and allow clients to complete one-time and infrequent projects.

Eligibility

Eligibility is limited to active faculty, staff, and student employees in good standing with the university. Exceptions may be made for acceptable business cases as determined by UCF IT.

Separate loan equipment pools should be established for students and faculty/staff where necessary to address funding source requirements such as those associated with the Technology Fee.

- ***Employee Equipment Loan:***
  - During Technical or Procurement Consultation it may be established that a client's need is temporary and can be satisfied by a loan of equipment. The consultant may recommend the client to check-out equipment, detail what pieces should be checked out, and direct the client to the check-out location.
  - Equipment loans may also be hot-swapped as an incident work-around for non-functional devices. Employees may check out a device to use while their regular workstation is being repaired or replaced.

        - Employees may reserve equipment in advance (with or without consultation) to accommodate planned events like conferences, travel and presentations.
        - Employee loaner equipment is available for pick-up and drop-off at one or more UCF IT Support Center zone locations.
            - Employees must present identification.
    - It is recommended that inventory management of the Equipment Loaner Pool be developed in conjunction with Asset Management and Academic Technology Services.
        - Equipment check-out frequency:
            - UCF IT may provide consultation with recommendation to purchase in cases where checkout periods are extended, frequent, or repeated.
            - Non-return of loaner equipment results in fines or the full equipment cost. Fines are payable in full or through payroll deduction.
            - Fines for damages to the loaner equipment can be assessed
        - Employee loan durations can vary. The standard duration is three (3) days, but justification can be provided when a longer duration is necessary. A maximum checkout period of thirty days is recommended.
        - Setup help for loaner equipment being used on campus can be requested from UCF IT Support Center.

- ***Loaner Equipment***

    - Should adhere to campus device and lifecycle standards for all UCF IT supported areas and audiences.
    - Should be portable, such as laptops, tablets, etc. Desktop loans are not recommended.
    - Should include peripherals and connectivity accessories in order for the employee to use the loaner equipment effectively (cables, adapters, docking stations, etc.).

- ***Exceptional Audiences and High Availability***

    - For audiences requiring high availability and special configurations, dedicated "hot swap" systems should be reserved in the IT Support Center zone. Hot swap systems are available for Incident tickets only and not available for checkout for general use.

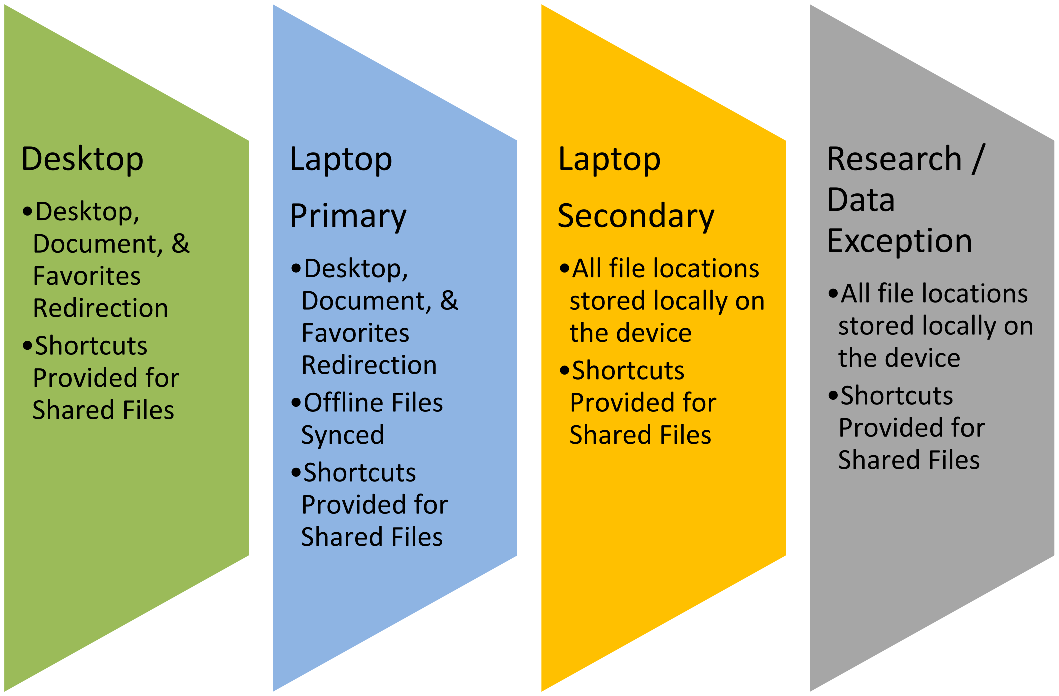
IX. FILE, PRINT, SCAN AND NETWORK ACCESS

This section defines how UCF IT clients will access University-provided file, print, scan, and network resources. Access is structured and provided around device and user categories.

FILE ACCESS

Device File Access Structure

UCF IT will store client device data and provide access as outlined below per device category. All file storage locations UCF IT uses will be reachable from the UCF wired, secure campus wireless, and outside networks with VPN authentication.



Desktop

- Desktop, Document, & Favorites Redirection
- Shortcuts Provided for Shared Files

Laptop Primary

- Desktop, Document, & Favorites Redirection
- Offline Files Synced
- Shortcuts Provided for Shared Files

Laptop Secondary

- All file locations stored locally on the device
- Shortcuts Provided for Shared Files

Research / Data Exception

- All file locations stored locally on the device
- Shortcuts Provided for Shared Files

Desktop

Clients using a UCF owned and managed desktop will have their desktop file location, documents file location, and favorites (bookmarks) from all UCF IT supported web browsers redirected to UCF IT centralized storage. Redirected data will only be located and accessed on the centralized storage and will not be stored on the local device. Client's desktop computer must be connected to the UCF network and the client must authenticate in order to access files. Shortcuts will be provided on the device in order for clients to access their UCF IT shared and client file locations.

UCF Owned and Managed Laptop Primary Device

Clients using UCF owned managed desktops will have their desktop, documents, and favorites from all UCF IT supported web browsers redirected to UCF IT centralized storage. Redirected data will only be located and accessed on the centralized storage and will not be stored on the local device. Offline local copies of the files will reside on the physical device and synchronize once the client has connected to the UCF network. Shortcuts will be provided on the device in order for clients to access their UCF IT shared and client file locations.

UCF Owned and Managed Laptop Secondary Device

Clients using UCF owned managed laptop secondary devices will not have their desktop, documents, and favorites from all UCF IT supported web browsers redirected from centralized storage provided by UCF IT. Data will only be stored on the local device. Shortcuts will be provided on the device in order for clients to access their UCF IT shared and client file locations.

UCF Owned Research Devices & Data Exceptions

Clients using UCF owned laptop or desktop devices with an approved business case will have the option to not have their desktop, documents, and favorites from all UCF IT supported web browsers redirected to centralized storage provided by UCF IT. Data will only be stored on the local device. Shortcuts will be provided to clients in order to access their UCF IT shared & personal file locations.

Example business case: a researcher having a signed agreement to protect data provided by the FBI that can only be located on one specialty device with specific restrictions.

Each client will have a file storage limit managed by a quota. Departments can request quota increases at cost for clients with an approved business case. Technical consultation may be required to help determine use of the data storage and provide alternate solutions.

Shared File Folder Request

Clients are able to request a shared file folder on UCF IT managed network storage in order to share files with other NID authenticated users. Clients must provide the following information in their request to UCF IT:

- First and last name
- NID
- Email address
- Phone number
- Supervisor name, supervisor email, and supervisor phone number
- Designated owners of the shared file folder (Minimum 2)
- Data type (Unrestricted, Restricted, or Highly Restricted)

- Business case
- List of clients who need access
- Timeframe share is requested

Once the request is received, UCF IT will provide a technical consultation to determine if a shared file folder is the best solution for the business case. Once a shared file folder has been determined to be the best solution, approval will be required from the unit. During the approval process, a quota will be established for the shared file folder.

Only designated owners are permitted to request a change in client access to the shared file folder. In order to maintain security, every year the shared file folder will require review and verification of client access by the owners. Client owners are responsible for submitting a change request to remove access for clients on the access list. Unit leadership can request shared file folder ownership changes.

Data Encryption

Encryption is required for all University owned equipment capable of encryption. UCF IT will only maintain storage of encryption keys for all equipment encrypted by UCF IT. UCF IT is not responsible for encryption keys on devices encrypted by non UCF IT personnel.

Device Level Backup

Device level backups are not performed on a regular schedule. A device level backup may be performed on University owned equipment as needed within certain IT workflows. Examples include OS refresh, OS upgrade, encryption, etc. Client is able to decline the device level backup with documented communication indicating an understanding of the associated risks.

Clients wishing to backup local desktop data can reqest a Technology Consultion to review options.

Data Recovery

UCF IT cannot guarantee recovery of data or verify file contents recovered. In the event of file data loss, occurring on University owned equipment, UCF IT may use recovery tools at its discretion to diagnose the incident. UCF IT will attempt to recover data if warranted by diagnostics. In cases that require advanced data recovery, UCF IT will provide recommendations for 3rd party data recovery services that will diagnose and attempt recovery of data at a cost to the client.

Research Data Storage

UCF IT recommends that all research data be stored on University owned and managed data storage solutions. Examples include UCF IT file servers, OneDrive for Business, etc.

Clients with business cases that can not be met by available University owned and managed data storage solutions can request a Technology Consultion to review options which may include on-premise and cloud storage solutions at additional cost to the client.

Computer Access

Access to sign into Public areas that require access for all NID authenticated users may be set up with an approved business case. Examples include public computer labs, classrooms, conference rooms, etc.

Access to sign into other managed University owned devices will be restricted to department / unit level. This will include managed University owned devices located in offices, research labs, staff areas, mobile devices, etc. Owners of the device will need to approve access for new clients. Authorized UCF IT personnel will require access to all supported devices.

Limited access guest accounts may be provided with an approved business case for non-NID authenticated users to use a public computer lab or space. Examples include departments hosting summer camps, outside organizations hosted by the university, etc. Existing UCF client will need to provide the following information:

- First and last name
- NID
- Email address
- Phone number
- Supervisor name, supervisor email, and supervisor phone number
- Designated reserved public location
- Business case
- Guest contact information
- Defined start and end date of access needed

The approved guest account will only be available in the designated reserved public location space during the defined start and end date.

Service or kiosk accounts will only be provided with an approved business case. Examples include sign in stations, print kiosks, etc. Client requesting the account will need to provide the following information on the request:

- First and last name
- NID
- Email address

- Phone number
- Supervisor name, supervisor email, and supervisor phone number
- Business case
- Timeframe account is requested
- Devices for which access is requested

Once the request is received, UCF IT will provide technical consultation to confirm the service or kiosk account is the best solution to the business case provided. Service or kiosk accounts will require yearly review to determine if they are still needed to fulfill the business case.

Remote Access

UCF IT will provide remote access to clients who need to access their dedicated, managed, UCF-owned device directly connected to the wired network. Client must request that remote access be setup for the device. Student employees must receive supervisor approval before access is granted. Anyone requesting access to a shared system must receive supervisor approval before access is granted. Remote access is provided per user per device. Clients who need access to multiple devices will need to request access to each device. Client requesting remote access will need to provide the following information:

- First and last name
- NID
- Email address
- Phone number
- Supervisor name, supervisor email, and supervisor phone number (If applicable)
- Device for which access is requested

Personal File Storage Exceptions

Client may request personal, network-attached, external file storage for approved business cases. Examples may include research data that is not able to be stored on UCF IT owned and managed network storage due to a specific business case. Network attached external file storage must be managed by UCF IT and be encrypted. Device must remain on UCF owned or leased property. The network attached storage device must be registered with UCF IT to obtain network access.

Unmanaged, University-owned, directly attached, external file storage devices (non-network) must be encrypted. Clients who possess unmanaged, University-owned file storage devices are solely responsible for the management and protection of the device.

Cloud Storage

UCF IT clients can store University data only on UCF approved cloud storage solutions in compliance with university policy 4-014. http://policies.ucf.edu

Current UCF approved cloud file storage solutions:

- UCF IT Office 365 OneDrive for Business
    - Approved for Restricted Data as defined by UCF policy 4-008.1. http://policies.ucf.edu

Current UCF approved endpoint file backup solutions:

- UCF IT provided CrashPlan Pro Enterprise licenses
    - Approved for Highly Restricted Data & Restricted Data as defined by UCF policy 4-008.1. http://policies.ucf.edu

UCF IT will only install software clients from the approved lists on University owned devices. Request to use other cloud storage providers will need to be submitted to UCF IT for review. Clients who request to install other cloud storage solutions will be provided a technical consultation to attempt to use the approved cloud storage solutions. If none of the approved solutions will meet the need of the business case of the client, UCF IT will communicate the request to the business relationship manager (BRM) of the department. The BRM will work with the client and UCF IT to determine if the request should be submitted. If the cloud storage provider is approved through the review process, the provider would be added to the approved list.

UCF IT will block installation of other cloud storage clients not part of the approved list on University owned managed devices.

PRINT & SCAN ACCESS

Network Printing

UCF IT will setup University-owned network printers (no wireless devices) purchased from the UCF IT catalog for centralized printing. All printers connected to the network will only receive their print jobs from a UCF IT managed print server. UCF IT is not responsible for managing print volume and quotas. This includes providing access codes and evaluation of print volume.

Clients are not allowed to share printers directly attached to their computer with other users on the network.

Scan to File or Email

University owned multifunction devices and network scanners from the UCF IT product catalog can be setup to scan to file share or email addresses as long as they meet the minimum-security requirements set by the information security office (ISO). Requests to configure devices will receive a technical consultation to determine the best option to fulfill the business case. Device owner will be responsible for management of the email address list.

UCF IT prefers that all scanning devices send jobs to a centralized managed scan server application.

NETWORK ACCESS

All devices that require wired network access regardless of ownership must be registered with UCF IT in order to gain access to the UCF wired network.

With an approved business case UCF IT may setup specific areas that do not require registration for wired access. Examples of this may include open public learning spaces and study areas. Business case would need to be approved and coordinated with network services, information security office (ISO), and the Support Center.

x. REFERENCES AND ADDITIONAL CONSIDERATIONS

UCF IT PRODUCT CATALOG

The latest version of the UCF IT Product Catalog can be located at this link: http://cstore.ucf.edu/departmental/ucf-it-product-catalog.html

UCF IT SERVICE CATALOG

The latest version of the UCF IT Service Catalog can be located at this link: http://it.ucf.edu/our-services/service-catalog/

ADDITIONAL CONSIDERATIONS

Support Audience Exceptions

The following Audiences may require support beyond our support and lifecycle standards that should be provided by staff with specialized training and/or in a specified method. The support level may need to be reviewed on a case-by-case basis.

Research	University / Grant Funded Research Data. How a device is classified as research will need to be defined.
FERPA	Student Data
HIPAA	Medical Data

CJIS	Criminal Justice Data
PCI	Financial Data
ADA	Specialty Use
NIST	Security Compliance Framework
D.O.D	Department of Defense

Platform Specific Considerations

Linux Distributions	Applications available by currently vetted repository can be eligible for installation after evaluation by UCF IT.