Asset Management Policy

Document Number: ITS-0024 **Date Published(sys):** 4/27/2022

General Description

Policy Summary:

Trinity University is committed to a secure information technology environment in support of its mission[1]. Within this Policy, the terms “Trinity University” & “Trinity” may be used interchangeably.

This policy provides a framework for managing the receiving, intake, distribution, and recovery of technology goods and encompasses the processing requirements.

The Asset Management Policy is aligned and complements the University *BUSO-0031 Purchasing Policy and Procedures*, the *ITS-0044 Technology Acquisition Procedure, the FACS-0002 Central Receiving Policy* and other related procedures.

[1] https://www.trinity.edu/about/mission-values

Purpose:

The purpose of this policy is to define standards, procedures, and restrictions for the management of technology assets such as all IT hardware, software, and computer-related components purchased with University funds. This policy is designed to provide Trinity with a documented and formalized process regarding technology asset management done by the University.

Additionally, compliance with the stated policy and supporting procedures helps ensure the confidentiality, integrity, and availability (CIA) of the University system components.

Scope:

This policy applies to all full-time and part-time employees and to the purchase of all equipment issued by the University regardless of University funding sources. The scope of this policy includes, but is not limited to, the following technology resources:

- Desktops, laptops, tablets, and servers
- Software running on the devices mentioned above

- Peripheral equipment, such as printers and scanners
- Cables or connectivity-related devices
- Audio-visual equipment, such as projectors and cameras

Exceptions:

In few instances, Trinity systems may require to be exempted from the Asset Management Processes due to possible technical difficulties or third-party contractual obligations. Any such exceptions to the current policy must be documented and approved via the Trinity's Exceptions Management Process.

Policy Content

① Roles and Responsibilities

Implementing and adhering to organizational policies and procedures is a collaborative effort, requiring a true commitment from all personnel, including management, internal employees, and users of system components, along with vendors, contractors, and other relevant third parties. Additionally, by being aware of one's roles and responsibilities as it pertains to the University information systems, all relevant parties are helping promote the Confidentiality, Integrity, and Availability (CIA) principles for information security in today's world of growing cybersecurity challenges.

ROLES	RESPONSIBILITIES
Management Commitment	Responsibilities include providing overall direction, guidance, leadership, and support for the entire information systems environment, while also assisting other applicable personnel in their day-to-day operations. The Chief Information Officer CIO is to report to other members of senior management on a regular basis regarding all aspects of the organization's information systems posture.
Internal Employees, Academic Community and Users	Responsibilities include adhering to the University's information security policies, procedures, practices, and not undertaking any measure to alter such standards on any University system components. Additionally, end users are to report instances of non-compliance to senior authorities, specifically those by other users. End users – while undertaking day-to-day operations – may also notice issues that could impede the safety and security of the University system components and are to also report such instance immediately to senior authorities.
Vendors, Contractors, Workforce	Responsibilities for such individuals and organizations are much like those stated for end users: adhering to the

	organization's information security policies, procedures, practices, and not undertaking any measure to alter such standards on any such system components.
ITS Business Affairs Unit	Responsible for the Software Acquisition / Procurement process. They keep the Software License Inventory Log.
ITS CORE Infrastructure Team	Support the product vetting as well as the network & security software provisioning process. Owns the implementation of networking and security software.
ITS Enterprise Applications Team	Support the new applications vetting as well as the major applications provisioning process. Owns the support of business-related applications and the implementation of CORE systems.
ITS Technical Support Services	TSS supports the users with the installation of software for the workstations, mobile devices, audio visual equipment and other equipment

② Policy

Trinity is to ensure that all applicable users adhere to the following policy for purposes of complying with the mandated University requirements set forth and approved by management.

All hardware, software, or components purchased with University funds are the property of Trinity University. This also includes all items purchased using any requestor's Department P-Card and any other Department P-Card, including ITS.

A personal computer may contain a data storage device on which personal, confidential, and legally protected information is stored. To prevent unauthorized access to sensitive data, identity theft, and liability, the University is committed to ensuring that devices on personal computers are properly recycled and stored data is unrecoverable.

New Technology Acquisition / Purchases for the University

All computer equipment purchases must be coordinated with the Information Technology Services or ITS before any purchases are made.
All requests should go through the ITSupport@trinity.edu email if asking for the purchase of new equipment.

Standard receiving from TU Central Receiving to the ITS Stockroom

1. Warehouse receiving is not simply a matter of purchasing inventory and having it delivered to the ITS Stockroom or TU Central Receiving

Warehouse; rather, it involves several key steps that must be done right to ensure the right items and correct quantity are being delivered and stored correctly. There are 4 major steps that had to be followed to ensure appropriate receiving of technology goods:

1. Ensure proper documentation and approvals are complete and in order:
    1. Before inventory is delivered, the ITS Business Affairs organization have gathered the complete documentation, approved by all parties, and have sent all the documentation electronically to the Procurement Office.
        1. Full technology acquisition / purchasing process is described in the *ITS-0044 Technology Acquisition procedure*.
2. Receive and unload stock:
    1. TU Central Receiving Warehouse staff meets the shipper at a loading dock and unload the necessary cargo. The ITS Receiving staff should also be standing by to bring their questions or concerns regarding the shipment with the delivery driver and TU Central Receiving personnel.
3. Count and Confirm inventory:
    1. As the cargo is being unloaded, the TU Central Receiving Warehouse staff checks the contents of each delivery, including the quantity, the integrity of seals, the product codes / SKUs, and the overall condition of the cargo to ensure that what's in the boxes matches what is listed on the receiving sheet and is expected to arrive.
    2. TU Central Receiving Warehouse staff counts boxes or pallets, rather than individual items.
        1. It is the responsibility of the ITS receiving personnel to ensure that what is being received is what was ordered.
4. Organizing and Storing products:
    1. Once all inventory is unloaded and inspected, the final step in the warehouse receiving process is organizing and storing new inventory in the warehouse.

University Surplus Property

Information Technology Services ITS is responsible for collecting personal computers from departments because of computer replacements. The University contracts with an external electronic recycling company to provide a certificate of destruction.

Data Storage Device Assets

All Trinity-owned computers will be wiped of university software and restored to default factory settings when returned for recycling or redistribution.

Media Storage, Distribution and Classification

Securing media, wherever it may physically be located, is an essential function for helping ensure the safety and security of critical University data.
Trinity is to ensure that all applicable users adhere to the following policies for purposes of complying with the mandated organizational security requirements set forth and approved by management:

- Controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes) are to be in place for protecting University data.
- Media backups are to be stored in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.
- All media is to be appropriately classified so the sensitivity of the data can be.
- All media is to be sent by secured courier or other delivery method, so that it can be accurately tracked.
- Management is to approve any and all media that is moved from a secured area (including when media is distributed to individuals).
- Strict control is to be maintained over the storage and accessibility of media.
- Inventory logs of all media are to be maintained, with media inventory procedures undertaken at least annually.

Storage Facility for Media Backups

All media stored at an offsite location is to have the following minimum physical and environmental security controls and safeguards in place:

- A facility with a valid Certificate of Occupancy (CO) issued.
- Stored in an isolated room or area that is not shared with another client of the offsite location facility.
- Access granted by traditional lock and key and/or electronic access control systems (ACS).
- 24x7 security monitoring, either by an alarm system or security guard.
- Handicap-accessible.
- Adequate lighting at night.

- Appropriate maintenance of grounds and landscaping so as to prevent intruders from concealing themselves.
- Appropriate fire monitoring, detection, and suppression controls.
- Appropriate water monitoring and detection controls.

The procedures for ensuring these controls and safeguards are in place require one to routinely request a tour of the facility and to ask for any compliance audits conducted on the offsite location by a third-party auditor. Additionally, any hardcopy and electronic media kept in a storage repository will be protected by encryption for media containing data information, thus allowing only authorized personnel to decrypt media as needed.
Data backup process is described in the *ITS-0038 Backup Strategy Procedure*.

Classification of Media and Information Assets

University Management and other authorized personnel are responsible for classifying media and information assets to ensure they are all adequately protected. The University has adopted the following media classification scheme:

- Public Information
- Protected Information
- Restricted Information

University Data that is classified as Public may be disclosed to any person regardless of their affiliation with the University. All other University Data is considered Sensitive Information and must be protected appropriately. Important to understand that for documents or data types that are not explicitly addressed within the *ITS-0013 Information Security Policy*, each Trinity University department should classify by considering the potential for harm to individuals or the University in the event of unintended disclosure, modification, or loss.

Management Approval for moving media from locations

Only ITS personnel approved by the CIO, or the CORE Infrastructure Manager are allowed to make changes – and ultimately approve – any movement of media to and from locations, and any other issues pertaining to media storage.

Specifically, only the authorized personnel may send, retrieve, and receive media from the offsite location and from other entities such as third-party vendors, clients, or governmental bodies (local, federal, and state). The

procedure for gaining permission to send, retrieve and receive media calls for one to submit a request to be added to the media distribution list, which will be reviewed by management or personnel authorized to grant this approval.

Software Licensing as an Asset

Software license management is a key process for the University. It involves keeping an inventory of all purchased software licenses and lining that inventory up with deployed software installations.

The software license management process doesn't work in a vacuum. It mainly interfaces with the asset management process. Under asset management, the University knows who is using what machine, whether the machine is under warranty or not and other necessary details like the software licensees installed on the machine.

Baseline activity

ITS owns the Software License Management process for Trinity.

- The ITS Business Affairs Unit owns the Software Acquisition / Procurement process, and the ITS technical groups support the product vetting as well as the software provisioning process.
- The ITS Business Affairs Unit also keeps the Software License Inventory Log updated.

The ITS Business Affairs Unit works with TSS and the other ITS Technology Managers to:

- Get up today KACE System report of Software license inventory (available or installed).
- Validate that the number of application installations, with either named or limited licensees, do not exceed the number of purchased / owned licensees.
- Check the usage status of the software licenses to make sure that the number of software licenses is optimal and there is no violation or surplus.
- Validate the total number of existing licenses and remaining licenses for each managed software
- Ensure that the application owner resolves any Software License violation by taking an appropriate action, such as requiring the

application owner to purchase additional software licenses or asking them to remove unused licensees from users.

Once the ITS Business Affairs Unit completes the purchase of the software license, the Supplier / Manufacturer will send the software installation instructions package to them and they will proceed to submit it to the ITS Manager of Technical Support & Client Services, within the original ticket created, for appropriate action and next steps.
The ITS Manager of Technical Support & Client Services is responsible to register the software license and managed-software information into the KACE Asset Management Module, as described in the *ITS-0037 Asset Receiving Procedure – Receiving new Software License into KACE system*.
The ITS Manager of Technical Support & Client Services will also:

- Assign the software installation ticket to the technicians after validating license availability.
- Make purchase request for additional licensees.
- Check whether Trinity has any surplus licenses. If it does, will assign the surplus licenses to the appropriate computers to maximize the license usage.
- Take inventory of software licenses.
- Discard software licenses. Will collect the software that is no longer in use from workplaces, to discard it following the appropriate / approved Asset Disposition process.

Performing Physical Inventory Count

The ITS Business Affairs Unit, at least once a year, will request the ITS TSS organization, through their Client Experience Director, to perform a software licensing physical inventory. To perform a physical inventory count of the software licenses, the ITS Business Affairs Unit will get a list of software license information to check the software licenses against the list.

1. ITS TSS will export a list of software license information from KACE / K1000.
    a. Create a list of software license information for physical inventory count.
    b. Export the software license information including the License number, Last Tracked Date, License Name, Total Licenses, and License Type.
2. Perform a physical inventory count based on the list of software license information.
    a. ITS TSS, with support from the ITS Business Affairs Unit, will check the Media and software license certificate (Purchase and sale contract)

b. ITS TSS, with support from the ITS Business Affairs Unit, will check the software license certificates and the software media against the list of software license information to make sure that the software licenses exist.

Limiting access for Installing Software

Users will have limited privileges as we need to ensure software compliance for the University.

1. University ITS users will not have admin or super user privileges. Exceptions will be approved in advanced by the University CIO after justified by the user's organization.
2. ITS will provide an alternate plan in mind for maintaining stakeholders' productivity, where the Stakeholder will contact the ITS Technical Support Services team – Client Experience. All requests should go through the ITSupport@trinity.edu email.

Asset Rationalization

Asset rationalization is the process of reorganizing Trinity assets to improve its operating efficiencies and boost its bottom line while disposing of those that are no longer fit for purpose.
Asset Rationalization involves:

- Retiring unused assets
- Eliminating assets with redundant functionality
- Validating the value of assets' investment
- Standardizing on common asset vendors
- Creating synergy within the asset's ecosystem
- Targeting university goals with the asset's portfolio

By doing so, ITS ensures scale, vitality, and adaptability of its IT landscape. The benefits from assets rationalization are many.

- Reduced ITS costs:
  - licenses, maintenance, integration, training, vendor management.
- Reduced ITS complexity:
  - less integrations, less dependencies, less change impact, less things to worry about when you need to decide on an application fast.
- Reduce ITS risks:
  - fewer vulnerable elements.

ITS Business Affairs Unit will define the Metrics and Key Performance Indicators, to monitor suppliers' performance based on spending, products/services availability, and participation on University business. This information will help the CIO recommend reducing the technology supplier's landscape and be able to reduce

costs through effective negotiations. Will also help consolidating services or technology acquisition through limited number of Suppliers.

Asset Categorization

An important element while doing Asset rationalization is having the assets divided into categories. It is expected from the team of technicians responsible to enter the assets in KACE to follow the established and agreed asset's categories defined in the system.
Assets are categorized and the fields for each type are build out in KACE to follow the format as described on the *ITS-0037 Asset Receiving Procedure.* The following categories were defined in KACE including the models approved by ITS or in use (when applies) and the asset field description;

1. Audio Visual Equipment
2. Computers

NOTE: Warranty Information is automatically populated for Dell devices in the inventory record

3. Docking Station
4. Monitors
5. Network Equipment
6. Peripherals
7. UPS
8. Tablet models

Hardware Replacement

Equipment replaced during any period shall be based on a minimum annual review of the asset management program and hardware replenishment schedule, hardware inventory, and fixed asset budget schedules.

Computers

Computers that are part of the ITS computer replacement cycle will be replaced with a new standard computer 5 years from its Purchase date. Standard model / brand as well as its configuration will be defined and approved by the ITS Organization. Refer to the *ITS-0008 Technology Acquisition Policy* for more information.

Performance Evaluation

Consequences of Policy Violation:

Any behavior in violation of this policy is cause for disciplinary action and violations of this policy may result in, but are not limited to, any or all the following:

- Loss of university computing, email and/or voice mail privileges.
- Disconnection from the residential hall internet network.
- University judicial sanctions as prescribed by the student code of conduct.
- Reassignment or removal from university housing and/or suspension or expulsion from the university.
- Prosecution under applicable civil or criminal laws.

Violations will be adjudicated, as appropriate, by the CIO, the Office of the Dean of Students, the Office of Housing and Residential Life, and/or the Human Resources Office.

Terms & Definitions

Terms and Definitions:

Term:	Definition:
Commodities	Supplies, materials, equipment, furniture, contractual services, and any other goods required by the University.
Contract	Legal agreement between Trinity University and a vendor or supplier
Emergency	An unexpected situation or sudden occurrence of a serious and urgent nature that demands immediate action, otherwise, it would endanger life, property or adversely affect essential University operations.
Invoice	An itemized bill for goods purchased or services contracted, containing individual prices, the total charge and payment terms.
Media in Electronic Format	Electronic media are the bits and bytes contained in hard drives, Random Access Memory (RAM), Read-Only Memory (ROM), disks, memory devices, phones, mobile computing devices, networking equipment and various others
Media in Hardcopy Format	Hardcopy media are physical representations of information. Paper printouts, printer and facsimile ribbons, drums and platens are all examples of hardcopy media
Non-Public Information	Non-Public Information includes both Protected and Restricted Information.
OPEX	Operating Expenditure
Packing or Delivery Slip	Proof of delivery from vendor

Term:	Definition:
Performance Specification	Based upon the specific needs. Total ownership cost for operating and maintaining the product should be included as an element of the specification.
Protected Information	Protected information includes all private data, records, documents, or files that contain information that is not to be shared publicly but also not restricted legally and might be provided upon reasonable request as long as the Data Owner is consulted about its responsible use and approves its release. Trinity employees must protect Trinity business-related data, whether on a Trinity-issued device or on a personal device used for business purposes and delete or preserve Trinity data as required. Employees must wipe Trinity data from their phones (personal or Trinity-issued) when they are no longer actively using that data for their current Trinity role, e.g., when they leave the University, switch devices, give their phones away, turn in phones to Verizon/AT&T, etc. If a phone (personal or Trinity-issued) that contains Trinity data (including email) is lost or stolen, the owner must immediately notify the Helpdesk so that the device can be remotely wiped if university-owned or wiped by an employee if personally owned. Department Chairs or equivalent officers are responsible for ensuring that local units abide by this policy.
Public Information	Information that the University has made available or published for the explicit use of the general public with no restrictions on access, use, or disclosure under University policy or contract, or local, national, or international statute, regulation, or law.
Purchase	Acquiring a commodity in exchange of money or other valuable consideration. The basic types of purchases that can be made may include but are not limited to: • The purchase of commodities or services on a one-time basis each year. • The direct purchase of commodity or service that is available from only one source. • Contracts used to obtain commodities or specific professional, technical, or other specialized services throughout the year.
Purchase Order	Form, generated by the Procurement unit that documents the purchase agreement or contract.
Quotation	An official document received from vendors that includes prices, availability of requested goods, payment, and delivery terms.
Requestor or	Person that is requesting the contracting or purchase of a commodity

Term:	Definition:
Requesting Party	
Restricted Information	Sensitive information that must be safeguarded at the highest priority levels in order to protect the privacy of individuals and the security and integrity of University systems. This information must be limited to authorized University faculty, staff, students, or others with a legitimate need. This information may not be transferred without mandatory security precautions or made vulnerable to unauthorized access, use, or disclosure. Restricted information is categorized as such due to legal protection or privilege, University policy, contract obligation, or important privacy considerations. Restricted Information includes but is not limited to “Sensitive Personal Information” as defined by Texas S.B. 122 § 48.002.2 (Identity Theft Enforcement & Protection Act).
Specification	A concise statement explaining the type of product or service, the quality level, special requirements in design, performance, delivery, and usage. Specifications must not be restrictive (locking in a specific vendor and limiting competition) or be vague (allowing a vendor to provide a lower than acceptable quality level product or service).
Vendor	Any supplier who has business with Trinity University.

Related Documents

Related Content:

The *ITS Asset Management Policy* is aligned with ISO 20400 Sustainable Procurement Guidance and with applicable laws and regulations.

Revision Management

Revision History Log:

Revision #:	Date:	Recorded By:
v2.0	4/27/2022 11:29 AM	Ben Lim
v1.0	2/1/2022 1:16 PM	Dan Carson

Vice President Approval:

Name:	Title:
Ben Lim	Chief Information Officer