Decentralized IT Asset Purchases

Audit Report # 22-102
February 14, 2024

The University of Texas at El Paso

Office of Auditing and Consulting

"Committed to Service, Independence, and Quality"

The University of Texas at El Paso
Office of Auditing and Consulting Services

500 West University Ave.
El Paso, Texas 79968
915-747-5191
WWW.UTEP.EDU

February 14, 2024

Dr. Heather Wilson
President, The University of Texas at El Paso
Administration Building, Suite 500
El Paso, Texas 79968

Dear Dr. Wilson:

The Office of Auditing and Consulting Services has completed a limited-scope audit of *Decentralized IT Asset Purchases.* During the audit, we identified opportunities for improvement and offered the corresponding recommendations in the audit report. The recommendations are intended to assist the departments in strengthening controls and help ensure that the University's mission, goals, and objectives are achieved.

We appreciate the cooperation and assistance provided by the Office of the Vice President for Business Affairs, Purchasing, Contracts and Grants, and Information Resources staff during our audit.

Sincerely,

Courtney H. Rios

Courtney H. Rios
Interim Chief Audit Executive

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Background

The University is responsible for maintaining accurate, complete inventory records for all capital and controlled assets, including IT assets. The use of decentralized purchasing methods to acquire IT assets poses a risk to the University, as these items may circumvent inventory tagging and necessary information security protections.

Audit Objectives

The objectives of this audit include:

- Determine compliance with the University's IT asset purchasing guidelines to ensure purchases are compatible with the network, supported by Information Resources, and do not expose the University to weaknesses.
- Determine if the University's IT asset inventory is complete and accurate for IT assets that meet the controlled and capital asset thresholds.

Scope

The scope of the audit includes information technology resources (laptops, desktops, servers, peripherals, and network hardware) as well as software, regardless of cost, acquired through decentralized purchasing methods (expense reimbursements, Pro Cards, and non-PO vouchers) from September 1, 2021, through February 28, 2023. Miner Mall purchases are excluded from the audit scope as a Miner Mall Audit is scheduled in the Fiscal Year 2024 Audit Plan.

Strengths

The Disbursement Services staff and the Pro Card Administrator encourage departments to contact the Inventory Department to tag decentralized IT asset purchases. In addition, the Inventory Department contacts departments directly when notified about an untagged controlled or capital asset. The University has a procurement system in place (Miner Mall) that involves the requisitioner department, Purchasing, Inventory, and General Accounting. If the departments follow Miner Mall procedures, inventory records should be properly updated at the end of the cycle.

Summary of Audit Results

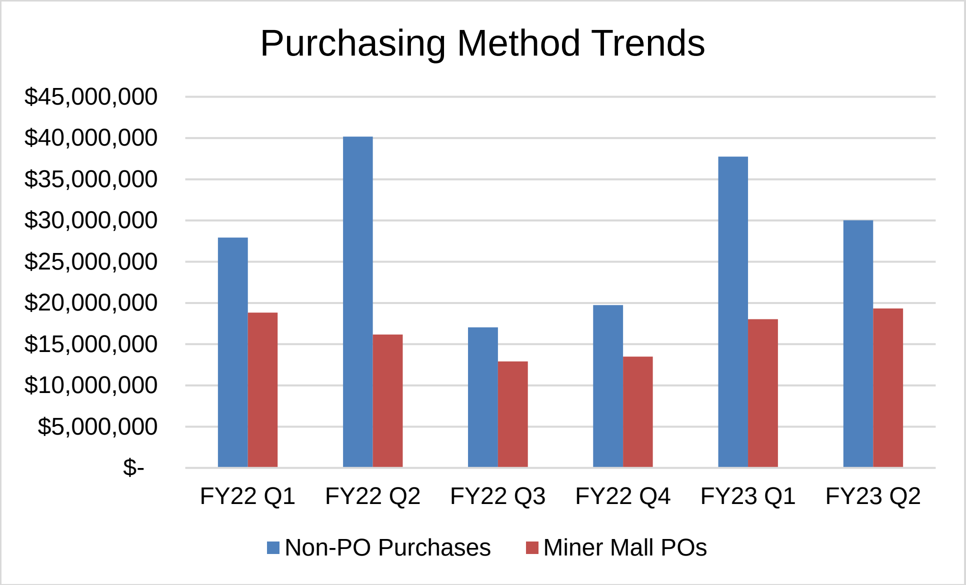
Issue	Risk Ranking
1. Departments do not follow procedures for receiving and tagging decentralized IT asset purchases.	High
2. IT assets are often classified under incorrect expense accounts.	Medium
3. IT assets that pose a medium to high-security risk are purchased via decentralized methods.	High

Conclusion

Based on the results of audit procedures performed, we conclude that departments are not following established state, UT System, and UTEP rules and policies when they purchase IT assets using decentralized methods. Noncompliance with established policies may expose the University to business and cybersecurity risks, as these assets may circumvent inventory tagging and necessary information security protections.

BACKGROUND

The percentage of non-PO purchases is consistently higher than purchases made through Miner Mall, as shown in the chart below. Non-PO purchases include employee expense reimbursements, Pro Card purchases, and other non-PO vouchers. The chart includes all University purchases in Fiscal Year (FY) 2022 and the first two quarters of FY 2023, which includes IT asset purchases.



Source: Disbursement Services Dashboard

Texas Government Code §403.2715(c) states the requirements UT System institutions must follow for property management:

"*A university system or institution of higher education shall account for all personal property as defined by the Comptroller under Section 403.272. At all times, the property records of a university system or institution of higher education must accurately reflect the personal property possessed by the system or institution."*

UTS 165 Information Resources Use and Security Policy outlines Standards regarding the use and safeguarding of institutional IT assets.

The audit was conducted in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing* and *Generally Accepted Government Auditing Standards*.

AUDIT RESULTS

A. Inventory Records and Classification

1. Departments do not follow procedures for receiving and tagging decentralized IT asset purchases.	**High Risk**

Per Texas Government Code §403.2715(c), the University is responsible for maintaining accurate, complete inventory records for all capital and controlled assets, including IT assets. The use of decentralized purchasing methods to acquire IT assets, such as employee expense reimbursements, Pro Card purchases, and non-PO vouchers, poses a risk to the University, as these items may circumvent inventory tagging and necessary information security protections. In addition, there is no current requirement to tag the item before reimbursement.

Auditors tested 19 IT asset purchases that required inventory tagging. Only two of the 19 IT assets were tagged before the audit, even though the Inventory Department, Purchasing, and Disbursement Services remind departments of tagging requirements.

Non-PO Purchase Sample	Number of IT Assets
Tagged controlled IT assets	2
Untagged controlled IT assets	3
Controlled IT assets tagged after the fact	14

Controls are not in place to ensure that departments are following HOP Section 7 Chapter 3 tagging requirements. *"All new institutional property with a value of $500 or more will be tagged with a UTEP property tag, assigned an inventory number and placed on the official inventory records maintained by the Office of Institutional Property Management."*

Recommendation:

Management should consider potential solutions to mitigate the risk of decentralized IT asset purchases not being recorded in the University inventory records and not having the necessary information security protections.

Management Response:

Disbursement Services will collaborate with Purchasing, Inventory, and Information Resources to review current policies and update them as needed. The policy is currently included in the Purchasing Manual. In the interim, Disbursement Services will implement a process that passes the information to the Inventory Department to ensure the tag is issued and upon notification, will issue payment as appropriate.

Responsible Party:

Ms. Danielle Martinez, Director, Disbursement and Travel Services

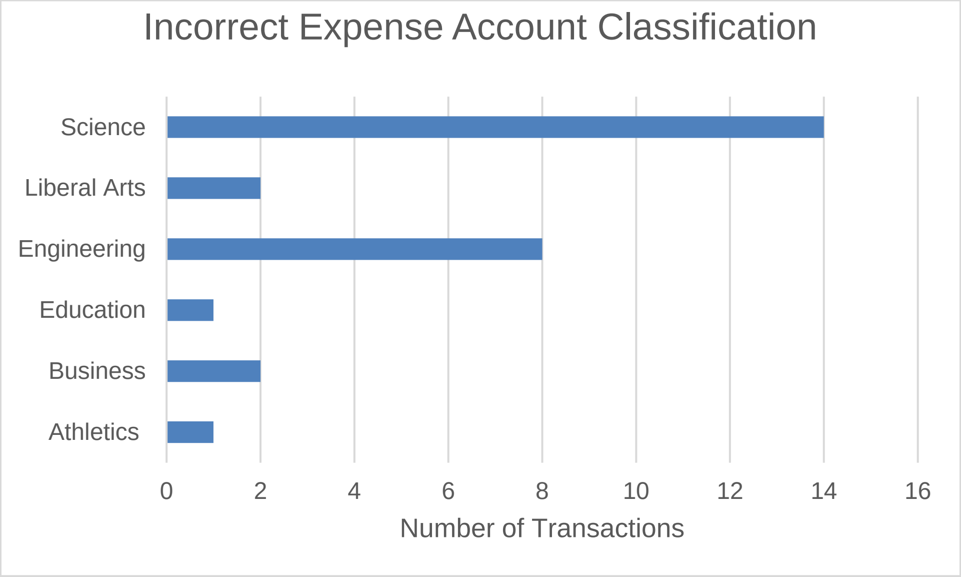
Implementation Date:

August 31, 2024

2. IT assets are often classified under incorrect expense accounts.	Medium Risk

When making a decentralized IT asset purchase, departments are required to select an expense account for the transaction in PeopleSoft. This process is subject to error and can lead to incorrect accounting and inventory records.

Of the 40 expense reimbursements tested, 24 items were classified under the incorrect expense account. Of the four non-PO vouchers tested, two were classified under the incorrect expense account. For example, a laptop purchased was classified under the Office Supplies expense account, a data projector was classified under Hardware & Materials, and an iPad was classified under Consumable Non-Office Supplies.



Recommendation:

Additional training or online guidance should be provided to departments campuswide to ensure that decentralized IT asset purchases are correctly classified.

Disbursement Services should continue reviewing the expense accounts selected by departments for decentralized IT asset purchases and sending them back for revision if necessary.

Management Response:

The General Accounting Office will provide additional training to Department Managers and Administrative Staff on how to properly classify their IT and other purchases. In addition, General Accounting will work with Disbursement Services to provide training on expense accounts related to decentralized IT purchases and returning documents needing revision.

Responsible Party:

Dr. Daniel Domínguez, Director, Accounting and Financial Reporting
Ms. Danielle Martinez, Director, Disbursement and Travel Services

Implementation Date:

February 28, 2024

B. Governance and Information Security Risks

3. IT assets that pose a medium to high-security risk are purchased via decentralized methods.	High Risk

IT assets such as Raspberry Pis (credit card size computers), laptops, tablets, computers, and cloud storage services are purchased via decentralized methods. The following table summarizes the testing conducted by purchasing method (regardless of cost) and IT asset category such as high or medium security risk. Security risks were assigned based on auditor judgment, assessing high-security risks to IT assets that store data and can connect to the internet and/or University network. Medium security risks were assessed to IT assets that meet at least one of the high-security risk parameters, but not all.

Security Assessment of Possible IT Asset Transactions*			
	Employee Reimbursements	**Pro Cards**	**Non-PO Vouchers**
High-Security Risk**	94	21	2
Medium Security Risk***	41	16	0

* Results may not be complete as items might have been misclassified to incorrect expense accounts.

** Includes Computers, laptops, tablets, Raspberry Pis, cloud storage services, MS 365 subscription, mobile devices, etc.

*** Includes Wi-Fi adapters, portable storage, cloud and non-cloud software, etc.

See **Exhibit A: IT Asset Security Risks**.

Computers purchased through centralized methods (Miner Mall) come preconfigured with the standard University image, including information security tools and applications. The same cannot be said for computers purchased through decentralized methods. Even if never connected to the University network, these computers still pose a security risk as confidential data may be breached and go undetected for an extended period. The same security risk applies to intangible IT assets like third-party cloud storage services, which may not be configured consistent with University security requirements.

IT asset management and related information security controls are addressed across multiple State, UT System, and UTEP policies. Per comparison of related policies, auditors noted they have gaps, are not clear, and some are more lenient while others are more restrictive. The current environment creates confusion and opportunities for individuals making decentralized IT asset purchases as well as departments trying to hold the line from both a business and information security perspective. See **Exhibit B: Policy Comparison Matrix**.

Recommendation:

The Purchasing Department's Operating Procedures (Purchasing Manual) includes a section that covers computer acquisitions, the importance of purchasing IT assets from the pre-approved listing (Miner Mall), standard configurations as well as exceptions to the policy and required IT approvals. Information Resources should provide guidance to Purchasing to update this section of the Purchasing Manual to better reflect current IT asset technologies and emerging risks. Then, on a going-forward basis, it should be reviewed and updated for changing technologies and trends, as well as business needs.

Management Response:

Purchasing will work with Information Resources to update Section 25: Computer Acquisitions of the Purchasing Manual and will establish a process for ongoing periodic reviews.

Responsible Party:

Dr. Diane De Hoyos, Associate Vice President, Purchasing and General Services
Mr. Luis Hernandez, Vice President for Information Resources

Implementation Date:

June 30, 2024

Other Recommendations to Consider (No Management Response Required)

Management should consider current emerging security risks and determine whether certain IT assets under the current required $500 threshold, like computers, laptops, tablets, and Raspberry Pis, should be tagged and tracked accordingly as these assets expose the University to similar cybersecurity risks as assets above those thresholds.

RANKING CRITERIA

Priority	An issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.
High	A finding identified by internal audit considered to have a medium to high probability of adverse effects to the UT institution either as a whole or to a significant college/school/unit level.
Medium	A finding identified by internal audit considered to have a low to medium probability of adverse effects to the UT institution either as a whole or to a college/school/unit level.
Low	A finding identified by internal audit considered to have minimal probability of adverse effects to the UT institution either as a whole or to a college/school/unit level.

Report Distribution:

University of Texas at El Paso:

Ms. Andrea Cortinas, Vice President and Chief of Staff
Mr. Luis Hernandez, Vice President for Information Resources
Dr. Ahmad M. Itani, Vice President for Research
Mr. Mark McGurk, Vice President for Business Affairs
Dr. Diane De Hoyos, Associate Vice President, Purchasing and General Services
Mr. Gerard Cochrane, Associate Vice President, Chief Information Security Officer
Mr. Charlie Martinez, Assistant Vice President/Comptroller
Dr. Daniel Dominguez, Director, Accounting and Financial Reporting
Ms. Danielle Martinez, Director, Disbursement and Travel Services
Ms. Mary Solis, Director/Chief Compliance and Ethics Officer, Office of Institutional Compliance (OIC)

University of Texas System (UT System):

System Audit Office

External:

Governor’s Office of Budget, Planning and Policy
Legislative Budget Board
Internal Audit Coordinator, State Auditor’s Office

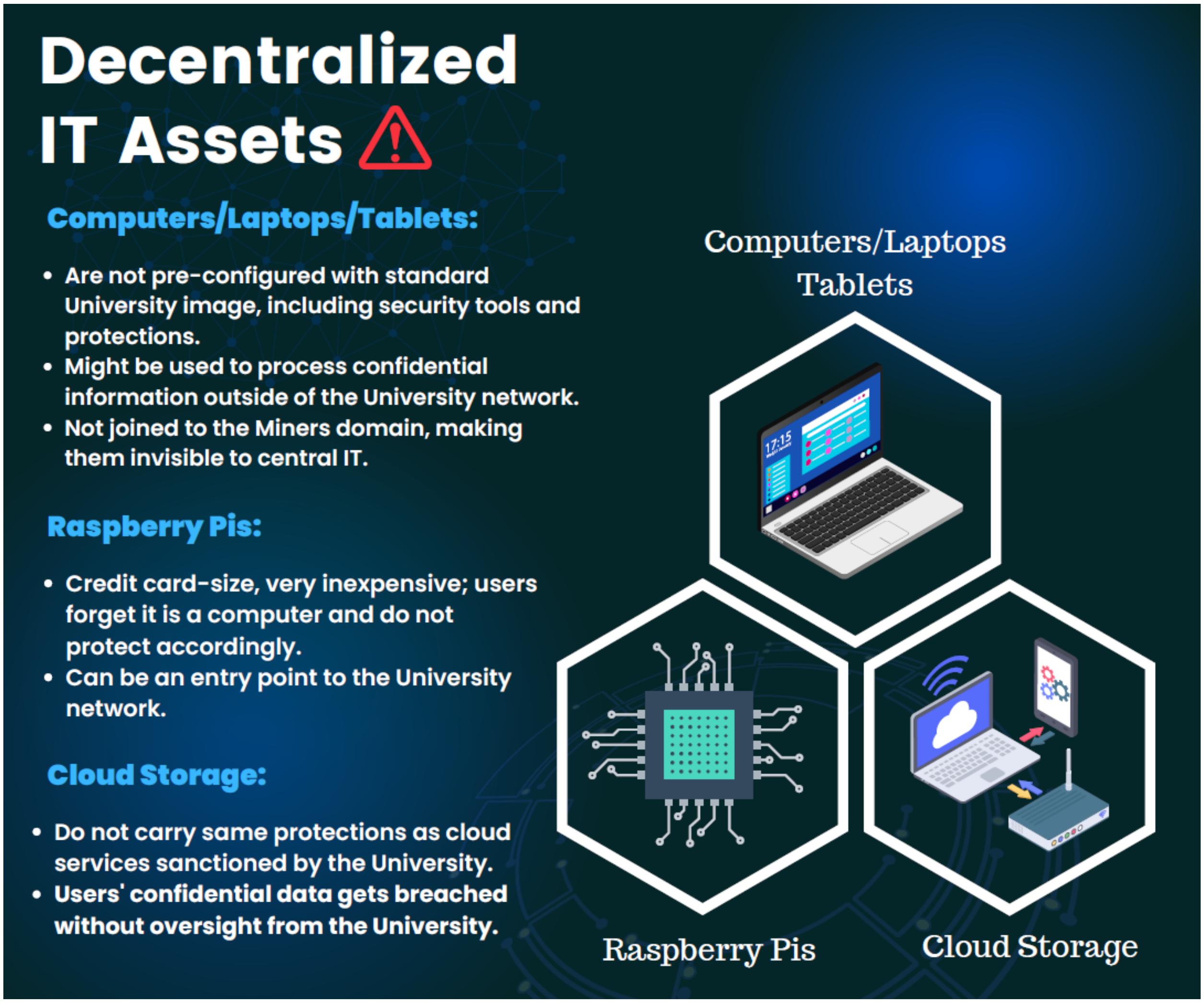
Audit Committee Members:

Mr. J. Stephen DeGroat, Audit Committee Chair
Mr. Fernando Ortega, External Member
Dr. John Wiebe, Provost, Vice President for Academic Affairs
Mr. Daniel Garcia, Associate Athletic Director, Business, Finance & Facilities
Ms. Guadalupe Gomez, Assistant Vice President for Research Administration

Auditors Assigned to the Audit:

Cecilia Estrada, IT Auditor II
Jannell Ballin, Senior Auditor I
Luis Carrera, IT Audit Manager

APPENDIX A: IT ASSET SECURITY RISKS



Decentralized IT Assets ⚠

Computers/Laptops/Tablets:

- Are not pre-configured with standard University image, including security tools and protections.
- Might be used to process confidential information outside of the University network.
- Not joined to the Miners domain, making them invisible to central IT.

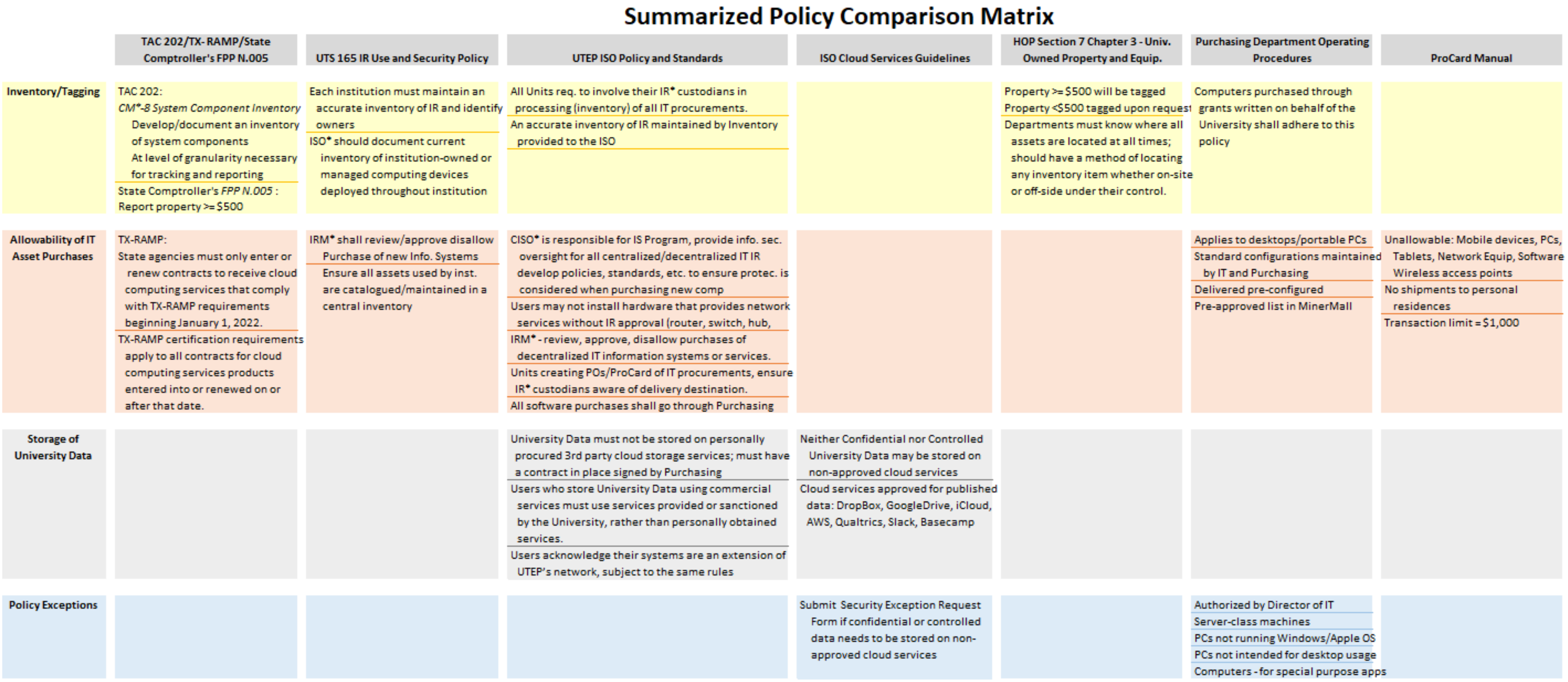
Raspberry Pis:

- Credit card-size, very inexpensive; users forget it is a computer and do not protect accordingly.
- Can be an entry point to the University network.

Cloud Storage:

- Do not carry same protections as cloud services sanctioned by the University.
- Users' confidential data gets breached without oversight from the University.

APPENDIX B: POLICY COMPARISON MATRIX



Summarized Policy Comparison Matrix

	TAC 202/TX- RAMP/State Comptroller's FPP N.005	UTS 165 IR Use and Security Policy	UTEP ISO Policy and Standards	ISO Cloud Services Guidelines	HOP Section 7 Chapter 3 - Univ. Owned Property and Equip.	Purchasing Department Operating Procedures	ProCard Manual
Inventory/Tagging	TAC 202: *CM*-8 System Component Inventory* Develop/document an inventory of system components At level of granularity necessary for tracking and reporting State Comptroller's *FPP N.005* : Report property >= $500	Each institution must maintain an accurate inventory of IR and identify owners ISO* should document current inventory of institution-owned or managed computing devices deployed throughout institution	All Units req. to involve their IR* custodians in processing (inventory) of all IT procurements. An accurate inventory of IR maintained by Inventory provided to the ISO		Property >= $500 will be tagged Property <$500 tagged upon request Departments must know where all assets are located at all times; should have a method of locating any inventory item whether on-site or off-side under their control.	Computers purchased through grants written on behalf of the University shall adhere to this policy	
Allowability of IT Asset Purchases	TX-RAMP: State agencies must only enter or renew contracts to receive cloud computing services that comply with TX-RAMP requirements beginning January 1, 2022. TX-RAMP certification requirements apply to all contracts for cloud computing services products entered into or renewed on or after that date.	IRM* shall review/approve disallow Purchase of new Info. Systems Ensure all assets used by inst. are catalogued/maintained in a central inventory	CISO* is responsible for IS Program, provide info. sec. oversight for all centralized/decentralized IT IR develop policies, standards, etc. to ensure protec. is considered when purchasing new comp Users may not install hardware that provides network services without IR approval (router, switch, hub, IRM* - review, approve, disallow purchases of decentralized IT information systems or services. Units creating POs/ProCard of IT procurements, ensure IR* custodians aware of delivery destination. All software purchases shall go through Purchasing			Applies to desktops/portable PCs Standard configurations maintained by IT and Purchasing Delivered pre-configured Pre-approved list in MinerMall	Unallowable: Mobile devices, PCs, Tablets, Network Equip, Software Wireless access points No shipments to personal residences Transaction limit = $1,000
Storage of University Data			University Data must not be stored on personally procured 3rd party cloud storage services; must have a contract in place signed by Purchasing Users who store University Data using commercial services must use services provided or sanctioned by the University, rather than personally obtained services. Users acknowledge their systems are an extension of UTEP's network, subject to the same rules	Neither Confidential nor Controlled University Data may be stored on non-approved cloud services Cloud services approved for published data: DropBox, GoogleDrive, iCloud, AWS, Qualtrics, Slack, Basecamp			
Policy Exceptions				Submit Security Exception Request Form if confidential or controlled data needs to be stored on non-approved cloud services		Authorized by Director of IT Server-class machines PCs not running Windows/Apple OS PCs not intended for desktop usage Computers - for special purpose apps	