Information Technology Asset Management Policy

ITPOL- 048

Owner: Executive Director of Information Technology

Report Errors: itcompliance@uth.tmc.edu

TABLE OF CONTENTS

1.0 PURPOSE

The University of Texas Health Science Center at Houston (UTHealth) requires Central IT to report the status of laptop encryption. Central IT is required to provide the means to have oversight of all IT assets that are owned and leased by the university.

2.0 RESPONSIBILITY

Role	Responsibility
Lead IT Management Administrator	• Functional lead on the central IT inventory software, Information Technology Asset Management System (ITAMS). Maintains a thorough knowledge of the ITAMS software functionality. • Responsible for the security roles and responsibilities in ITAMS. • Develops and maintains training materials for IT Inventory Specialists • Trains IT Inventory Specialists in the functionality of the software. • Receives information on enhancements from Context Administrators. • Organizes, prioritizes, and manages requests for enhancements. • Collaborates with ITAMS Development Manager / Project Manager on improvements and enhancements. • Manages communications on outages; including Initial impact, updates when necessary, and resolution. • Manages communications on feature enhancement going to Production. • Responsible for ensuring policy changes are managed with all Context Administrators. • Submit feature enhancements. • Determine role assignments of Administrator and Technician within context **.** • Determine context settings.
IT Inventory Specialist/Tech	• Reports to Lead IT Management Administrator

nician/LAN Manager	• Provides support for the IT Inventory processes where needed. • Provide support in inventory control • Administers and manages IT inventory with the central IT inventory management system. • May require determining, entering and maintaining detail inventory information including vendor information, hardware/registration tag information, software licenses, various institutional forms, encryption, lease, and information on medical/research/scientific equipment. • Receives, deploys, decommissions, and disposes of IT inventory in compliance with university guidelines, policies, and practices; ensures security of equipment prior to and post deployment. • Resolves inventory discrepancies and issues, including tracking the location and status of IT inventory as well as identifying inconsistencies in IT Inventory policies and procedures; makes recommendations for improvements. • Assists with the deployment of new assets. • Helps update the ITAMS database for better inventory tracking. • Performs IT inventory equipment reviews, including validation of encryption, settings, OS, etc.
ITAMS Software Development Team	• Assesses all change requests and determines whether the request is a new feature or other development priority. • Receives issues on production functionality during the monthly meetings. • Maintains software enhancements of ITAMS.
Context Administrator	• Determine and maintain new and existing user and administrative settings within ITAMS. • Provide support in inventory control. • Enter tickets for bugs or issues. • Manages Application access for support school.

3.0 SCOPE

This policy is applicable to all IT equipment, purchased or leased with university funds/grants, and applies to those involved in the management of IT inventory and users as defined.

4.0 DEFINITIONS

Term	Definition
IT Management Group	The overseeing management of each UT Health entity. McGovern Medical School (MMS), General Administration (GADM), School of Dentistry (SOD), School of Nursing (SON), Graduate School of Biomedical Sciences (GSBS), School of BioMedical Informatics (SBMI), School of Public Health (SPH) and Harris County Psychiatric Center (HCPC).
IT Equipment	The context of this policy includes, but may not be limited to servers, desktop computers, laptops, docking stations, mobile phones, tablets, printers, photocopiers, scanners, monitors, hard drives, USB storage devices, network attached storage, routers, cabling, telecommunications.
LAN Manager	The name of desktop support personnel. Local Area Network Manager
Software	Examples include desktop business applications, operating system, and administration software.
Audio Visual equipment	Equipment such as projectors, smart boards, control systems.
Context Administrator	The administrator in charge of changing user and administrative settings specific to the IT management Group.
Medical Equipment	Devices designed to aid in the diagnosis, monitoring, or treatment of medical conditions in a clinical or research environment. E.g. x-ray, ultrasound, etc.
Asset Owner	An asset owner is an individual assigned an IT Asset in order to perform their assigned job or role (this would exclude users of shared IT Assets such as kiosks and lab computers).

ITAMS	Information Technology Asset Management System. A software product developed by internal UTHealth resources at the School of Public Health (SPH), which provides the functionality to track, bill, report, and reconcile all IT equipment owned and leased within a central data repository.
Onboard Process	The process taken when a new LAN Manager is hired on. This process covers all of the different security groups and accesses needed to perform the daily duties as an information technology employee.
CAM	Capital Assets Management is responsible for accurately tracking and reporting UTHealth's investments in capital assets. The department uses a software module within FMS which maintains information on purchased assets valued at $5,000.00 or more and controlled assets valued at $500.00 or more.
FMS (Financial Management System)	A collection of software modules developed and maintained by PeopleSoft Oracle used to maintain the financial data at UTHealth.
Leasing Vendor	The leasing company we use for leasing equipment.

5.0 PROCEDURES

5.1 Change Management

The method used to maintain the ITAMS product through change.

5.1.1 Change Types

- Minor Updates – New equipment type.
- Major Updates – New features.
- Functionality anomalies which prohibit use of the software are submitted through bug reporting procedure or contact your Context Administrator.

5.1.2 Change Procedures

5.1.2.1 All proposed changes are reviewed by the Context Administrator.

5.1.2.2 Development work is addressed based on priority.

5.1.2.3 Testing of changes is required prior to moving major changes into Production. Minor changes can be tested and approved to move to Production by the Development Team. Major changes must be tested by Context Administrators.

5.1.2.4 Approvals – All testing performed on major enhancements must have a signed approval by the Context Administrators prior to moving to Production.

5.1.2.5 Communications are managed by the Lead IT Management Administrator.

5.2 Request/Removal of Access

5.2.1 During the onboarding process, access to ITAMS is given to the newly hired LAN Manager. If for some reason, the access is not given, email the Context Administrator to obtain the access needed. The context Administrator will verify the request with the appropriate school IT Director and then grant the LAN Manager their respective access**.**

5.2.2 All cross context access requests will have to go through an approval by the school/entities Context Administrator. Anyone requesting access will need to apply through the Lead IT Management Administrator.

5.2.3 Removal of access will occur when the employee leaves the University. This process is initiated when the manager contacts the Context Administrator requesting that the employee be deactivated from ITAMS.

5.3 Process/Procedure for reporting stolen assets

5.3.1 Any IT equipment, including leased, that becomes lost/stolen or missing (cannot be located) must be reported to your IT Management group immediately.

5.3.2 Report stolen/missing asset to UT Police via 713-792-2890.

5.3.2.1 Stolen/missing asset is reported to IT Security via the ITS Lost/Stolen UTHealth-Managed Device (AOG 74-194) Report.

5.3.3 Keep all of the paperwork and update the ITAMS status to Lost/Stolen. (any reference to forms required to report Lost/Stolen)

5.3.4 Contact leasing vendor for buyout information if the equipment is a leased item. Equipment status is set to Lost/Stolen with buyout information attached.

5.3.5 Contact CAM if it is a purchased piece of equipment**.**

5.4 Mandatory Items tracked in ITAMS

The following assets must be entered. Additional assets can also be tracked if needed.

- Desktop Computer Systems
- Laptop Computer Systems
- iPad Devices
- Tablet Devices
- Medical Computers and Equipment
- Research Computer Systems

5.5 Mandatory Fields in ITAMS

The following fields must be entered.

5.5.1 System Name and serial number

The system name and serial number must be unique and cannot be an empty field.

5.5.2 Owner information

If the equipment is a shared device, then use the Office Manager, Department Designee or placeholder as the owner.

5.5.3 Location

The location in ITAMS is updated at the time the equipment is transferred to a new users/office or returned to IT.

5.5.4 Department

5.5.4.1 The department is the area where an asset is assigned.

5.5.4.2 The *sub*-department field is *not* mandatory. Some areas may use it to further define where a system is assigned. For example, Stroke is a division under the Neurology department.

5.5.5 Make, Model

Every equipment/asset has a make and model.

5.5.6 Encryption – *For computers/tablets only*

5.5.6.1 If the device cannot be encrypted, requests for exceptions to this policy need to be submitted to the Chief Information Security Officer via the *Information Technology Security Policy Exemption/Exception Request Online Tool* for review and consideration, then the encryption status must be changed to ITS pending. When the exemption is approved, update the encryption status to EXEMPTED

and upload the approval document. This exemption needs to be renewed every 2 years.

5.5.6.2 If the operating system is WinXP or older, an exception needs to submitted to the Chief Information Security Officer via the *Information Technology Security Policy Exemption/Exception Request Online Tool* for review and consideration. When the exception is approved by the CISO, upload the approval document into ITAMS. This exception needs to be renewed every two years.

5.5.7 Operating System

5.5.7.1 Medical / Research device

5.5.7.1.1 If the device contains an operating system, the OS field must be completed.

5.5.7.1.2 If the OS is WinXP or older, or a third party custom made OS, an exception needs to submitted to the Chief Information Security Officer via the *Information Technology Security Policy Exemption/Exception Request Online Tool* for review and consideration and all pertinent documents must be uploaded.

5.5.7.1.3 If the OS cannot be encrypted, an exception needs to submitted to the Chief Information Security Officer via the *Information Technology Security Policy Exemption/Exception Request Online Tool* for review and consideration. All pertinent documents must be uploaded for the exemption.

5.5.7.1.4 For a medical device, under the MRS table, the device must have a CLASS grade entered.

5.5.8 Leased Equipment

5.5.8.1 Before the leased equipment is returned to the leasing company, replacement equipment must be ordered and received before the expired equipment is returned to the leasing vendor. (Where applicable)

5.5.8.2 The department may continue the lease on a month to month basis.

5.5.8.3 If the department is 'buying out' the equipment, the equipment status is changed to 'DEPARTMENT BUYOUT' located under the lease information area. Then, enter the date of coverage for the IT department. It is usually 2 years from the date that the department purchased it, where applicable.

5.5.8.4 If the equipment is purchased by a user when the lease ends, the status is still changed to "Return to leasing vendor".

5.5.9 Purchased Equipment - Capital Asset Management (CAM)

5.5.9.1 If the requirements of CAM for tagging are met, then you must contact CAM at 713-500-4732 to tag it when the equipment arrives.

5.5.9.2 Assist CAM in performing their annual physical inventory check.

5.5.9.3 If the equipment is already in ITAMS, update the CAM tag under General Information after the CAM team has tagged the equipment.

5.6 Disposal -Surplus Process/Procedure.

5.6.1 Remove the hard drive when the equipment is ready to be surplused.

5.6.2 Put a surplus sticker on the equipment when it is ready to be surplused.

5.6.3 Submit all equipment that needs to be sent to surplus by using the Surplus Transfer of Equipment from this website: (https://apps.uth.edu/ehssurplus/)

5.6.4 Contact CAM at capitalassets@uth.tmc.edu and schedule a pickup date, or visit https://inside.uth.edu/finance/capital-assets-management/surplus.htm

5.6.5 When the CAM team picks up the equipment update the ITAMS status to SURPLUS.

5.6.6 Hard drive shredding is scheduled as needed.
For More Detailed Disposal-Surplus information, please check the CAM website

6.0 EXCEPTIONS/EXEMPTION

6.1 Computers/Tablets or any device with an operating system and hard drive must be updated under the 'ENCRYPTION FIELD' within ITAMS.

6.2 If the device cannot be encrypted, an exception request needs to submitted the Chief Information Security Officer via the *Information Technology Security Policy Exemption/Exception Request Online Tool* for review and consideration. While waiting, please update the encryption status to ITS pending. When the exemption is approved, update the encryption to EXEMPTED and upload the approval document. The Exemption needs to be renewed every 2 years.

6.3 If the operating system is WinXP or older, an exception request needs to submitted the Chief Information Security Officer via the *Information Technology Security Policy Exemption/Exception Request Online Tool* for review and consideration. When the Exception is approved by the CISO, note the exemption number into ITAMS. This exemption needs to be renewed every two years.

7.0 ENFORCEMENT

Violation of this policy may result in the revocation of network access for the affected systems; and disciplinary action that may include the termination of employees, contractors, and consultants. Early dismissal applies to interns and volunteers who violate the UT policies. Additionally, individuals are subject to loss of UTHealth Information Resources access privileges, civil, and in some cases criminal prosecution.

8.0 CONTACTS

Name of IT Management	Title or Office/Department	Telephone	E-mail
Rick Miller	VP Information Technology & CIO	713-486-3603	Richard.L.Miller@uth.tmc.edu
Bassel Choucair	Executive Director, Information Technology • MS School IT Approver • UTP Clinics IT Approver • SON IT Approver	713-500-5034	Bassel.Choucair@uth.tmc.edu
Krishna Sankhavaram	Executive Director, Information Technology • SPH IT Approver	713-500-9086	Madhavkrishna.sankhavaram@uth.tmc.edu
Kevin Granhold	Executive Director and Chief Technology Officer, • General Administration Approver • SOD IT Approver	713-486-3624	Kevin.B.Granhold@uth.tmc.edu
Ryan Bien	Associate Dean for Management I • SBMI IT Approver	713-500-3640	Ryan.L.Bien@uth.tmc.edu
Patricia Bruesch	Associate Dean for Management II • GSBS IT Approver	713-500-9878	Patricia.Cruz@uth.tmc.edu
James Griffiths	Executive Director & Clinical Technology Officer; • Clinical Technology Approver • HCPC IT Approver	713-500-6940	James.J.Griffiths@uth.tmc.edu

9.0 REVISION HISTORY

Author	Version	Reason For Change	Effective Date
Wang, YenSheng	1.0	Initial Release	6/27/2017
Tammy Gardiner	1.1	IT Compliance & CIO Review	07/26/2017
Bonnie McDonough	1.2	Update verbiage to comply with IT audit's recommendations	09/12/2017

10.0 APPROVAL

Tammy Michelle Gardiner

Digitally signed by Tammy Michelle Gardiner
Date: 2017.09.12 16:18:01 -05'00'

Certified by Tammy Michelle Gardiner
IT Risk and Compliance Manager

Richard L Miller

Digitally signed by Richard L Miller
DN: postalCode=77030, ou=UTHEALTH NON-ESCROW, o=The University of Texas Health Science Center at Houston, street=7000 Fannin, st=Texas, l=Houston, c=US, cn=Richard L Miller, email=richard.l.miller@uth.tmc.edu
Date: 2017.09.13 11:13:49 -05'00'

Approved by Richard L. Miller, CIO