**Information Technology Asset Management**

**ITAMS**

**Architecture & Design**



Document Control

Please note that printed copies of this document, permitted or otherwise, are uncontrolled and shall be treated as such.

Document Authorization

|  |  |
| --- | --- |
| Name | Role |
| ITAMS Project Team |  |
|  |  |
|  |  |
|  |  |

Change History

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version | Date | Author | Reviewer | Approver | Summary of changes |
| 1.0 | 10/11/17 | ITAMS Team | ITAMS Team |  | Final Review |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Document References

|  |  |  |  |
| --- | --- | --- | --- |
| Document | Version | Date | File name |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Information Technology Asset Management System (ITAMS) Design Document 3](#_Toc493226877)

[1.0 ITAMS Overview 3](#_Toc493226878)

[1.1 ITAMS MS SQL and Web Servers Diagram 3](#_Toc493226879)

[1.2 ITAMS Users 3](#_Toc493226880)

[2.0 Responsible Parties 4](#_Toc493226881)

[3.0 ITAMS Picklist 4](#_Toc493226882)

[4.0 Picklist Process flows 6](#_Toc493226883)

[4.1.1 ERD Picklist Process 6](#_Toc493226884)

[4.1.2 Location Picklist Process 7](#_Toc493226885)

[4.1.3 Standard Asset ERD Process 7](#_Toc493226886)

[4.1.4 Software ERD Process 8](#_Toc493226887)

[5.0 ITAMS Procedural Instructions 8](#_Toc493226888)

[5.1 ITAMS primary screens for application 8](#_Toc493226889)

[6.0 Reporting ITAMS Bug: 16](#_Toc493226890)

[Appendix A - Screens: Categories and Picklist 17](#_Toc493226891)

**Table and Figures**

[Table 3‑1 ITAMS Pick List 6](#_Toc493225637)

[Figure 2‑1 ITAMS Responsibilities 4](#_Toc493225645)

[Figure 4‑1 ITAMS ERD Process Flow 6](#_Toc493225646)

[Figure 4‑2 ITAMS Location Process 7](#_Toc493225647)

[Figure 4‑3 ITAMS Standard Asset ERD Process 7](#_Toc493225648)

[Figure 4‑4 ITAMS Software ERD Process 8](#_Toc493225649)

Information Technology Asset Management System (ITAMS) Design Document

# ITAMS Overview

The central building block of ITAMS is the idea of a **Context**. A **Context** is an isolated grouping of assets, picklist values, and user permissions. Each context presents a unique dashboard to a unique group of users different levels of functionality based on the requirements of that Context group. (see 1.2)

* Database built in SQL Server 2008 R2
* ASP.NET WebAPI 2.2 REST architecture
* 1.0 client is a hybrid ASP.NET MVC5 and AngularJS application
* 1.2 client is written in pure JavaScript

## ITAMS MS SQL and Web Servers Diagram



## ITAMS Users

ITAMS supports the following organizations:

* GLOBAL – All contexts
* GADM – General Administration
* HCPC – Harris County
* MS – Med School
* SBMI - Informatics
* SPH – School of Public Health

# ITAMS Picklist

A picklist is a context specific pre-defined set of values:

|  |  |
| --- | --- |
| * Asset Status
 | * Encryption Type
 |
| * Operating Systems
 | * Responsible Party
 |
| * Equipment
 | * + Single User
 |
| * + Types
 | * + Multiple Users
 |
| * + Makes (Dell, etc.)
 | * Asset Document Types
 |
| * + Models (9020, etc.)
 | * Department / Sub-Department
 |
| * Campus / Building / Location
 | * Encryption Type
 |

| Pick List type | CommonFields | StandardAsset | Dept’s | Sub-Dept’s | Locations | Lease | MedicalEquipment | Software | SoftwareLicense |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Asset Document Types |  |  |  |  |  |  |  |  |  |
| Id | **√** | **√** | **√** | **√** | **√** |  |  | **√** | **√** |
| Context Id | **√** |  | **√** | **√** | **√** |  |  | **√** |  |
| System Name |  | **√** |  |  |  |  |  |  |  |
| Tag Number |  | **√** |  |  |  |  |  |  |  |
| Serial Number |  | **√** |  |  |  |  |  |  |  |
| Other Id |  | **√** |  |  |  |  |  |  |  |
| Operating System |  | **√** |  |  |  |  |  |  |  |
| Type |  | **√** |  |  |  |  |  |  |  |
| Make |  | **√** |  |  |  |  |  |  |  |
| Model |  | **√** |  |  |  |  |  |  |  |
| Status | **√** | **√** | **√** | **√** | **√** | **√** | **√** | **√** | **√** |
| Location |  | **√** |  |  |  |  |  |  |  |
| Encryption |  | **√** |  |  |  |  |  |  |  |
| Encryption Date |  | **√** |  |  |  |  |  |  |  |
| Encryption Verified By |  | **√** |  |  |  |  |  |  |  |
| Department |  | **√** |  |  |  |  |  |  |  |
| Sub-Department |  | **√** |  |  |  |  |  |  |  |
| Responsible Party |  | **√** |  |  |  |  |  |  |  |
| Parent Asset |  | **√** |  |  |  |  |  |  |  |
| Created Date / By |  | **√** |  |  |  | **√** | **√** | **√** | **√** |
| Created By | **√** |  | **√** | **√** | **√** |  |  |  |  |
| Created Date | **√** |  | **√** | **√** | **√** |  |  |  |  |
| Last Modified Date / By |  | **√** |  |  |  | **√** | **√** | **√** | **√** |
| Last Modified Date |  |  | **√** | **√** | **√** |  |  |  |  |
| Modified By | **√** |  | **√** | **√** | **√** |  |  |  |  |
| Modified Date | **√** |  |  |  |  |  |  |  |  |
| Asset Id |  |  |  |  |  | **√** | **√** |  |  |
| Lease End Date |  |  |  |  |  | **√** |  |  |  |
| Rent |  |  |  |  |  | **√** |  |  |  |
| Billable Department Id |  |  |  |  |  | **√** |  |  |  |
| Schedule |  |  |  |  |  | **√** |  |  |  |
| Description | **√** |  | **√** | **√** |  | **√** | **√** |  |  |
| Department Id (from FMS) |  |  | **√** |  |  |  |  |  |  |
| Campus Id |  |  |  |  | **√** |  |  |  |  |
| Building Id |  |  |  |  | **√** |  |  |  |  |
| Location Id |  |  |  |  | **√** |  |  |  |  |
| Chartstring |  |  | **√** | **√** |  | **√** |  |  |  |
| IsDefault |  |  |  |  | **√** |  |  |  |  |
| Context |  | **√** |  |  |  |  |  |  |  |
| Category |  |  |  |  |  |  | **√** |  |  |
| ITS Exemption Number |  |  |  |  |  |  | **√** |  |  |
| ITS Exemption Expiration Date |  |  |  |  |  |  | **√** |  |  |
| ITS Exception Number |  |  |  |  |  |  | **√** |  |  |
| ITS Exception Expiration Date |  |  |  |  |  |  | **√** |  |  |
| Manufacturer |  |  |  |  |  |  |  | **√** |  |
| Title |  |  |  |  |  |  |  | **√** |  |
| Version |  |  |  |  |  |  |  | **√** |  |
| Software Id |  |  |  |  |  |  |  |  | **√** |
| Number of Licenses (integer) |  |  |  |  |  |  |  |  | **√** |
| Unlimited licenses (boolean) |  |  |  |  |  |  |  |  | **√** |
| Purchase Date |  |  |  |  |  |  |  |  | **√** |
| Purchased By |  |  |  |  |  |  |  |  | **√** |
| Purchased For |  |  |  |  |  |  |  |  | **√** |
| Comment |  |  |  |  |  |  |  |  | **√** |
| License Key |  |  |  |  |  |  |  |  | **√** |
| License Form(at) |  |  |  |  |  |  |  |  | **√** |
| Legacy License Id |  |  |  |  |  |  |  |  | **√** |
| Sub-Department Id (from FMS) |  |  |  | **√** |  |  |  |  |  |
| DeptPk (PK of parent Department) |  |  |  | **√** |  |  |  |  |  |

Table 3‑1 ITAMS Pick List

# Picklist Process flows

## Responsible Parties

Responsible parties allow an asset to be associated with one-or-more users listed in the Global Address List (GAL)

Users may be part of 1-to-N responsible parties. A users **primary** responsible party is the one with their email address as the description. When assigning the owner of an asset, users are assigned using their primary responsible party. OwnerId property on each asset is associated to the Id of the ResponsibleParty



### ERD Picklist Process



Figure 4‑1 ITAMS ERD Process Flow

### Location Picklist Process



Figure 4‑2 ITAMS Location Process

### Standard Asset ERD Process



Figure 4‑3 ITAMS Standard Asset ERD Process

### Software ERD Process



Figure 4‑4 ITAMS Software ERD Process

# ITAMS Procedural Instructions

## ITAMS primary screens for application

* Inserting new equipment into ITAMS.
* Click on the action button located on the top right hand side of the page.
* Click “Add Asset”



* Fill in all the boxes shown below



* System name depends on the equipment that is being inserted into ITAMS
* Desktop/Laptop: The computer name provided by the Lan manager.
* Scanners/Printers/fax: Use the MSIT tag has the system name and the Other ID
* Tag Number box is for Capital Asset tags and Other ID will be the MSIT tags
* More information about Capital Asset will be on the next page.
* Equipment Type: It can be a, Desktop, Laptop, Research, Medical, etc. this is also a required field.
* Equipment Make: What is the brand of the equipment? For example, Dell, Apple, Fujitsu, etc. Also a required field when adding a device.
* Equipment Model: The model of the equipment. For example, OptiPlex 7040, fi-7160, IX500, etc.
* Owner Type: Will be “GAL USER”
* Owner: This is a required field. The person who will be using that device. If the device is clinical or Research, please type down the POA name.
* After you have filled in everything click “OK” and it would take you to the page shown below.



* General Information should have the following boxes filled out
* System name, Cam tag, serial number, other ID (MSIT #), Type, Make, Model, OS, Department, Sub-Department (optional).
* Operating System (OS)
* CAM tag box only filled if the equipment was purchase, in addition, Capital Asset team should provide the tag number.
* Tablet only if it’s over $500.00
* Desktop/laptops tagged by capital asset whenever purchased.
* On the picture shown above, please fill in the required fields needed.
* ‘Encryption Information’ box only filled if the device is a computer/laptop or anything with a hard-drive.
* “Location Information” Box: Should contain the Campus where the device will be located
* Remote Clinic: Are campuses that are located outside of the medical center.
* Ex: Woodland, Bellaire, Katy, Memorial, etc…





* Building: Provides the building and department where that device will be located
* Location: Should be exactly where that device is located.
* Example: 5/510 (6431 Fannin St. Houston TX 77030)
* Five: stands for 5th floor and 510 stands for the suite number.
* Owner Information
* Owner information should have the person name who will be using the device.
* For clinic computers please have the clinic manager name.



* Lease Information
* The description column should have the PO number, and the rest are optional.



* MRS tab
	+ Medical/Research/Scientific equipment areas include:



* Description: What type of device is it?
* Medical Device Category:
* *Category 1:* Device is not capable of storing PHI
* Includes and medical and scientific devices that are not able to store any PHI. The risk will be minimal due to no storage of PHI if the device location is unknown.
* *Category 2:* device is capable of storing PHI
* Category II includes medical and scientific devices that are able to store PHI persistently on local media, but are unable to connect to the wired or wireless computer network. Category II risks include the unauthorized disclosure of PHI when the device is missing or stolen. Category II devices must be configured with encryption to protect against data disclosure or configured so that PHI is unable to accumulate beyond 100 records on the local media if encryption is not permitted by the manufacturer.
* *Category 3:* device is capable of storing PHI and is connected to the network.
* Category III includes medical and scientific devices that are able to store PHI persistently on local media and are able to connect to the wired or wireless computer network, but are unable to interface with the EHR or other patient care systems. Category III risks include the unauthorized disclosure of PHI when the device is missing or stolen and possible vulnerabilities in the operating system or the software that could allow a network attacker to compromise the security of the device. Category III devices must be configured with encryption to protect against data disclosure or configured so that PHI is unable to accumulate beyond 100 records on the local media if encryption is not permitted by the manufacturer. Security patches, anti-virus software, or in-line intrusion prevention system should be applied to category III medical and scientific devices in order to mitigate the risk of network attacks.
* *Category 4:* device is capable of storing PHI, is connected to the network, and is interfaced with any EHR or any systems (e.g. the device can upload and download PHI to and from an EHR or any other system.
* Includes medical and scientific devices that are able to store PHI persistently on local media, are able to connect to the wired or wireless computer network, and are able to interface with, e.g. download/upload PHI, the EHR or other patient care systems. risks include the unauthorized disclosure of PHI when the device is missing or stolen and possible vulnerabilities in the operating system or the software that could allow a network attacker to compromise the security of the device, which is especially important considering that these devices have access to the EHR and are able to import a large amount of PHI. PHI is unable to accumulate beyond 100 records on the local media if the manufacturer does not permit encryption. Security patches, anti-virus software, and in-line intrusion prevention system is applied to category VI medical and scientific devices in order to mitigate the risk of network attacks.
* Exception #: After IT Security have approved your order, and then they will provide an Exception number.
* Exception Expire Date: The ITS will provide this information when the exception has been approved.
* Exemption #: After Clinical Technology have approved your order, and then they will provide an exemption number.
* Exemption Expire Date: The Clinical Technology will provide this information when the exemption is approved.
* Make sure everything in the MRS tab is filled out
* For additional information, please click on the link below:
	+ - [Medical and Scientific Device SOP](https://inside.uth.edu/it/cio/policies/policy.htm?id=f9c83db4-3a0a-4121-880e-301df81c079a&catVar=itSop)
* Comment Tab: Please write down any comments here for additional information about the equipment.



* Documents Tab: Please upload any documents that can provide more information about the equipment. In addition, adding the encryption key, Exception and Exemption form of approval can help a lot.



* Change log Tab: Shows any changes done in ITAMS for that device, and will show the person who made those certain changes.



* Linked Assets Tab: If the computer linked to any other device.



* Software Tab: allows an association between an asset and the license for the software installed on it.
* Administrators and Technicians can associate a software license to an asset.
* Some assets have multiple licenses.
* Multiple licenses may exist for particular software.



* CAM Data Tab: The information provided in this tab derives directly from FMS.



* Bulk Upload: Bulk upload will help reduce the time by inserting multiples devices into ITAMS all at once. A temperate of the bulk upload file is in the Bulk upload screen. Please fill out all the required fields and then upload to ITAMS.



# Reporting ITAMS Bug:

For any technical difficulties, please report a Bug, so our ITAMS team can resolve the problem.

Priority: This will help the ITAMS team determine how critical this issue is.

Summary: Describe where the issue is occurring

* Example:
	+ Bulk upload not working.
	+ Document cannot be uploaded

What went wrong? : Give a description of the issue, and the error it is giving you. Please be specific and detailed oriented so it can be clear to the ITAMS team.

Attach file: If possible, please attach a picture of the error message or any documents that you are trying to upload into ITAMS.



1. - Screens: Categories and Picklist
2. Login
3. Dashboard main page
	1. Search
	2. Information (detail Main page).
		1. General info
		2. Encryption info
		3. Owner Info
		4. Location info
		5. Lease info
	3. MRS
		1. Edit MRS
	4. Comments
		1. Add Comments
	5. Documents
		1. Add files to upload
		2. Remove document
	6. Change log
	7. Link Assets
		1. Search for asset to link.
		2. Unlink Asset
	8. Software
		1. Add Software
		2. Remove Software
	9. Cam data
4. Action
	1. Bulk upload
		1. Choose file
	2. Add Asset
5. Administration
	1. Picklist
		1. General
			1. Permission
				1. Add users
				2. Edit user
				3. Remove Users
				4. Search Users
			2. Asset Status Codes
				1. Add Status
				2. Edit Status
				3. Re-assign assets
				4. Find asset
				5. Remove Status
			3. Document Types
				1. Add Document types
		2. Users & Responsible parties
			1. Users
				1. Search user
				2. Add users
				3. Reload users
				4. Edit users
				5. Sync with Gal
				6. Re-assign assets
				7. Find assets
				8. Remove users
				9. Display total assets under user
			2. Responsible parties
				1. Add parties
				2. Edit Parties
				3. Find users
				4. Find assets
				5. Delete parties
				6. Display total assets under parties
		3. Encryption
			1. Add Encryption type
			2. Search Encryption Type
			3. Reload
			4. Edit Encryption Type
			5. Re-Assign asset
			6. Find asset under Encryption type
			7. Remove Encryption type
		4. Operation systems
			1. Search OS
			2. Add OS
			3. Edit OS
			4. Re-assign asset to diff OS
			5. Find asset under OS type
			6. Remove OS
		5. Equipment
			1. Equipment Makes
				1. Search Makes
				2. Edit Makes
				3. Find asset under Makes
				4. Remove Make
			2. Equipment Types
				1. Search Types
				2. Edit Types
				3. Find asset under types
				4. Remove Type
			3. Equipment Model
				1. Edit Model
				2. Re-assign Model
				3. Find asset under Models
				4. Remove Model
		6. Campus & Building
			1. Campus
				1. Add Campus
				2. Edit Campus
				3. Find asset under Campus
				4. Remove Campus
			2. Building
				1. Find Building
				2. Edit Building
				3. Find asset under building
				4. Remove Building
		7. Locations
			1. Search location
			2. Edit location
			3. Find asset under location
			4. Remove location
		8. Departments
			1. Add Department
			2. Edit Department
			3. Find asset under department
			4. Remove Department
		9. Sub Department
			1. Add Sub-Department
			2. Edit Sub-Department
			3. Find asset under Sub-Department
			4. Remove Sub-Department
	2. Software
		1. Find Software
		2. Edit software
		3. View software
			1. Edit Software
			2. Find asset use software
			3. Remove software
		4. Remove software
6. Report Bug
	1. Detail input
	2. Upload file
	3. submit