IT ASSET MANAGEMENT POLICY

Business Function: Human Resources

1. POLICY

It is a SIGMASOFT INFOTECH (SSIT) requirement that physical (hardware) and logical (software) IT assets used to manage SIGMASOFT INFOTECH. (SSIT) client, third party and internal information throughout their lifecycles (including creation, processing, storage, transmission, deletion, and destruction) must be identified, protected, and kept confidential for only valid business purposes.

2. PURPOSE

The purpose of this policy is to establish the controls and responsibilities to meet the requirements set forth in this document.

3. APPLICABILITY

This Policy applies to

I. Covered SIGMASOFT INFOTECH (SSIT) Employees
II. Covered SIGMASOFT INFOTECH (SSIT) Third Parties
III. Covered SIGMASOFT INFOTECH (SSIT) Information

4. DEFINITIONS

"Covered SIGMASOFT INFOTECH (SSIT) Information" means all SIGMASOFT INFOTECH (SSIT), Customer, Supplier, Employee, and other Third Party confidential, proprietary, financial, personal or other sensitive information stored, transmitted, or received using a Covered SIGMASOFT INFOTECH (SSIT) Information System whose unauthorized disclosure or access can result in harm to SIGMASOFT INFOTECH (SSIT) Technology or a Third Party to whom that information belongs. The term "Information" applies regardless of whether the information exists in digital, audio, electronic, facsimile, or other form.

"Covered SIGMASOFT INFOTECH (SSIT) Information Owners" for the purposes of this standard, means SSIT Management, Business Units and Functions.

"Covered SIGMASOFT INFOTECH (SSIT) Employee" means any employees of SIGMASOFT INFOTECH (SSIT), its wholly owned subsidiaries, and their affiliates.

"Covered SIGMASOFT INFOTECH (SSIT) Third Party" means any business
partner, supplier, sub-contractor, reseller, distributor, joint venture, consortium, teaming partner, lobbyist, law firm or other business partner that will either assist SIGMASOFT INFOTECH (SSIT) in delivering services, represent SIGMASOFT INFOTECH (SSIT)'s interests to a customer or third party, or provide SIGMASOFT INFOTECH (SSIT) a service.

"SIGMASOFT INFOTECH (SSIT) Technology," for purposes of this standard, means SIGMASOFT INFOTECH (SSIT) Technology Company, its parents, subsidiaries, affiliates, and inherited businesses; SIGMASOFT INFOTECH (SSIT)'s Suppliers and Vendors; and SIGMASOFT INFOTECH (SSIT)'s Employees.

5. REQUIREMENTS

5.1 Inventory of IT Assets: IT assets are the property of SIGMASOFT INFOTECH (SSIT) and should be protected all the time. Certain IT asset Classes (shown below) must be inventoried, tracked and accounted in an approved SIGMASOFT INFOTECH (SSIT) Technology asset repository. These IT Asset Classes include: workstations, network, servers, office network printers and software. In addition, any IT asset that is capitalized or leased must be inventoried. Assets in support of client or "Trade" engagements must be inventoried at an account level. Peripherals and mobile devices should be inventoried by exception only.

Covered SIGMASOFT INFOTECH (SSIT) Information Owners are responsible for maintaining an inventory in electronic format of all IT assets under their control which includes tracking all pertinent information regarding the IT asset as described below. Covered SIGMASOFT INFOTECH (SSIT) Information Owners may delegate this task to the SIGMASOFT INFOTECH (SSIT) approved function that has responsibility for controlling the lifecycle of IT assets. However, Covered SIGMASOFT INFOTECH (SSIT) Information Owners must maintain and be ready to confirm that the inventory is current and accurate.

Sampling of IT assets in each of the inventoried IT Asset Classes is required to be selected to complete the Financial Sample Based Audit (SBA) process to support the reporting of capital assets. Details surrounding this requirement can be found within the F&A 3600 Accounting for Fixed Assets policy.

Assets are defined in the following classes

Chart 1.0

IT Asset Class	Type of Asset	Inventoried
Workstations	Desktops, Laptops.	Y
Network	Switches, routers, hubs, etc.	Y
Servers	Servers (e.g. virtual, cloud)	Y
Storage	Storage Array, Racks	Y
Office Printers	Office Printers (excluding Desktop Printers).	N
Peripherals	Monitors, keyboards, docking stations, racks	N
Mobile	Cell phones, handhelds, tablets	N
Software	Operation, Development, Application, System	Y
Media	Removable memory, CD's hard drives	N

The following information is the minimum requirements that must be maintained in the asset management inventory system of record:

IT Asset Class: Workstations, Network, Servers, Storage

Asset Data:

I. Serial Number (primary key field for tracking assets)
II. Name and location of the system
III. Name of the Device Owner
IV. Make and model of the hardware platform
V. Purchase date, Purchase order, Warranty end date
VI. Financial information (Original cost, capitalization amount, Net Book Value) – OPTIONAL for asset systems **Configuration Item Data:**
VII. List of CPU/RAM/memory residing on the system
VIII. Host name of the system
IX. Primary and secondary IP address of the system
X. List of Software operating system on PC's (including version and service pack)
XI. List of relevant versions, updates, patches, and fixes that have been installed (including security controls)
XII. Type and classification stored or processed on the system

As applicable, any relevant statutory, regulatory, and contractual requirements

IT Asset Class: Software

I. Name of the software
II. Description of the software function
III. Name of the Information Owner
IV. Current version/release of the software
V. Licensing information that covers entitlement and usage information
VI. List relevant of security controls that have been applied to secure the information resource
VII. List of relevant versions, updates, patches, and fixes that have been installed
VIII. List of individuals or groups who are authorized to access the information stored in processed by the application
IX. Listing of hardware asset on which the software resides

Recommended but optional items for IT classes include the following:

IT Asset Classes: Workstations, Network, Servers, Office Printers

I. Name of the Resource or Organization administrator
II. Business Owner and/or Application Owner
III. Other key contacts including any third parties that support maintain the resource
IV. Group name and purpose for multiple or devices/platforms that are used to provide a single service
V. Financial Information (e.g., purchase order ID, purchase date, cost capitalization amount)

IT Asset Class: Software

I. Description of the application's technical architecture

II. Name of the Resource or organization administrator
III. Other key contracts including any third parties that support or maintain the application
IV. List of any key business initiatives or business processes that the application supports

The relationships between assets and configuration items must be maintained to deliver IT services, and provide and accurate view of the estate.

5.2 **Labelling IT Assets**: IT assets must be labelled with the appropriate information as required to ensure identification, protection and tracking. Serial number, model name and description, purchase order, and location are the generally accepted primary tracking mechanism for hardware. IT asset tags are optional for use as requested/required.

5.3 **Acceptable use of IT Assets**: SIGMASOFT INFOTECH (SSIT) IT assets are provided for SIGMASOFT INFOTECH (SSIT) business purposes and restricted to such use. These business purposes include, but are not limited to: internet access, email (both SIGMASOFT INFOTECH (SSIT) internal email and web-based email), data and Intellectual Property (IP) owned or managed by SIGMASOFT INFOTECH (SSIT), including IP related to sales, marketing, and products.

5.3.1 Specific to SIGMASOFT INFOTECH (SSIT) Workstation, Network, and Server IT Assets
SIGMASOFT INFOTECH (SSIT) IT Assets specific to Workstation, Network, and Server must not be used:

- To perform any activity not related with the current SIGMASOFT INFOTECH (SSIT) users job role.
- To commit illegal copyright infringement. This includes the sharing of copyright-protected works by posting them on websites internal or external to SIGMASOFT INFOTECH (SSIT), or through file-sharing services

The following rules apply specifically to the use of SIGMASOFT INFOTECH (SSIT) Workstation IT assets:

- They are not to be used for testing, factory systems, as a second workstation, or for system monitoring. They are not to be used for training centers or as demo units.
- They are not to be kept as a spare, loaner, backup, or for unexpected events.
- They are provided to the employee, not the position. The device stays with the employee if he or she change internal jobs or is transferred. NOTE: Exceptions include when a device may not be moved between countries or legal entities.

The following rules applies to proper use of IT Software:

- Only IT Software provided or approved by SIGMASOFT INFOTECH (SSIT) shall be installed and utilized on Workstation IT assets downloadable from approved internal sources. Refer to Available Standard Software for more information.
- For the acceptable use of Office Printers, refer to the IT Office Print Policy.

5.4 Handling of Removable Media

The following requirements are mandated to avoid the unauthorized disclosure, modification, removal or destruction of information stored on media.

Management of removable media: Procedures are mandated for the management, protection and handling of removable media in accordance with the sensitivity of the information stored on them, as defined by the SIGMASOFT INFOTECH (SSIT) Information Categorization Standard. At a minimum, the requirements for these procedures must include the following:

- If the contents of any re-usable media are no longer required and the media is to be removed from SIGMASOFT INFOTECH (SSIT) control, the media is to be made unreadable as per para 5.4.1.
- All media must be stored in accordance with manufacturers' specifications and in a safe, secured environment.
- Information stored on removable media classified SIGMASOFT INFOTECH (SSIT) Medium or High Sensitivity is to be encrypted in accordance with the SIGMASOFT INFOTECH (SSIT) Information Encryption Standard.
- When media is at risk of degrading due to damage or end of life, information that is still needed must be transferred to fresh media before becoming unreadable.
- Multiple copies of valuable information are to be stored on separate media to reduce the risk of unexpected data damage or loss.
- Removable media drives are to be used only if there is a business justification.
- Where there is a need to use removable media to transfer High Sensitivity information, the business requirement must be validated and authorized by management, and the media controlled by SIGMASOFT INFOTECH (SSIT).

Physical media containing SIGMASOFT INFOTECH (SSIT) information assets must be protected throughout their lifecycle and securely disposed when no longer in use or being repurposed.

5.4.1 Securing Information for Media Reuse or Disposal

All media must be securely erased electronically, by overwriting or degaussing, or else physically, destroyed prior to disposal or reassignment of the system in accordance with the requirements of the SIGMASOFT INFOTECH (SSIT) Sanitization Standard.

5.4.2 Physical media transfer

To protect against unauthorized access, misuse, or corruption of media during transportation, the following requirements must be met:

- The use of authorized and reliable transportation or couriers with proof of delivery
- A list of authorized couriers approved by management
- The verification and identification of couriers

- Package sufficiently to protect the contents from any physical damage likely to arise during transit, and in accordance with any manufacturers' specifications. For example, packaging should protect against any environmental factors that may reduce the media's restoration effectiveness, such as exposure to heat, moisture, or electromagnetic fields
- Logs are to be kept, identifying the contents of the media and the protection applied, as well as the time of transfer to the transit custodians and time the media is received at its final destination.
- Media containing highly sensitive information must be double sealed (e.g., two envelopes, wrapping in paper or plastic and sealed in a box)

5.5 Return of IT Assets

All SIGMASOFT INFOTECH (SSIT) employees are required to return all SIGMASOFT INFOTECH (SSIT) IT assets assigned to them upon termination of their employment, contract, or agreement. Returned IT assets are to be consigned to the responsible party and updated in the inventory record with their status reflecting that they have been returned.

5.5.1 Terminations and Role Changes

- Any SIGMASOFT INFOTECH (SSIT) IT asset assigned to an employee must be returned to either the employee's manager or designated representative when the employee leaves the company or when the IT asset reaches its end of life and has been replaced.
- Information contained on SIGMASOFT INFOTECH (SSIT) equipment or an individual's personal equipment must be transferred to SIGMASOFT INFOTECH (SSIT) and all SIGMASOFT INFOTECH (SSIT) information on the medium or equipment must be securely erased. Refer to local HR policies and procedures that support this portion of this policy.

5.6 Disposal of IT Assets

All SIGMASOFT INFOTECH (SSIT) IT assets that are returned must be properly decommissioned/recommissioned, or disposed in compliance and adherence to corporate requirements as stated in the SIGMASOFT INFOTECH (SSIT) Sanitization and Destruction Standard for the reuse and/or disposal of company assets.

5.7 Audit Control of Assets

Assets should be controlled in the way they are procured, paid for, capitalized and disposed of conjunction with F&A 3600 Accounting for Fixed Assets policy:

5.8 Reporting a Lost or Stolen SIGMASOFT INFOTECH (SSIT) - issued IT Asset

In the event a SIGMASOFT INFOTECH (SSIT)-issued IT asset (such as a PC, laptop) is lost or stolen, refer to the Report/Replace a Lost or Stolen SIGMASOFT INFOTECH (SSIT)-issue PC for instructions.

6. EXCEPTIONS & VARIANCES (If applicable)

This policy complements but does not dictate financial policies for SIGMASOFT INFOTECH (SSIT) related to IT assets. Any exceptions to this policy required the prior written approval of the SIGMASOFT INFOTECH (SSIT) IT Asset Management organization and the CIO. All exceptions with be reviewed annually.

7. ROLE & RESPONSIBILITIES (define as necessary)

Role	Responsibility
Covered SIGMASOFT INFOTECH (SSIT) Employees	Protect and maintain SIGMASOFT INFOTECH (SSIT) physical and logical IT assets and information stored on those assets. Return or confirm the return of SIGMASOFT INFOTECH (SSIT) IT assets upon end of employment, end of need for use, or end of life of the IT asset. Proper handling and disposal of information and asset.
Covered SIGMASOFT INFOTECH (SSIT) Information Owner	SIGMASOFT INFOTECH (SSIT) management is responsible to ensure that information security is implemented within their organization as stated in this policy and the supporting information security standards. SIGMASOFT INFOTECH (SSIT) Business Units and Functions are responsible for controlling their information in accordance with this policy.
SIGMASOFT INFOTECH (SSIT) approved function that has responsibility for controlling the lifecycle of assets	Persons responsible for the operation and management of SIGMASOFT INFOTECH (SSIT) systems and servers that collect, manage, and provide access to SIGMASOFT INFOTECH (SSIT), client, and third-party information. They are responsible for maintaining inventory, in electronic form, of all information assets under their control

8. COMPLIANCE & VIOLATIONS

SIGMASOFT INFOTECH (SSIT) employees, contractors, third parties or representatives who knowingly violate or attempt to violate this Policy shall be subject to disciplinary action, up to and including termination from SIGMASOFT INFOTECH (SSIT) subject to applicable local employment laws and regulations.

9. RELATED POLICIES/STANDARDS

Related Policy	Relevance
Acceptable Use Policy	Define SIGMASOFT INFOTECH (SSIT) requirements for addressing security, reputational, and legal risks associated with the use of SIGMASOFT INFOTECH (SSIT) information Systems and SIGMASOFT INFOTECH (SSIT) Managed Devices.
Code of Conduct	Ensure our employees, contractors, third parties or representatives have everything they need to offer Cutting-edge, transformative technology solutions to our clients. That's why we're committed to using assets responsibly, and to guarding against waste, Abuse, theft, and loss
Confidential Information Policy	All SIGMASOFT INFOTECH (SSIT) employees and SIGMASOFT INFO TECH (SSIT) third parties are obligated to know when they're handling confidential SIGMASOFT INFOTECH (SSIT) information, to use the information discreetly and only for valid business need to have it, and to protect the information from unauthorized internal or external disclosure.
SIGMASOFT INFOTECH (SSIT) IT Asset Management Enterprise Data Lake (EDL)	The single source of truth providing a consolidated repository for identifying, managing, analyzing, reporting and summarizing SIGMASOFT INFOTECH (SSIT) internal owned and leased IT assets (hardware & software) utilizing a comprehensive portfolio of dashboards.
SIGMASOFT INFOTECH (SSIT) Information Categorization Standard	Requirements for the security categorization and protection of SIGMASOFT INFOTECH (SSIT) Information
SIGMASOFT INFOTECH (SSIT) Information Encryption Standard	Requirements for the encryption of SIGMASOFT INFOTECH (SSIT) information.

SIGMASOFT INFOTECH (SSIT) IT PC Hardware Policy	Company policy specifying that only one SIGMASOFT INFOTECH (SSIT) supplied, standard-issue personal computing device (PC) will be provided per worker.
SIGMASOFT INFOTECH (SSIT) Laptop & Mobile Device Security Standard	The requirements governing the security of mobile devices. (e.g., laptops, smartphones, and tablets) and mobile device applications used to conduct SIGMASOFT INFOTECH (SSIT) business.
SIGMASOFT INFOTECH (SSIT) Sanitization and Destruction Standard	The requirements for the secure sanitization or destruction of SIGMA SOFT INFOTECH (SSIT) Information.
F&A 3600 Accounting for Fixed Assets	All operating units will maintain records sufficient to describe the age, cost, net book value and location of individual capital assets and will control and protect such assets by periodic physical inventories and other prudent business measures.
Mobility: Bring Your Own Device (BYOD) Terms of Use	The BYOD Program in alignment with the SIGMASOFT INFOTECH (SSIT) BYOD Program allows employees of SIGMASOFT INFOTECH (SSIT) Technology Company, its subsidiaries and affiliates, and its contingent workers, the ability to use a personal device (smart phone, tablet) of their choosing to conduct SIGMASOFT INFOTECH (SSIT) business.
Records and Information Management	SIGMASOFT INFOTECH (SSIT) records and information assets shall be created, Managed, and dispositional in a way that fully supports SIGMASOFT INFOTECH (SSIT)'s business objects, controls for unnecessary or redundant cost, drives workflow efficiencies and reliable managerial decision making, and meets all legal, regulatory and contractual requirements.

Version Control History

Version	Amendment	Date of Amendment
V1.0	Policy updated	31-Jul-0222

V2.0	Policy Updated	23-Nov-2022