Policy Owner: CF - Information Technology (IT)	**Approval Date:** March 23, 2020
Approver: CIO - Vittorio Cretella	**Effective Date:** October 1, 2020
Contact: Willah Magbanua	**Scope:** Global

Business use

IT Asset Management Policy

1. Intent

The purpose of the IT Asset Management Policy (the "Policy") is to protect the P&G against loss, prevent security incidents, reduce the company's risk profile, to meet legal compliance commitments, and to lower cost and improve productivity through more efficient and effective IT Asset Management.

IT Asset Management is a foundational policy, which supports IT Operations and Information Security policies.

The policy ensures, that any P&G-owned hardware software or application, that is used in the course of business activities, or anything, that connects to the P&G Internal Network (the "IT Assets"), is acquired in a secure manner, and effectively documented and tracked throughout its life-cycle including the known interdependencies and relationships.

IT Assets are documented, so that change management, impact analysis, and compliance activities can be executed.

2. Scope

This policy applies to all employees, non-employees, and 3rd party vendors, who are owners, custodians or users of P&G IT Assets. This includes entities who manage, deploy, or support IT Assets, either internally or externally to the P&G environment.

The IT Assets covered by this policy, include:

- Software: i.e. commercial off-the-shelf software (the "COTS"), open source software, *software-as-a-service*, services, and/or applications used individually or in support of business processes (hosted internally or externally to the P&G environment e.g. cloud providers).
- Applications: i.e. Information Systems, Application Platforms, Widely Distributed Software & *End-User Developed Applications* (EUDAs).
- Hardware: i.e. desktop workstations, laptop and mobile computers, mobile phones, network cameras, tablets & handheld devices printers, copiers, multifunction machines, servers including virtual servers, firewalls, routers, switches.

IOT and facilities devices' operational technology (the "OT") is not the IT Assets' category covered by this policy.

3. Policy Requirements

P&G requires, that all Hardware & Application IT Assets must be managed, documented and tracked through their entire lifecycle – i.e. the changes in their status are promptly reflected in the Configuration Management Database (CMDB). This tracking shall be at latest from installation or deployment until such time that the Asset has reached end of life and has been properly removed from P&G environment.

3.1 IT Asset Acquisition

IT Assets can only be introduced into the P&G environment via approved methods. These methods shall include appropriate vetting for security, information architecture, and purchases compliance.

3.1.1 IT Assets' Procurement

Procurement of Information Technology should route to one of the companies provided channels where standard products and solutions are made available.
All newly acquired IT Assets must comply with the company's legal and information security requirements.

3.1.2 Software Compliance

Software Asset Management (SAM) assures that the SAM Application holds up-to-date entitlement data on all relevant Software IT Assets. The SAM team monitors compliance of software license to assure P&G has appropriately licensed software. For tier-1 software, compliance positions are reviewed on a regular basis and managed within acceptable standards.
All PCs and servers shall report installation data into the central SAM application to enable software compliance.

3.2 IT Asset Registration

A Configuration Management Database must be established, managed, and controlled. All IT Assets within the scope of this Policy must be registered within the CMDB. The CMDB must contain all information deemed necessary for key business processes. The CMDB must maintain complete up-to-date and accurate information on IT Assets, and have established processes to verify, reconcile and certify the data it contains.

The CMDB shall be populated by automated discovery mechanisms where possible and manual methods where not reasonably possible. It must be protected against data loss and alteration by unauthorized persons.

3.3 IT Asset Identification

All IT Assets must have an assigned unique ID number from a centrally managed pool of ID numbers. The unique assigned ID number must be maintained throughout the lifecycle of the IT Asset.
Critical equipment must be clearly labeled where needed for compliance and IT Operations.

3.4 IT Asset Disposition

Unused IT Assets must be either redeployed or disposed. IT Assets with residual value to the P&G must be evaluated for redeployment within the company.

All Assets with storage medias (regardless of media format) are internally sanitized (S1 sanitization) prior to redeployment or disposition. All Asset with storage medias (regardless of media format) are externally sanitized (S2 sanitization) prior to disposition. Both S1 & S2 sanitization must be performed in accordance NIST wiping standards (NIST SP 800-88 respectively).

The S2 sanitization & disposition must be performed by the designated ITAD supplier.

Software IT Assets, that are no longer being used must be marked as no longer being leveraged and made available for redeployment.

Software licenses cannot be transferred or provided to external entities without expressed permission granted under the license agreement and the IT Asset Management 2LOD organization.

3.5 IT Asset Documentation

CMDB must provide capability to track IT Assets based on their ID. The database must contain complete information on IT Asset ownership, purpose, classification, version, location, details of compliance requirements, licensing details, lifecycle status in line with the relevant asset class standard. The scope of the information on IT Assets, maintained in the CMDB must be sufficient for the needs for effective application management including governance, information security, financial, purchases, and IT Operations.

Standards shall be maintained to define which asset classes must be maintained and what data is required by asset class. These standards shall cover Hardware and Application assets.

Changes to status of Hardware & Application IT Assets must be promptly reflected in the CMDB, throughout those Assets' entire lifecycle. The minimum scope of IT Assets' status changes which must be reflected in the CMDB in timely manner include transfer, usage, lifecycle and disposition.

3.6 IT Asset Governance

A global IT Asset Management 2LOD organization ensures, that the IT Asset Database is checked regularly (independently, using discovery/mapping tools) to identify any discrepancy, and is signed off by a senior business leader or their delegate. IT Assets must enable compliance / legislation, security, financial and operational efficiency.

Formal responsibilities and procedures must be in place to ensure IT Asset data is kept up-to-date and accurate, with satisfactory control of all changes.

Methods shall be used to assure the completeness of the inventory including network scans, integration of asset management into external processes, cross system reconciliations, and data certification sign offs.

4. Definitions

2LOD (2nd Line of Defense)	P&G employees in governance roles who are updating policy, standards, and controls, consulting on compliance, and enabling the governance process via tools and procedures.
Application IT Assets, Application	From TOGAF 9.1: A deployed and operational IT system that supports business functions and services; for example, a payroll. Applications use data and are supported by multiple technology components but are distinct from the technology components that support the application.
Application Platforms	From TOGAF 9.1: The collection of technology components of hardware and software that provide the services used to support applications.
Commercial Off the Shelf Software	A packaged software that is either downloaded or installed directly onto an individual machine e.g. MS Office, 7Zip, mobile applications, and/or platforms.
Configuration Item	Any component, that needs to be managed in order to deliver an IT Service, an aggregation of work products that is designated for configuration management and treated as a single entity in the configuration management process. This aggregation consists of all required components: hardware, software, and other items that comprise a baseline. Examples include but are not limited to applications, software, operating systems, platforms, servers, databases, firewalls, switches, routers, etc. A configuration item does not include the settings, parameters, attributes needed to ensure the running of a system or its hardware.
Configuration Management Data Base, CMDB	A database which stores Assets unique identifiers and asset attributes.
EUDA	End User Developed Applications – Business Application developed using office technology such as Word, Excel, Access from Microsoft or OpenOffice products with significant automation programmed into the tool.
Hardware IT Assets, Hardware	IT Asset taking form of: - desktop workstations, laptop and mobile computers; - mobile phones, network cameras, tablets & handheld devices; - printers, copiers, fax machines, scanners, multifunction machines; - servers including virtual servers; - firewalls, routers, switches; IOT and Facilities devices.

Information System	Set of applications, services, information technology assets, or other information-handling components.
IT Assets	Any P&G-owned hardware software or application, that is used in the course of business activities, or anything, that connects to the P&G Internal Network. IT Assets include, but are not limited to: - desktop workstations, laptop and mobile computers; - mobile phones, network cameras, tablets & handheld devices; - printers, copiers, multifunction machines; - servers including virtual servers; - firewalls, routers, switches; - business applications (including cloud platforms and subscriptions); - software licenses including entitlements; - subscription or cloud services; IOT and facilities devices' operational technology (the "OT") is not IT Assets' category in the understanding of this Standard.
Open-source Software	Computer software with its source code made available with a license in which the copyright holder provides the rights to study, change, and distribute the software to anyone and for any purpose.
Operational Technology, OT	Operational Technology includes Industrial Control Systems (ICS) and other equipment, that is involved in the generation, transport, or analysis of data related to the manufacturing process, supplemental and/or ancillary systems such as backups, and protection controls such as firewalls or anti-malware solutions. OT is not covered by the hereby Standard.
Platform-as-a-Service	A category of cloud computing services that provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure.
Software-as-a-Service	A cloud service licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. It is sometimes referred to as "on-demand software". Typically accessed via web browsers.
Software IT Asset, Software	IT Asset taking form of software license, entitlement, subscription or cloud services software code or software carrier.

5. References

- NIST CF - ID.AM-1,2,3
- NIST CF - PR. IP-1,2,3
- NIST SP 800-88
- NIST 1800-5
- ITAM BPL - Vol. 6,7,8,11,12