



Policy Owner: CF - Information Technology (IT)
Approver: CIO - Vittorio Cretella
Contact: Willah Magbanua

Approval Date: November 30, 2021
Effective Date: February 1, 2022
Scope: Global

Business use

IT Asset Management Policy

Intent

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

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

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

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

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:

- **Applications:** Includes Information Systems, Application Platforms, Widely Distributed Software, etc.
Note: The Application Governance Framework (AGF) contains more details and examples.
- **Software:** Includes Commercial End-user software, 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).
- **Hardware:** Includes desktop workstations, laptops, mobile computers, mobile phones, network devices, etc.
Note: The Technology Governance Framework (TGF) contains more details and examples.

This policy also applies to Operational Technology (OT) assets used in Manufacturing, Supply Network, and R&D sites that use traditional IT hardware and software (e.g., servers, workstations, and network devices). The IT and OT Asset Management control requirements are detailed in the respective standards.

Policy Requirements

P&G requires that Application, Software, and Hardware IT Assets be documented, tracked, and managed through their lifecycle (e.g., the changes in their status are promptly reflected in the Corporate Approved Registry). This tracking shall be from registration, installation, maintenance, and until such time that the IT Asset has reached end of life and is properly removed from the P&G environment.

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. Procurement of Information Technology shall route to one of the company-provided channels where standard products and solutions are made available.

Definitions

2LOD (2 nd Line of Defense)	P&G employees in governance roles who are updating policies, standards, and controls, consulting on compliance, and enabling the governance process via tools and procedures.
Corporate Approved Registry	A database, which stores IT Assets' unique identifiers and attributes throughout the lifecycle of the asset. The following are the approved enterprise CMDBs of IT Asset Management: <ul style="list-style-type: none"> • Application and Hardware - ServiceNow CMDB • Software - Flexera
IT Assets	Any P&G-owned hardware, software, or application that is used in the course of business, or anything that connects to the P&G Internal Network. Please go to the Scope section for examples of IT Assets under application, hardware, and software.
Application	An Application/Information System/Business Application is a computer program designed to perform a group of coordinated functions, tasks, or activities for the benefit of the user or business. Typically, there is some code or logic installed, vs. simply presenting information.
Information System	Set of applications, services, information technology assets, or other information-handling components.
Application Governance Framework (AGF)	The framework used to define required fields and data quality characteristics for applications.
Application Platforms	Hosts applications and allows for other applications to be developed and maintained.
Software	IT Asset taking the form of software license, entitlement, subscription, or cloud services software code or software carrier.
Commercial End User Software	These are applications or software products that have all the following characteristics: <ul style="list-style-type: none"> • Centrally managed with identified resources that own full policy compliance (e.g., patching, license, etc.). Note: If there is no central group managing, it must be registered as a "Business Application". • Have risks that are already reviewed, and vendors vetted • Are locally installed or deployed to End User devices (e.g., PCs, mobile) • Commercial off-the-shelf These are typically deployed/available through BigFix PG Apps Center (for PCs) or the P&G AppStore (for mobile).
Hardware	Physical components that are connected to the P&G network (i.e., desktops, laptops, servers, etc.) Please refer to TGF for more details and examples of Hardware IT Assets.

Violating this Policy may result in disciplinary action, consistent with local laws, up to and including termination. Employees affected by this Policy are expected to read and follow it, directing any questions to the Policy Contact.

Technology Governance Framework (TGF)	The framework used to determine classes that require registration, classes that require auto discovery, and the field level requirements by asset class.
Operational Technology Asset (OT Asset)	Operational Technology includes Industrial Control Systems (ICS) and other equipment 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 Asset Management	Process ensuring that all OT Asset with traditional IT are introduced in an approved manner, registered in the centralized system of record, have unique identifier assigned, disposed of/reclaimed or re-deployed in a compliant manner, properly documented, and governed.

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
- ITAM 2LoD Charter: [Link->](#)
- Application Governance Framework: [Link->](#)
- Technology Governance Framework: [Link->](#)
- OT Asset Management Standard/Procedures: [Link->](#)
- SAFE Purchases 3 - Approved Purchasing and Payment Channels: [Link->](#)