Policy Owner: CF - Information Technology (IT)	**Approval Date:** October 31, 2017
Approver: CIO - Javier Polit	**Effective Date:** March 1, 2018
Contact: Michael Williamson	**Scope:** Global

IT Asset Management Policy

1.0 Intent

The purpose of the IT Asset Management Policy (the "Policy") is to protect the company against loss and prevent security incidents, to reduce the company's risk profile to external and internal pressures, to state commitment to legal compliance and to lower cost and improve productivity through more efficient and effective IT Asset Management. IT Asset Management is a foundational policy which helps support other IT Operations and Information Security policies.

The policy ensures that information systems, applications and components on or accessed from P&G's network, and owned by P&G or hosting P&G data, are effectively documented and tracked throughout their life-cycle.

2.0 Scope

This policy applies to all employees and non-employees who are owners, custodians or users of P&G IT Assets, or those entities who manage, deploy, or support P&G IT Assets either internally or externally to the P&G intranet.

3.0 Policy Requirements

P&G requires that all IT Assets must be documented and tracked from the day they enter our network or environment, until after they have been decommissioned.

3.1 IT Asset Acquisition

Hardware and software must be acquired through approved corporate acquisition methods and from approved software distribution channels, adhering to the *"Portable Digital Media Standard"* and the "*IT Services and System Acquisition Policy*".

Hardware and software that is acquired must be on the corporate approved Deployable Technology List (DTL) or have an approved exception granted. The Deployable Technology List is managed by the IT Asset Management 2LOD organization.

3.2 IT Asset Registration

A corporate IT Asset Database must be established, managed, and controlled for an established scope of IT Assets.

All IT Assets must be registered within the corporate IT Asset Database.

The IT Asset Databases can be populated from both manual and automated discovery mechanisms. It must be protected against data loss and alteration by unauthorized persons.

3.3 IT Asset Identification

All IT Assets must have a unique assigned ID number from a centrally managed pool or standard.
The unique assigned ID number must be maintained throughout the lifecycle of the IT Asset.

3.4 IT Asset Disposal

All data stored on IT Assets must be sanitized prior to disposal, as documented in the "*Portable Digital Media Standard"*, so that all data is removed from the IT system.

IT Assets with residual value to the company must be evaluated for reclamation and re-deployment within the company.

Software License 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

IT Asset Databases must provide capability to track IT Assets based on their ID. The databases must contain all information on IT Asset ownership, purpose, classification, version, location/ portability, details of compliance requirements, licensing details, lifecycle status in accordance with the *"IT Configuration Management Policy"*.

Changes to the IT Asset (transfer, usage, lifecycle and disposal) with according dates must be tracked in the IT Asset Database.

Asset ownership information must be maintained to enable governance, escalation, and budget allocation/ re-conciliation purposes and in accordance with Records Retention requirements.

The IT asset owner or manager is responsible in keeping the IT Asset Database up to date at all times.

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. 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.

4.0 Definitions

IT Assets	Any information or operations system, tool, database, application, repository, technical services, hardware and/or device that is used while providing or meeting P&G business activities or business needs, or any technical tool (devices, hardware, etc.) that connects to the P&G internal network directly. For the sake of clarity, these include both Company-owned systems, tools, applications, databases, devices, repositories, technical services , (collectively, the "Tools") and any such Tools procured from third parties. Specific examples of IT Assets include, but are not limited to: - Desktop workstations, laptop and mobile computers - VOIP & Mobile Phones, network cameras, tablets & handheld devices - Printers, copiers, fax machines, scanners, multifunction machines

	- Servers including Virtual Servers, databases including cloud based resources - Application and Middleware Platforms - Firewalls, routers, switches - Specialty equipment (refer to OT detailed guidance on OT equipment for a list of applicable devices) - Network attached Storage devices and cloud storage - Business Applications (including cloud platforms and subscriptions sourced/created internally and/or provisioned by our vendors – including layered applications which may include multiple vendors/tools necessary to meet the business need). For example, this would include the SaaS-based user interface and the IaaS-based cloud storage for the SaaS application, whether operated by the same or independent vendors – e.g., a mobile application with personal data storage on the Azure cloud.) - Software Licenses including entitlements - Personal data collection and storage tools, whether internal or provided by our vendors, such as website CRM and behavioral advertising tools, technical data sharing arrangements, personal data collection tools, etc.
IT Assets Database	A database which stores assets unique identifiers and asset attributes.
Deployable Technology List (DTL)	Deployable technology (hardware, software) means that it is approved for use in P&G and by P&G employees, all deployable technology is documented in the DTL.
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.

5.0 References

- NIST CF - ID.AM-1,2,3
- ISO 38500 - 5.3, 5.4, 5.5
- ISO 27002-2013 - 8.1, 8.2.3, 11.2.7
- IA ITAM BPL - Vol. 6,7,8,11,12