



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 Configuration Management Policy

1.0 Intent

The purpose of the IT Configuration Management Policy (the “Policy”) is to help ensure that all IT Assets are documented with their known interdependencies and relationships so that change management, impact analysis, and compliance activities can be executed. Configuration Management does not include the specific settings or parameters of individual hardware and software.

The policy ensures that Configuration Items and components on P&G’s network are effectively documented and subsequent changes are controlled and tracked.

2.0 Scope

This policy applies to all employees and non-employees who manage, deploy, or support Configuration Items and their changes either internally or externally to the P&G intranet. These individuals are typically titled as configuration, device, or application managers.

3.0 Policy Requirements

P&G requires that all configuration items and their relationships are documented and tracked for the life of the lifecycle of the configuration item.

3.1 Configuration Management

A configuration model must be established which records the relationship between configuration items.

There must be a documented plan that will define the activities, applicable standards and organization for configuration management.

The configuration Management Database must be managed to ensure continued availability and integrity. Repairs and maintenance must be scheduled, communicated, and arranged to minimize business disruption in accordance with the Change Management Policy.

3.2 Configuration Item Management

All Configuration Items must be uniquely identifiable, and their functional and physical characteristics must be documented in a Configuration Management Database. Configuration Baselines must be established.

Configuration Items must be added, modified, replaced in the Configuration Management Database to support the Change Management Policy.

Each Configuration Item must have one or more life cycle states through which it can progress over the course of the configuration item’s life.

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.

3.3 Governance

Formal responsibilities and procedures must be in place to ensure Configuration Item documentation is kept up-to-date and accurate.

Regular checks (Verification and Audit) must be performed, to ensure that the information contained in the Configuration Management Database (CMDB) reflects an accurate representation of the Configuration Items (CIs) as they exist in the live production environment.

4.0 Definitions

Configuration Item	<p>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, and etc...</p> <p>A configuration item does not include the settings, parameters, attributes needed to ensure the running of a system or its hardware.</p>
Configuration Model	<p>A model that defines the structure and attributes that all Configuration Items must follow.</p>
Configuration Baseline	<p>A configuration information formally designated at a specific time during a product’s or product component’s life. Configuration baselines, plus approved changes from those baselines, constitute the current configuration information.</p>
Configuration Management Database	<p>A database used to store attributes of Configuration Items and relationships with other Configuration Items.</p>
System Maintenance	<p>Maintenance comprises activities to correct faults or to ensure effective performance, security and compliance</p>

5.0 References

- NIST CF - PR.IP-1,2,3
- ISO 27002-2013 - 11.2.4
- ITIL Service Asset and Configuration Management

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.