Policy Owner:	**Octavio Flores**	**Effective date:**	**January 1, 2019**
Approver:	**Javier Polit**	**Scope:**	**Global**
Contact:	**Sarah Ackerman**		

Information Security Governance Policy

1.0 Intent

The intent of the Information Security Governance Policy ("the policy") is to establish requirements for the governance of information security, and therefore to ensure that P&G's overall approach to information security supports high standards of governance.

2.0 Scope

This policy and related standards apply to all organizations and individuals, including third party partners, who deploy, manage, or support P&G IT assets (applications, data, platforms, software, networks and information systems). This policy also applies to OT assets (Operational Technology used in Manufacturing and Supply Network sites) that use traditional IT hardware and software (e.g. servers, workstations, network devices). Other OT assets (e.g. PLCs, robots) must reside on an Information Security approved segment of the P&G network; refer to the applicable OT policy.

All aspects of this policy are effective upon the date listed above except as noted in specific sections within this policy or supporting standards.

3.0 Applicability

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.

4.0 Policy Requirements

4.1 Security Governance Approach

P&G requires the establishment of a framework for information security governance, and commitment demonstrated by the company's Board of Directors. Control over information security must be provided by a high-level group including both business and technical representatives as established by ESLT, and managed by the CISO.

4.2 Security Governance Components

An information security strategy must be maintained that is aligned with P&G's strategic objectives. P&G requires that processes are implemented to measure the value delivered by information security initiatives and report the results to all stakeholders. P&G requires that a consistent and structured

information security assurance program is implemented and assessed annually by an external third party in order to ensure the program remains current based on industry best practice.

5.0 Definitions

CISO: Chief Information Security Officer.

Information Security Approved Network Segment: A portion of the P&G network utilizing a method for isolating a system from other systems or networks; for example, air gapped, NOC/SOC managed reverse proxy, or other approved Information Security segmentation.

ESLT: Enterprise Security Leadership Team.

The P&G Network: The network infrastructure that is accessible from within the physically secured areas of Company sites.

NOC/SOC: The P&G Network Operations Center and Security Operations Center.

6.0 References

- Appropriate Use Policy
- IT Governance Policy (not yet published)

Related Standards:

- Security Governance Approach
  - Information Security Governance Framework
  - Information Security Direction and Strategy
- Security Governance Components
  - Information Security Assurance
  - Stakeholder Value Delivery
- People Management
  - Human Resource Security
  - Security Awareness and Education