Policy Owner:	John Toney	**Effective date:**	January 1, 2019
Approver:	Javier Polit	**Scope:**	Global
Contact:	John Toney		

Security Monitoring and Improvement Policy

1.0 Intent

The intent of the Security Monitoring and Improvement Policy is to establish requirement for conducting thorough, independent and regular audits of the security status of in-scope environments (critical business environments, processes, applications, and supporting systems/networks). These audits monitor information risks; compliance with the security-related elements of legal, regulatory and contractual requirements; and the overall information security condition of the company on a regular basis and their results are reported to specific audiences, such as executive management.

The purpose of these audits is to ensure that:

- Required security controls have been implemented to provide a sufficient level of protection to mitigate identified information risks and
- Executive management can make informed decisions about information security and risk management.

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

P&G requires security monitoring through use of both security audits and performance assessments.

4.1 Security Audit

P&G requires that the information security status of in-scope environments be subject to thorough, independent and regular security audits.

P&G requires that security audits of in-scope environments are subject to thorough planning, which includes identifying risks, determining audit objectives, defining the approach and scope of security audits, and preparing a security audit plan.

P&G requires that security audit fieldwork conducted for in-scope environments includes collecting relevant background material, performing security audit tests and recording the results of the tests.

P&G requires that the results of security audits of target environments are documented and reported to stakeholders.

P&G requires that actions to address security audit findings be incorporated into a program of work and monitored continuously.

4.2 Security Performance

P&G requires information security performance be monitored regularly and reported to specific audiences, such as executive management and the audit committee.

P&G requires that reports relating to information risk be produced and presented to executive management and the audit committee management on a regular basis.

P&G requires that a security compliance management process be established, which comprises information security controls derived from regulatory and legal drivers and contracts.

5.0 Definitions

Security Audit: An independent review of a system (e.g., application, infrastructure, device, platform) to evaluate how well it protects P&G information and/or complies with legislation, regulations, contracts, industry standards, or company policies. This includes, but is not limited to, monitoring activities led by the information security organization (e.g., penetration testing team, network monitoring team), the internal audit organization, and the external audit firm.

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.

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

- Security Audit Standard
- Security Performance Standard