Policy Owner: William Fryberger
Policy Approver: Javier Polit
Policy Contact: William Fryberger

Scope: Global
Approval Date: November 29, 2018
Effective Date: January 1, 2019

Threat and Incident Management Policy

Intent

The intent of the Threat and Incident Management Policy is to establish a comprehensive and approved Information Security Incident management framework that includes policy, access to Cyber Incident investigators and forensic experts; threat related information, and technical investigation tools. The framework is supported by a process for the identification, response, recovery and post-implementation review of Information Security Incidents. The framework and process will protect information assets by managing threats and vulnerabilities associated with business applications, systems and networks.

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.

Policy Requirements

1. Cyber Security Resilience

   P&G requires the establishment of a process to identify and remediate technical vulnerabilities in business applications, systems, equipment and devices.

   P&G requires that security-related events are recorded in logs, stored centrally, and protected against unauthorized access/change. Security-related event logs must be reviewed and analyzed on a regular basis, by security specialists, using a combination of automated and manual methods.

   P&G requires the establishment of a threat intelligence capability, supported by an intelligence cycle and analytical tools.

2. Security Incident Management

   P&G requires that an information security incident management framework and process be established and supported by relevant individuals with the information and tools required to identify and resolve information security incidents.

   P&G requires that information security incidents are identified, responded to, recovered from, and followed up using an information security incident management process, which may include shutting down systems or taking them offline as required based on the nature and severity of the incident.

P&G requires that emergency fixes to business information, business applications and technical infrastructure are tested, reviewed, and applied quickly and effectively, in accordance with documented standards/procedures.

P&G requires that a process be established for addressing information security incidents or other events (e.g., e-discovery requests) that require forensic investigation.

Definitions

Forensic Investigations	The application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.
Information Security Approved Network Segment	The application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.
NOC / SOC	The P&G Network Operations Center and Security Operations Center.
P&G Network	The network infrastructure that is accessible from within the physically secured areas of Company sites.

References

- Technical Vulnerability Management Standard
- Security Event Logging and Monitoring Standard
- Cyber Security Resilience Standard
- Digital Forensic Investigations Standard
- Security Incident Management Standard