

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

## Threat and Incident Management Policy

### 1.0 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.

### 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 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.

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.

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

## 4.2 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.

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.

## 5.0 Definitions

**Event:** An indication of a potential compromise of P&G IT resources or electronic data/information. Events have the potential to escalate into Incidents.

**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.

**Incident:** Event that violates the law or company policy/standard; related to P&G information/systems; has or could compromise the confidentiality integrity or availability of P&G information; caused through intentional or unintentional means.

**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

- [Technical Vulnerability Management Standard](#)
- [Security Event Logging Standard](#)
- [Cyber Security Resilience Standard](#)
- [Security Incident Management standard](#)