Policy Owner: William Fryberger
Policy Approver: Vittorio Cretella
Policy Contact: William Fryberger

Scope: Global
Approval Date: May 1, 2020
Effective Date: July 1, 2020

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). For other OT assets (e.g. PLCs, robots that must reside on an Information Security approved segment of the P&G network); refer to the applicable OT policy.

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. Data Loss Prevention

   P&G requires that Data Loss Prevention mechanisms must be applied to information systems and networks that process, store or transmit information, to identify information that may be at risk of unauthorized disclosure and detect if information is disclosed to unauthorized individuals or systems.

3. 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 on 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

Data Loss Prevention	Data Loss Prevention (sometimes referred to as information leakage protection) typically involves technical solutions that scan/monitor systems and networks to prevent and detect the (often accidental) leakage (i.e., unintended disclosure) of sensitive information. Sensitive information that is at risk of leakage or is leaked often includes shared and unencrypted content such as word-processed documents, presentation files and spreadsheets that could leave an organization via many different points or channels (e.g., via email, instant messaging, Internet browsing or on portable storage devices).
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 (internal network)	The network to which access (on any layer of OSI model) is exclusively authorized, provisioned and secured by P&G or parties authorized by P&G and therefore is not shared with any other party unauthorized by P&G.

References

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