Policy Owner: Alok Sinhasan
Policy Approver: Vittorio Cretella
Policy Contact: Alok Sinhasan

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

Technical Security Management Policy

Intent

The intent of the Technical Security Management Policy (the "Policy") is to build a sound technical security infrastructure, applying Security Architecture Principles and integrating technical security solutions in a consistent manner across the organization to help protect the confidentiality, availability, and integrity of information.

Scope

This policy and related standards apply to all organizations, 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 thatmust reside on an Information Security approved segment of the P&G network), refer to the applicable OT policy.

Policy Requirements

1. Security Architecture
   P&G requires that a security architecture be established to help manage the complexity of providing information security at scale throughout the organization and to implement consistent, simple-to-use security functionality across multiple business applications and systems throughout the organization.

2. Malware Protection
   P&G requires that activities be performed to make users aware of the risks from malware, and to specify the actions required to minimize those risks. This ensures all relevant individuals understand the key elements of malware protection, why it is needed, and how to help to keep the impact of malware to a minimum. P&G requires that systems throughout the organization be safeguarded against all forms of malware by maintaining up-to-date malware protection software, which is supported by effective procedures for managing malware-related security incidents to protect the organization against malware attacks and ensure malware infections can be addressed within defined timescales.

3. Intrusion Detection
   P&G requires that intrusion detection mechanisms be applied to all systems and networks, to identify suspected or actual malicious attacks and enable the organization to respond before serious damage is done.

4. Digital Rights Management
   P&G requires that information or software that is accessed and used outside of the control of the organization should be protected using digital rights management (DRM) to ensure that the access to and processing of data is restricted to specific functions by a limited number of authorized individuals.

5. Encryption Solutions
   P&G requires that encryption solutions be subject to approval, documented and applied throughout the organization to protect the confidentiality of information, preserve the integrity of information and confirm the identity of the originator of transactions or communications.

6. Encryption Key Management
   P&G requires that encryption keys be managed tightly, in accordance with documented standards/procedures, and protected against unauthorized access or destruction to ensure that cryptographic keys are not compromised (e.g. through loss, corruption, or disclosure), thereby exposing information to attack.
7. Public Key Infrastructure
   P&G requires the use of an Information Security approved public key infrastructure (PKI), one or more Certification Authorities (CAs) and Registration Authorities (RAs) be established and protected to ensure that the PKI operates as intended, is available when required, provides adequate protection of related cryptographic keys and can be recovered in the event of an emergency.
8. Business Application Security
   P&G requires business applications align with the organization's security architecture, technical security infrastructure, standards, guidelines to protect the information they process.
9. Cloud Security
   P&G requires secure cloud applications. The Cloud Security Standard defines the controls necessary for provisioning cloud environments and completion of iRisk to obtain production approval after an Architecture Review Board approval and verification of security controls in line with the application BIA criticality.

Definitions

Certification Authority (CA)	Comprises the people, processes and tools that are responsible for the creation, issue and management of public key certificates that are used within a PKI.
Information Security Approved Network Segment	A portion of the P&G network utilizing a method for isolating a system from other systems or networks. Approved methods are air gapped and NOC/SOC managed reverse proxy.
Malware	Typically includes computer viruses, worms, Trojan horses, spyware, rootkits, botnet software, ransomware, and malicious mobile code (e.g., malicious executable code, often in the form of Java applets, ActiveX, JavaScript, or VBScript, that has been written deliberately to perform unauthorized functions).
NOC / SOC	The P&G Network Operations Center and Security Operations Center.
Registration Authority (RA)	Typically represents the interface between a CA and users of the PKI. The RA is often a combination of technology and people responsible for functions such as verifying the identity of PKI users, registering users, providing status information about certificates, handling digital certificate requests and revoking certificates.
Security Architecture Principles	Design principles that are fundamental to security and should be followed during the development and use of a security architecture, when reviewing and approving IT projects, and when implementing security controls.
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

- Application Program Interface Security Standard
- Business Application Security Standard
- Cloud Security Standard
- Encryption Key Management Standard
- Encryption Standard
- Internet Facing Websites and Mobile Applications Standard
- Intrusion Detection Standard
- Malware Protection Standard
- Security Architecture Principles
- Secure Coding Guideline
- Technical Security Standards