Policy Owner: Alok Sinhasan
Policy Approver: Javier Polit
Policy Contact: Alok Sinhasan

Scope: Global
Approval Date: July 11, 2018
Effective Date: October 1, 2018

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) must 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 must be established to help manage the complexity of providing information security at scale throughout the organization 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 are performed to make users aware of the risks from Malware, and to specify the actions required to minimize those risks to ensure all relevant individuals understand the key elements of Malware protection, why it is needed, and help to keep the impact of Malware to a minimum. P&G requires that systems throughout the organization must 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. Identity and Access Management
   P&G requires that identity and access management arrangements must be established to provide effective and consistent user administration, identification, and authentication and access control mechanisms throughout the organization to restrict system access to authorized users and ensure the integrity of data. See User Authentication Standard for further details.
4. Intrusion Detection
   P&G requires that intrusion detection mechanisms must 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.

5. 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.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. Technical Vulnerability Management
    P&G requires business applications to maintain support to address security vulnerabilities on all applications. Addressing these security vulnerabilities is critical to maintaining a secure enterprise architecture. The Technical Vulnerability Management Standard details the controls for addressing vulnerabilities.
12. Network Security Architecture
    P&G requires a secure networking architecture. The IT Network and Communication Policy addresses the policy and standards necessary for a secure network. This policy requires the creation and the use of technical security standards for all networking equipment.
13. 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 go-live 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.
Data Loss Prevention	Data Loss Prevention (sometimes referred to is information leakage protection) typically involves the implementation of 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).
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	Security Architecture Principles (sometimes referred to as design principles) 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.
The P&G Network	The network infrastructure that is accessible from within the physically secured areas of Company sites.

References

- Application Program Interface Security Standard
- Business Application Security Standard
- Cloud Security Standard
- Consumer Websites Standard
- Encryption Key Management Standard
- Encryption Standard
- Intrusion Detection Standard
- Malware Protection Standard
- Security Architecture Principles
- Secure Coding Guideline
- Technical Security Standards