Policy Owner: (-)
Policy Approver: (-)
Policy Contact: (-)

Scope: Global
Approval Date: October 4, 2019
Effective Date: December 1, 2019

System Access Policy

Intent

The intent of the System Access Policy is to protect business information within systems (Business applications, mobile devices, systems and networks). This policy requires that individuals are authorized for specific business purposes by requiring them to be granted access privileges in line with their role. Individuals must be authenticated use access control mechanisms (e.g. password, token, biometric) and subject to a rigorous sign-on process before being provided with approved levels of access.

This policy also protects the business information that provides access to partners, customers, contractors, and consumers by performing information risk assessment to determine the information security requirements and implementing security arrangements in contracts and agreements.

This policy will provide assurance that:

1. only authorized users can gain access to information, business applications, systems, computing devices and networks necessary for their job roles,
2. access privileges are limited based on need-to-know principle,
3. there is appropriate segregation of duties,
4. high risk transactions and information are protected with strong controls
5. employees, customers, partners, contractors, and consumers protect related critical and sensitive information according to agreed contractual obligations,
6. information is protected based upon the business risk and Information Asset Classification.

Policy Requirements

P&G requires that only authorized individuals gain access to business applications, information systems, networks ad computing devices. P&G requires that individual accountability is assured and that individuals have the access privileges that are sufficient to perform their duties but do not permit them to exceed their authority.

Definitions

None	