Policy Owner: CF IT - Information Technology (IT)	**Effective date:** July 1, 2021
Approver: Vittorio Cretella, Chief Information Officer	**Scope:** Global
Contact: Lauren Benjamin	

Network and Communications Policy

1.0 Intent

The intent of the Network and Communications Policy is to ensure that the P&G wired, wireless, and voice networks are managed in such a way that the network will remain fit for purpose and fit for use while ensuring that the networks are secure and supportable.

2.0 Scope

This policy and related standards apply to all employees and non-employees deploying and/or supporting the global network, network infrastructure devices, and network applications via the Network Services team. Only devices and networks managed by the Network Operations Center are in scope for this policy.

3.0 Policy Requirements

P&G requires network performance monitoring be done for the purposes of ensuring that WAN bandwidth is appropriately provisioned.

P&G requires that device configurations are secure, validated, and documented.

P&G requires that network device operating system versions be compliant with the P&G recommended standard.

P&G requires that global and regional datacenters are designed and deployed to be highly available and allow for services to continue during events of prolonged unavailability.

P&G requires that network design segments traffic by distinct groups of users or services via firewalls.

P&G requires that any connection to the internal P&G network from outside of the internal P&G network, including External Business Partner connections, is managed to ensure the connection is appropriate, authorized, and approved. Additionally, all traffic leaving or entering the internal P&G network must be secured.

P&G requires that VPN access is limited to people with a valid P&G Active Directory account.

P&G requires the use of firewalls to recognize and eliminate unauthorized traffic from the internal P&G network. To ensure this is maintain, all firewall rules must be authorized and regularly reviewed to ensure the traffic leaving or entering the internal P&G network is necessary to support current business needs.

P&G requires appropriate DNS logging to capture specific outbound network connections.

P&G requires that physical access to global and regional data centers is limited to authorized staff.

P&G requires protection for internal VOIP traffic. Additionally, voice traffic to the Contact Centers is protected.

P&G requires wireless connectivity to the internal P&G network secured using layers of access control. Additionally, wireless access for non-P&G devices and people must be approved by a P&G employee. Guest wireless has no access to the P&G internal network.

4.0 Allowed Endpoint Devices on the Network

All endpoint devices (i.e. laptops, desktops, mobile devices, printers, etc.) connecting to the P&G Network should follow the IT Asset Management Standard for Hardware found here. These are maintained by the IT Asset Management team.

References:

Network and Communications Policy Page