

Network Access Control Policy

Reference: PCI POL 7.2

DocumentKits Issue No: 1.1

Organisation Issue No:

DocumentKits Issue Date: 29/06/2020

Organisation Issue Date:

1. Scope

Organisation Name protects its networked services in line with its [Access Control Policy](#) from unauthorised access.

2. Responsibilities

2.1 The System Administrator is responsible for the configuration and maintenance of Organisation Name's network access controls.

2.2 The Information Security Manager is responsible for approving configuration changes to network access control mechanisms.

3. Requirements

3.1 Organisation Name ensures that
"insert brief details of appropriate interfaces"

are in place between Organisation Name's network and
"external third party network"

and the Internet.

3.2

"Insert details of appropriate"

authentication mechanisms are applied for Users and equipment and that control of user access to information services is enforced.

3.3 The networks and network services, and their access rights, which are allowed to be accessed are detailed
"where?"

3.4 Authorisation procedures are used to ensure that Users only have access to those services and networks which are appropriate for their role and to their business needs.

3.5 Management controls and procedures are used to protect access to network connections and network services.

"Identify those controls and procedures here."

3.6 There are specific procedures for controlling access to network services.

3.7 As a minimum, the following security steps are required in respect of wireless technology, modems and routers used in respect of any part of an organisational network on which cardholder data is processed:

3.7.1 Such equipment may only be purchased from approved vendors and in line with approved types and models.

3.7.2 Explicit management authorisation from the Head of IT (CIO) is required prior to deployment of all such equipment.

3.7.3 User authentication is required before any user or service can connect to the network.

3.7.4 For every such device, there must be an approved list of Users and services that have authorised access to the device, and this list must be maintained.

3.7.5 Each such device must be clearly labelled with contact details and name of the Owner of the device, and its purpose must be also be marked on it.

3.7.6 Each such device may only be used for the purposes and in the location for which authorisation was obtained.

3.7.7 Remote-access technologies must automatically disconnect after a period of inactivity.

"Specify length"

<< 3.7.8 – 3.1.11 removed for sample purposes >>

Document Owner and Approval

The Network Manager is the owner of this document and is responsible for keeping it up to date.

The current version of this document is available to

"Specify which members of staff this document is intended for"

and is published

"Describe the location(s) - electronic and physical - where this document is available"

Its approval status can be viewed in the [Master List of Document Approval](#).