

Network Configuration Standard

# Overview/Purpose

Network equipment plays an important role in protecting the network and data assets.

# Scope

This standard is intended to define rules for network equipment configuration, configuration modification, and documenting changes.   
*{This document requires modification to include specific network equipment used by utility such as private radio or fiber network}*

# Standard

## Network Documentation

**<Utility Name>** maintains a current network diagram which identifies all physical connections. The network diagram will be kept updated by the network administrator to reflect changes in the network, with a date indicating when the most recent update was made.

## Firewalls and routers

* Firewalls must be implemented between each internet connection and any demilitarized zone (DMZ), and the internal company network.
* A network diagram detailing all the inbound and outbound connections must be maintained and reviewed every 6 months.
* A firewall and router configuration document must be maintained which includes a documented list of services, protocols, and ports allowed, including a business justification.
* Firewall and router configurations must restrict connections between untrusted networks and any systems in the cardholder data environment (CDE).
* Stateful firewall technology must be implemented where the Internet enters the CDE to mitigate known and on-going threats. Firewalls must also be implemented to protect local network segments and the IT resources that attach to those segments.
* All inbound and outbound traffic must be restricted to that which is required for the CDE.
* All inbound network traffic should be blocked by default, unless explicitly allowed. Any rules set to allow inbound traffic must be documented, including the appropriate justification.
* All outbound traffic has to be authorized by management. Any rules to allow outbound traffic must be documented.
* **<Utility Name>** will deploy firewalls between any wireless networks and the CDE.
* **<Utility Name>** will quarantine wireless users into a DMZ, where they will be authenticated and firewalled as if they were coming in from the Internet.
* Disclosure of private IP addresses to external entities must be authorized.
* A topology of the firewall environment must be documented, and must be updated in accordance to the changes in the network.
* The firewall rules will be reviewed every 6 months to ensure that they are consistent with the rules previously approved.
* No direct connections from Internet to CDE are permitted.   
  All traffic must traverse through a firewall.
* Firewall configuration changes are conducted according to *Firewall Configuration**Procedure* and documented in *Firewall Configuration Change Form*.
* The *Firewall Rules Design Form* is used for:
  + Initial design of firewall rules
  + Documenting business requirements for allowing specific traffic

## Wireless devices

### Office Wireless Device Requirements

All office wireless infrastructure devices must adhere to the following:

* Installation or use of any wireless device or wireless network intended to be used to connect to any of the networks or environments is prohibited, except as specifically authorized by IT Department.
* Stateful packet inspection firewalls are to be used to block wireless traffic from entering the networks. Firewall connected to wireless network are must use IDS/IPS.
* VLANs are not used for segmentation with MAC address filters for segmenting wireless networks.
* A wireless analyzer (or a wireless IDS/IPS) should be used at least every 6 months to detect unauthorized/rogue wireless devices that could be connected to the network at all locations.
* Automatic alerts and containment mechanisms are to be used on the wireless IPS to eliminate rogue and unauthorized wireless connections into the network.
* If any violation of this standard is discovered as a result of the normal audit processes, the IT Manager has the authorization to remove the offending device immediately.
* If the need arises to use wireless technology, it should be approved through the *IT**Change Request Procedure,* with the following wireless standards to be applied:
  1. Default SNMP community strings and passwords, passphrases, encryption keys, and other security-related vendor defaults (if applicable) should be changed immediately after the installation of the device. Any such settings should be changed when a person with knowledge of them leaves the company
  2. The firmware on each wireless devices must be updated promptly following release by the vendor.
  3. The firmware on the wireless devices must support strong encryption for authentication and transmission over wireless networks.
  4. Wireless networks must implement industry best practices (IEEE 802.11i) and strong encryption for authentication and transmission of cardholder data.

### Home Wireless Device Requirements

All home wireless infrastructure devices that provide direct access to a network, such as those behind Enterprise Teleworker (ECT) or hardware VPN, must use the following settings:

* Enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS;
* When enabling WPA-PSK, a complex shared secret key (at least 20 characters) must be used on the wireless client and the wireless access point;
* Disable broadcast of SSID;
* Change the default SSID name;
* Change the default login and password.

# Compliance

## Compliance Measurement

The <**person or group responsible for policy**> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the <**person or group responsible for policy**> in advance.

## Non-compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with **<Utility Name>** HR policies.

# Related Standards, Policies, and Processes

* PCI DSS Requirements   
  (<https://www.pcisecuritystandards.org/document_library>)
  + (Requirement 1.1.2)
  + (Requirement 1.1.4)
  + (Requirement 1.1.6)

# Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible | Accountable | Consulted | Informed |
| CIO | **CEO/GM** | **IT Department** |  |

*[Explanatory Note: <Utility Name> should feel free to alter section to reflect the specific responsibility requirement determined by <Utility Name> management.]*

# Approval

\_

<**Insert title of approver**> Date

# Revision History

|  |  |  |
| --- | --- | --- |
| Date of Change(s) | Revised by | Summary of Change(s) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |