Wireless
Version 3.2

1. Purpose

1.1. The purpose of this policy is to define the requirements for all wireless routers and devices.

1.2. The intent of this policy is to prevent unauthorized access to the network and specifically to the Card Data Environment (CDE). The CDE is any computer or device that has any role in processing, transmitting or storing credit card information

1.3. These requirements are designed to minimize exposure to the company from the loss of credit card information and comply with the Payment Card Industry Data Security Standard (PCI).

2. Scope and Responsibility

2.1. This policy is implemented by the Information Department or personnel responsible for information technology or security.

3. Policy

3.1. For all hardware and software the password shall be changed from the original vendor default password to a strong password in accordance with the company's requirements for administrative passwords.

3.2. Wireless Routers

3.2.1. Wireless routers shall use WPA encryption.

3.2.2. Wireless router rule sets shall be maintained in accordance with the Firewall Policy.

3.2.3. Network name should not be broadcast, prevent broadcasting by setting 'Broadcast SSID' to OFF or choosing the "private network" setting.

Copyright 2008-2016 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

3.2.4. Wireless access must be restricted to authorized devices only by specific MAC address.

3.2.5. Wireless routers, access points and handheld devices must be secured so they are accessible only to authorized individuals.

3.2.6. For Wireless devices connected to the cardholder environment or transmitting cardholder data defaults shall be changed as follows:

3.2.6.1. Encryption keys shall be changed from default at installation and anytime someone with knowledge of the keys leaves the company.

3.2.6.2. Simple Network Management Protocol (SNMP) community strings shall be changed on all wireless devices.

3.2.6.3. Default passwords/passphrases on access points shall be changed.

3.2.6.4. Firmware shall be updated on all wireless devices to support strong encryption for transmission of cardholder data.

3.2.6.5. Any other applicable security related wireless defaults shall be changed.

3.2.7. A wireless network scan shall be performed monthly to detect unauthorized wireless devices. A physical inspection of all the device on the network to make sure there are no unauthorized wireless devices is acceptable to meet this requirement.

3.2.7.1. If an unauthorized wireless device is discovered, activate the Incident Response plan shall be activated immediately.

Copyright 2008-2016 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

3.2.8. There shall be a firewall between the perimeters of the cardholder environment and the wireless network that denies or controls traffic to the cardholder environment to only the traffic necessary for business.

4. Enforcement

4.1. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.2. External service providers found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

5. Definitions

5.1. *SSID* - (Service Set IDentifier) The name assigned to a wireless Wi-Fi network. All devices must use this same, case-sensitive name to communicate. The SSID may not be broadcast.

5.2. *WEP* – Wireless Equivalent Privacy or Wireless Encryption Protocol a technology that was once considered secure, but with the advent of faster computers is easily compromised. Must not be used under any circumstances.

5.3. *WPA* – Wireless Protected Access the best currently available wireless encryption technology

Copyright 2008-2016 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.