Network Security Policy
Version 3.2

Implementation Notes

IMPLEMENT THIS POLICY FIRST - IT ESTABLISHES THE BASIS FOR FOLLOWING THE PRIORITIZED APPROACH TO PCI IMPLEMENTATION.

A full explanation of the prioritized approach is located on the PCI Security Standards Council at https://www.pcisecuritystandards.org/security_standards/documents.php titled "Prioritized Approach for PCI DSS Version 3.2"

This policy provides only the basic requirements that apply to all networks.

It will be necessary to write implementing procedures that are specific to your network environment and your organization. Depending on the size and complexity of your network you will have to write procedures and/or additional policies to control your network.

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.

Network Security Policy
Version 3.2

1. Purpose

1.1. The purpose of this policy is to define standards to be met for all equipment owned and/or operated by the company located inside and outside the corporate Internet firewalls.

1.2. This policy establishes the requirement for establishing and maintaining a network diagram.

1.3. This policy specifies vulnerability and penetration scanning requirements.

1.4. These standards 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).

1.5. Devices that are Internet facing and outside the Company firewall are considered part of the "de-militarized zone" (DMZ) and are subject to this policy. These devices (network and host) are particularly vulnerable to attack from the Internet as they reside outside the corporate firewalls.

2. Scope and Responsibility

2.1. The Information Department or personnel as identified on the Errata Sheet to this procedure shall be responsible for implementing this policy.

2.2. All equipment or devices deployed in a DMZ owned and/or operated by the company (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by the company must conform to this policy.

2.3. All internal network computers and equipment shall conform to this policy.

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.

2.4. This policy also covers any host device outsourced or hosted at external/third-party service providers, if that equipment resides in the "the company" domain or is owned by others but appears to be part of the company. An example of this is a server operated by a hosting company.

3. Policy

Note – All components, systems, applications, security systems, terminals etc., that use passwords and/or accounts, shall have the passwords changed to strong passwords or phrases and default accounts shall be removed, disabled or documented and their use justified and specifically authorized.

3.1. Network Diagram

3.1.1. Construct a network diagram that identifies ALL network connections to the cardholder environment and includes all processes and machines that store, process or transmit cardholder data.

3.1.2. Ensure the diagram includes hosted environments that appear to be part of the corporate environment.

3.1.3. Establish a process and procedure to update the diagram and review the impact of changes prior to making changes.

3.1.4. The network diagram shall be consistent with the company firewall configuration standards.

3.1.5. Establish a review process that ensures the network diagram is kept current.

3.2. Firewall Configuration – this section contains the requirements for developing configuration standards. The

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.

company shall develop documentation, as needed, to address the specific configuration standard for each firewall.

Firewall and router configuration rules shall be implemented and remain in force at all times.

3.2.1. Router configurations shall be secured to protect them from unauthorized access and synchronized.

3.2.2. A list of ports and services used shall be documented in Appendix C Ports and Services List.

3.2.3. Demilitarized Zone (DMZ)

3.2.3.1. There shall be a firewall present at each connection to the Internet and at any connection between the cardholder environment and the DMZ.

3.2.3.2. The DMZ configuration shall take into account the following minimum requirements:

3.2.3.2.1. Inbound traffic shall be limited only to system components specifically authorized publicly accessible services, protocols and ports.

3.2.3.2.2. Inbound traffic shall be limited to IP addresses within the DMZ.

3.2.3.2.3. Direct connections between the cardholder data environment and the internet shall be prohibited.

3.2.3.2.4. Internal addresses shall not pass from the company network into the DMZ

3.2.3.2.5. ALL outbound data from the cardholder environment shall be specifically authorized.

3.2.4. For each firewall the configuration shall include:

3.2.4.1. The password must be changed from the original vendor default password to a strong password in

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.

accordance with the company's requirements for administrative passwords.

3.2.4.2. Disclosure of internal IP addresses and routing information to the Internet shall be prohibited unless specifically authorized.

3.2.4.3. All firewalls shall be set for:

3.2.4.3.1. Network Address Translation (NAT)

3.2.4.3.2. Stateful packet inspection

3.2.4.3.3. Domain blocking

3.2.4.3.4. Port Blocking

3.2.4.3.5. Intrusion detection and blocking shall be turned ON and notifications shall be turned ON

3.2.4.3.6. Anti-spoofing measures shall be implemented:

3.2.4.3.6.1. To detect and block forged source IP addresses from entering the network

3.2.4.3.6.2. To detect and block internal IP addresses from entering the network

3.2.4.3.7. Any other methods of obscuring IP addresses as needed

3.2.4.4. If the router, gateway or other device is not capable of ALL of these items, it must be replaced with one that is.

3.2.5. Firewall requirements for System Components that Store Cardholder Data

3.2.5.1. Each file server containing PAN data shall have its own firewall.

3.2.5.2. There shall be only one function for any server storing cardholder data.

3.2.5.3. System components storing cardholder data shall be in an internal network zone that is segregated from the DMZ and any untrusted network.

3.2.5.4. Inbound and outbound traffic to the cardholder data environment shall be restricted to only that necessary for the cardholder data environment. Authorization shall be documented in Appendix D.

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.

3.2.5.5. All traffic not specifically authorized shall be denied.

3.2.5.6. There shall be a perimeter firewall installed between the cardholder environment and any wireless network. These firewalls shall be configured in accordance with the standards for wired firewalls and shall permit only authorized traffic between the wireless network and the cardholder data environment.

3.2.5.7. Insecure services, ports and protocols shall be specifically allowed and documented and implemented.

This list includes, but is not limited to: FTP, Telnet, POP3, IMAP and SNMP v1 and v2.

3.2.5.8. SSL and early versions of TLS shall not be used unless there is a written plan to secure their use that includes a migration plan that discontinues them by 6/30/2018.

3.2.5.8.1. The name of the policy <Company Name> Network Security Policy.

3.2.5.8.2. The date, before 6/30/2018, the migration will be complete.

3.2.5.8.3. A confirmation that this is the formal policy of the company.

3.2.5.9. Change or disable any default Simple Network Management Protocol (SNMP) community strings.

3.2.5.10. Wireless Encryption keys shall be changed in accordance with the Encryption policy.

3.2.6. Before using any firewall ensure it is capable of and set to:

3.2.6.1. Block both inbound AND outbound traffic

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.

3.2.6.2. Log intrusion attempts
3.2.6.3. Notify administrators of intrusion attempts

3.3. Changes to Firewalls

3.3.1. The firewall settings shall be documented in Appendix A of this policy, Firewall Configuration.

3.3.2. Changes to company firewalls shall be approved, tested and logged in Appendix B Firewall Change Log.

3.3.3. Firewall rule sets and configuration shall be reviewed every six (6) months and documented in Appendix A.

3.3.4. Firewall configurations shall be synchronized on all routers and firewalls.

3.3.5. Router configuration files shall be accessible only to authorized individuals.

3.4. Mobile/Personal Computers

3.4.1. Mobile computers or employee personal computers that can access the company network shall have a firewall installed and turned on at all times.

3.4.2. Mobile computer firewalls shall conform to the company firewall configuration standards in this policy.

3.4.3. Mobile/personal computers firewall configurations shall not be alterable by the user.

3.5. Unauthorized wireless connections

3.5.1. Unauthorized wireless connections shall be detected and identified by at least one of the following methods:

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.

3.5.1.1. Deployment of Intrusion Detection/Prevention software. Software shall be capable of and set to generate alerts.

3.5.1.2. Physical inspection of network components for unauthorized devices.

3.5.1.3. Any inspection method shall detect WLAN cards, portable wireless devices connected to system components and/or network ports and network devices.

3.5.1.4. Automated detection or prevention software or processes shall run continuously. Physical inspections or manual processes shall be performed quarterly.

3.5.1.5. Any unauthorized wireless device detected or discovered shall be disabled and removed according to company procedures

3.5.1.6. Discovery of an unauthorized wireless device shall be considered an intrusion incident and the Incident Response Plan shall be activated

3.6. Scanning shall be performed on a timely basis, as indicated in this section, and after any significant system change, including operating system upgrades, infrastructure, software architecture (e.g. adding a sub-net), web server additions, etc.

3.6.1. Internal penetration testing shall be performed quarterly by a qualified individual or vendor who has organizational independence from the entity or department that has responsibility for the network.

3.6.1.1. Penetration tests shall include network layer penetration tests.

3.6.1.2. Vulnerabilities scoring 4.0 or above on the Common Vulnerability Scoring system (CVSS), found at http://nvd.nist.gov/ shall be resolved.

3.6.1.3. Rescans shall be performed until a report can be generated documenting the successful results of the scan.

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.

3.6.2. External penetration testing shall be performed annually by a qualified individual or vendor who has organizational independence from the entity or department that has responsibility for the network.

3.6.2.1. Penetration tests shall include network layer penetration tests.

3.6.2.2. Vulnerabilities scoring 4.0 or above on the Common Vulnerability Scoring system (CVSS), found at http://nvd.nist.gov/ shall be resolved.

3.6.2.3. Retests shall be performed until a report can be generated documenting the successful results of the scan.

3.6.3. Internal vulnerability scanning shall be performed quarterly by a qualified individual who has organizational independence from the entity or department that has responsibility for the network.

3.6.3.1. Vulnerabilities identified shall be resolved until a passing result is obtained. Vulnerabilities scoring 4.0 or above on the Common Vulnerability Scoring system (CVSS), found at http://nvd.nist.gov/ shall be resolved.

3.6.3.2. The final report of a passing scan shall be retained as evidence of meeting this requirement.

3.6.4. External vulnerability scanning shall be performed quarterly by an Approved Scan Vendor (ASV) listed by the PCI Security Standards Council at https://www.pcisecuritystandards.org/

3.6.4.1. Vulnerabilities identified shall be resolved until a passing result is obtained.

3.6.4.2. The final report of a passing scan shall be retained as evidence of meeting this requirement.

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.

4. Enforcement

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

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

5. Records

5.1. Errata Sheet

5.2. Appendix A: Firewall Configuration

5.3. Appendix B: Firewall Change Log

5.4. Appendix C: List of Ports and Services

5.5. Appendix D: Cardholder Data Environment – Authorized Connections

6. Definitions

6.1. *Firewall* – An appliance or software that prevents unauthorized access to networks or computers.

6.2. *DMZ (de-militarized zone)* - Any un-trusted network connected to, but separated from, the corporate network by a firewall, used for external (Internet/partner, etc.) access from within the network, or to provide information to external parties. All DMZ networks connecting to the Internet fall under the scope of this policy.

6.3. *Perimeter Firewall* – The firewall that resides on the router or gateway that has contact with the Internet. Commonly

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.

available routers, even those intended for home use come with a robust firewall that should be able to protect the company from most attacks.

6.4. *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.

6.5. *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.

Network Security Policy
Version 3.2

Errata Sheet

Positions responsible for firewall compliance:

Department	Title	Activities Responsible for

Scan Vendor
Approved Scan Vendor Name:

_____

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.

Appendix A: Firewall Configuration Settings

Router

Setting	Required	Actual
Broadcast SSID (Wireless Only)	OFF	
Network Address Translation (NAT)	ON	
Notifications	ON	
Intrusion Detection and Blocking	ON	
Domain Blocking	ON	
Stateful (Dynamic) Packet Inspection	ON	

Computer

Setting	Required	Actual
Masquerading	ON	
Network Address Translation (NAT)	ON	
Notifications	ON	
Intrusion Detection and Blocking	ON	
Domain Blocking	ON	
Stateful (Dynamic) Packet Inspection	ON	
Event Logging	ON	
Login Failures	ON	

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.

Appendix B: Firewall Change Log

Device Name/Address	Reason for Change	Date Approved	Date Changed

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.

Appendix C: List of Ports and Services

Computer Name		
PORT NUMBER	**Services Supported**	**Status (Circle One)**
80	HTTP - Unsecured	Disabled Automatic Manual
443	Secure Sockets Layer	Disabled Automatic Manual
		Disabled Automatic Manual
		Disabled Automatic Manual
		Disabled Automatic Manual
		Disabled Automatic Manual
		Disabled Automatic Manual
		Disabled Automatic Manual
		Disabled Automatic Manual

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.

Appendix D: Cardholder Data Environment – Authorized Connections

Connection Designation	Purpose of Connection	Authorized By

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.