PCI DSS Requirements by Terminal Type

This document helps you answer PCI DSS requirements pertaining to payment terminals in your environment. If your terminal is not listed below, please consult with your terminal provider to obtain assistance answering the terminal specific PCI DSS requirements around your device. This document is just one of many tools intended to support you in your PCI Compliance Validation efforts, which the entire set of which can be found here: www.paymentstartnow.com/secure

version	SAQ Question	ICT250	ICT220	IWL 250G	IWL 220B	VX520	VX680	VX680G	PINPad 220	PINPad 320	PINPad 820
SAQ B & B-IP (3.1)	3.2.c – Is sensitive authenitification data deleted or rendered unrecoverable upon completion of the authorization process?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SAQ B & B-IP (3.1)	3.2.1 – The full contents of any track are not stored after authorization?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SAQ B & B-IP (3.1)	3.2.2 – The card verification code or value is not stored after authorization?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SAQ B & B-IP (3.1)	3.2.3 – The Personal Identification Number (PIN) or the encrypted PIN block is not stored after authorization?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SAQ B & B-IP (3.1)	3.3 – Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed) such that only personnel with a legitimate business need can see the full PAN?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SAQ B-IP (3.1)	2.1.a – Are vendor-supplied default passwords always changed before installing a system on the network? [1]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
SAQ B-IP (3.1)	2.3.a – Is all non-console administrative access encrypted with strong cryptography, and is a strong encryption method invoked before the administrator's password is requested? [2]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
SAQ B-IP (3.1)	2.3.b – Are system services and parameter files configured to prevent the use of Telnet and other insecure remote login commands? [2]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
SAQ B-IP (3.1)	2.3.c – Is administrator access to web-based management interfaces encrypted with strong cryptography? [2]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
SAQ B-IP (3.1)	2.3.d – For the technology in use, is strong cryptography implemented according to industry best practice and/or vendor recommendations?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

1 Processing equipment is shipped to customers with a standard/default password still live; however, this password cannot be used for any malicious intent to change the firmware or software in the terminal or be used to gain access to cardholder data processed by the terminal. Customer can change password if desired.
2 Non Console access and remote access are not allowed on Processing terminals.

© Elavon, Inc. 2017. This document is intended to support, summarize, and implement data security best practices and does not replace or supersede the Elavon Terms of Service, Merchant Operating Guide, the PCI DSS standards, payment card network rules and regulations, or the Elavon PCI compliance program, as may be amended from time to time. The materials and recommendations herein are general in nature and may not apply to all merchant payment configurations or to unique data security diagrams.

version	SAQ Question	ICT250	ICT220	IWL 250G	IWL 220B	VX520	VX680	VX680G	PINPad 220	PINPad 320	PINPad 820
SAQ B-IP (3.1)	2.3.e – Is there documentation that verifies the devices are not susceptible to any known exploits for SSL/early TLS? [3]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	4.1.a – Are strong cryptography and security protocols such as TLS, SSH, or IPSEC used to safeguard sensitive cardholder data during transmission over open public networks?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	4.1.b – Are only trusted keys and/or certificates accepted?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	4.1.c – Are security protocols implemented to use only secure configurations and to not support insecure versions or configurations?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	4.1.d – Is there proper encryption strength implemented for the encryption methodology in use?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	4.1.e – For TLS implementations, is TLS enabled whenever card-holder data is transmitted or received? [4]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	4.1.f – See 2.3.e for same answer.	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	6.1 – Is there a process to identify security vulnerabilities, including: using reputable outside sources for vulnerability information and assigning a risk ranking to vulnerabilities that includes identification of all "high" risk and "critical" vulnerabilities? [5]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	6.2.a – Are all system components and software protected from known vulnerabilities by installing applicable vendor-supplied security patches?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	6.2.d – Are critical security patches installed within one month of release?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	8.3 – Is two-factor authentication incorporated for remote network access originating from outside the network by personnel and all third parties? [2]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	8.5 – Are group, shared, or generic accounts, passwords, or other authentication methods prohibited as follows: Generic user IDs and accounts are disabled or removed; shared user IDs for system administration activities and other critical functions do not exist; and shared or generic user IDs are not used to administer any system components.	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

2 Non Console access and remote access are not allowed on terminals. 3 Terminals are included in the overall AoC, which is supplied to customers as part of the PCI Tool Kit found at www.paymentstartnow.com
4 The customer is using a version of the terminal application that is still available for download and support. 5 We have a process identified with the terminal vendors (Verifone/Ingenico) to be made aware of vulnerabilities and build the fix into upcoming software releases.