NINJIO

2820 Townsgate Road
Suite 101
Westlake Village, CA 91361

Phone: +1 805 864 1999
Email: info@ninjio.com
Website: www.ninjio.com

PCI-DSS COMPLIANCE

3-PART SERIES

NINJIO has developed a unique 3-part series on PCI Compliance as it relates to the end-user. In the NINJIO tradition, the series is done all through storytelling, and one of the largest credit card breaches in history was inspiration to the story.

This series specifically focuses on the "end-user" i.e. those employees, primarily in the back office, who come across credit card information as part of their daily responsibilities.

NINJIO also has a 4th PCI Episode that specifically addresses "card-handling." Ask your NINJIO Rep for the password then click play to watch Episode 4----->

WHAT'S COVERED IN THE 3 EPISODE SERIES:

1.4

Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE.

This requirement applies to employee owned and company-owned portable computing devices. Systems that cannot be managed by corporate policy introduce weaknesses and provide opportunities that malicious individuals may exploit. Allowing untrusted systems to connect to an organization's CDE could result in access being granted to attackers and other malicious users.

4.2

Never send unprotected PANs by end user messaging technologies (for example, email, instant messaging, SMS, chat, etc.).

5.1

Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers) Note: this applies to any employee owned devices that are allowed on the network and not managed under an MDM program.

5.3

Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.

7.1

Limit access to system components and cardholder data to only those individuals whose job requires such access.

9.7

Maintain strict control over the storage and accessibility of media.

9.8

Destroy media when it is no longer needed for business or legal reasons.

Examine the periodic media destruction policy and verify that it covers all media and defines requirements.

Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hardcopy materials cannot be reconstructed period.

9.81

Shred, incinerate, or pulp hard copy materials so that cardholder data cannot be reconstructed.

9.9

Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.

11

Regularly test security systems and processes.

12.6

Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.

EPISODE #4

With the number of restaurant and retail employees that handle large numbers of credit cards on a daily basis, the 4th PCI episode is meant to be a "stand alone" that focuses exclusively on "card handling." This was done so that if you only need to train your front-line people on card handling, our entire 3-part series isn't necessary. They will only need Episode 4.

EPISODE #4