HFTP
Hospitality Financial and Technology Professionals

HFTP PCI Compliance Roundtable Report

PCI Boot Camp: Best Practice Takeaways

Best practices primarily fall into three (3) distinct but interwoven areas: *operations, networks* and *documentation*.

1. Operations Best Practices

- Discontinue the imprinting of credit cards if still imprinting.
- Review proper merchant bank retrieval request and chargeback information requirements: Don't keep documents containing complete credit card numbers for fear of losing a chargeback.
- Discourage facsimile receipt of credit card authorizations: secure fax machines and their output.
- Prohibit e-mail receipt of credit card numbers.
- For all voice, facsimile, or other methods of card receipt, enter directly into the system and destroy (shred) the paper.
- Review sales & catering department files for maintenance of documents containing credit card numbers.
- Do not use notes, comments, or other unencrypted fields in sales, catering, and other electronic systems for credit card numbers.
- Review who has access to view guests' complete credit numbers in both the PMS and POS.
- Review if card data or computer passwords are written on a "sticky note" placed on computer monitors or are otherwise visible or unsecured.
- Train users to log off their terminals and use tight auto-log off timeouts on payment applications if available.
- Always consider proper storage, retention and disposal of paper and other sources of credit card numbers.
- Select photocopiers and facsimiles with encrypted disk drives with auto-delete capability (24 hours).
- Control physical access to server rooms, front desk and any other areas where credit card numbers are stored or processed. Consider logging and badging all visitors to these areas and requirement to surveil all data centers by video.
- Conduct training on PCI Compliance to include making training materials consumer-friendly, annual training certification signed by all employees, making training certification a part of the "Acceptable Use Policy," and awareness of phishing, spear-phishing, pharming, and "vendor impostors."

2. Networks Best Practices

Best practices regarding networks fall into three (3) categories: *passwords, remote access,* and *operations.*

- *Passwords.*
  - Changing all default passwords before connecting a device to the network. Devices to be reviewed include: payment application servers, other servers, routers, and firewalls.
  - Changing the SSID names for wireless networks: how many networks named "Linksys Router" have you observed when looking for wi-fi hot spots!?
  - Being mindful of the definition of a "strong password" for PCI purposes, as it differs from that for non-PCI purposes.
  - Making passwords for all users of payment applications unique by not permitting the sharing of passwords, by creating unique passwords for vendors, and by using tools and policies to expire passwords, force strong passwords, and not allowing re-use of prior passwords.

- *Remote Access (for **vendors** and **employees**).*

  *Best practices regarding **vendors** include:*
  - Access being "on-request" from the property and not from the vendor.
  - The property initiating the remote access connection.
  - The embedding of logging in the access tool used.
  - Changing default ports.
  - Adding remote access to vendor agreements and contracts.
  - Training hotel employees to authenticate callers purporting to be vendors requesting access for support – *very important*!

  *Best practices regarding **employees** include:*
  - Access being "on-request" from the employee, approved by the department head/EC member, with a valid reason for access.
  - Access being granted only to those applications needed by the employee and not to the entire network, depending upon where payment applications reside.
  - Changing default ports.
  - Using a remote access program with strong authentication and logging.

- *Operations.*
  - Maintaining separation of guest and employee networks.
  - Insuring that there are anti-virus subscriptions on all computers and that they are current.
  - Seeing that security patches are applied regularly.
  - Being alert for skimmers and keystroke loggers.
  - Being alert for rogue software, PCs, and wireless or USB devices.
  - Using a laptop or smartphone to scan for rogue devices.

3. Documentation Best Practices

- Acceptable use policy.
- Backups and disaster recovery.
- Incident response plans.
- Merchant-level determination letters from acquirers.
- Proof of PCI PA-DSS Compliance letters from payment applications used.
- Network vulnerability scan reports.