PCI Compliance & Sustainability
Payment Card Assessments, LLC

PHYSICAL SECURITY CHECKLIST FOR ONSITE ASSSESSMENTS

Requirement 9: Restrict physical access to cardholder data. This checklist can be used to prepare for your onsite physical security assessments of data centers and call centers.

Onsite assessments may take up to 90 minutes to complete.

Feed two birds from one hand: sample call center rep devices to ensure that anti-virus software is installed, running, up-to-date, and can't be disabled per PCI DSS requirement 5.

- [ ] Physical access controls such as badge readers, lock and key or other devices are implemented to ensure access restrictions.
- [ ] Video cameras or other access control mechanisms are implemented to monitor entry/exit points.
- [ ] Ensure video cameras or other access control mechanisms can't be tampered with.
- [ ] Provide evidence that video or other access control mechanisms are reviewed and stored for at least 3 months.
- [ ] During the walk through, personnel will need to provide details how physical or logical access is restricted on publicly accessible network jacks, wireless access points, wireless gateways, wireless handheld devices, network/comm hardware, teleco lines
- [ ] Visitor Access: Demonstrate how you distinguish onsite personnel from visitors, changes to access requirements, how access is revoked or terminated for personnel and visitors.
- [ ] Ensure visitors are easily identifiable.

- [ ] Have your access control processes for the badging system ready to walk through. Provide roles, groups, and ensure access is limited to authorized personnel.

PCI DSS requirements 9.2.c & 9.3 loops with access controls in PCI DSS requirement 7.

- [ ] Physical access for onsite personnel follows concept of least privilege, must be authorized, and access must be revoked immediately upon termination. Provide access control lists to prove access is authorized and required for the role.

- [ ] QSA will observe personnel accessing sensitive areas to verify that personnel are authorized before being granted access.

- [ ] Visitors: must be authorized before access is granted, escorted at all times in areas where cardholder data is processed or maintained.

- [ ] Visitor badges: must be easily distinguishable, expire, and surrendered upon visitor departure.

PCI DSS requirements 9.2 and 9.4.2.a loop together.

- [ ] Visitor logs must be: in use to record physical access to the facility, computer rooms, or wherever cardholder data is stored or transmitted. Visitor logs must be retained for at least 3 months.

- [ ] Visitor logs must contain:
  - visitor name
  - firm represented
  - onsite personnel authorizing access