

Physical Security Policy

**Internal Use Only**

Version Status

This version of this document is currently:

|  |  |
| --- | --- |
|  | In Progress |
|  | In Review |
|  | Published |
|  | In Test |
| **⇒** | **Tested/Applicable** |

Document History

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version | Author | Reviewers | Publisher | Date | Description |
| 0.5 | MSW |  |  | 7 May 2013 | First draft |
| 0.6 | A. TREPS |  |  | 18 February 2014 | Includes Thales procedures.  Version for IOM review. |
| 1.0 |  | A. BEN DAAS | A.TREPS | 23 October 2014 | Publication |
| 1.1 | YH | A.TREPS |  | 25/01/2016 | Minor Change |
| 1.2 | A.TREPS |  |  | 23/02/2017 | Precisions for badge management in Evry |
| 1.3 |  | P.AURE |  | 14 March 2018 | Annual Review |
| 1.4 |  | P.AURE |  | 25 March 2019 | Annual Review |
| 1.4.1 |  | P.AURE |  | 16 July 2019 | Add Minh as Approbator for Evry DC Access |
| 1.5 |  | P.AURE |  | 24 Feb 2020 | Annual Review |
| 1.6 |  | KGUYOT |  | 11 June 2020 | Annual Review & modification approbator |
| 1.7 |  | P. AURE |  | 17 March 2021 | Update URLs (ACSA to confluence) |
| 1.8 |  | F. REGNIER |  | March 2022 | Annual Review |

Projected Review Date:

(= 12 months after publication)

This Document

|  |  |
| --- | --- |
| Purpose | The objective of this document is to specify the measures Accor intends for providing physical protection of sensitive information. |
| Audience | The principal audiences for this document are:   * Information Technology’s teams * PCI Countries Committees |
| Applicability | This document is to be applied from the date of its approved publication.  The recommendations in this document apply to all Accor-owned entities worldwide Accor Central, and the head offices of countries, as well as subsidiaries of Accor, and all regional and local entities (including agencies, hotels, etc.). |
| Related Documentation | The information in this document must be completed and supplemented with information in a set of documents that includes:   * *Network Security Policy* * *Accès salle info et serveurs* |
| Using this guide | This document contains guidelines and procedures. |
| Questions? | Contact [security@accor.com](mailto:security@accor.com). |

Table of Contents

[1 Introduction 6](#_Toc66879401)

[1.1 Context 6](#_Toc66879402)

[1.2 Policy Objective 6](#_Toc66879403)

[1.3 Scope 6](#_Toc66879404)

[2 Central datacenters 7](#_Toc66879405)

[2.1 Isolation 7](#_Toc66879406)

[2.2 Video cameras 7](#_Toc66879407)

[2.3 Network access 7](#_Toc66879408)

[2.4 Visitor Procedures 8](#_Toc66879409)

[2.4.1 Primary datacenter (Elancourt) 8](#_Toc66879410)

[2.4.2 Backup datacenter (Evry) 8](#_Toc66879411)

[2.4.3 Badge management (Evry) 8](#_Toc66879412)

[2.5 Datacenter review 9](#_Toc66879413)

[3 Procedures for hotels 10](#_Toc66879414)

[3.1 Protect the PC at the front desk 10](#_Toc66879415)

[3.2 Protect sensitive papers with payment card numbers 11](#_Toc66879416)

[3.3 Protect access to the Accor network 11](#_Toc66879417)

[3.4 Protect the Back-office 11](#_Toc66879418)

[3.5 Shred sensitive paper 11](#_Toc66879419)

[3.6 Install video cameras 11](#_Toc66879420)

[4 Console lockout 12](#_Toc66879421)

[5 Media management 13](#_Toc66879422)

[5.1 General policy 13](#_Toc66879423)

[5.2 Central systems procedures 13](#_Toc66879424)

[5.2.1 Primary datacenter (Elancourt) 13](#_Toc66879425)

[5.2.2 Backup datacenter (Evry) 13](#_Toc66879426)

[5.2.3 Media distribution 13](#_Toc66879427)

[5.2.4 Media Destruction 14](#_Toc66879428)

[5.3 Hotels 14](#_Toc66879429)

[6 PCI DSS requirements for physical security 15](#_Toc66879430)

# Introduction

## Context

To be effective, organizational and logical security measures in place to protect payment card data must be completed by physical security.

Physical security main objectives are to guarantee **access control** and **traceability** to all components in the PCI DSS scope.

## Policy Objective

The goal of this document is to describe the organization, guidelines, and procedures that Accor puts in place to manage the physical security of its confidential data.

## Scope

This document addresses physical security for the cardholder data environment, at the central scope (PCI dedicated infrastructure in Elancourt and Evry datacenters) and hotel scope.

# Central datacenters

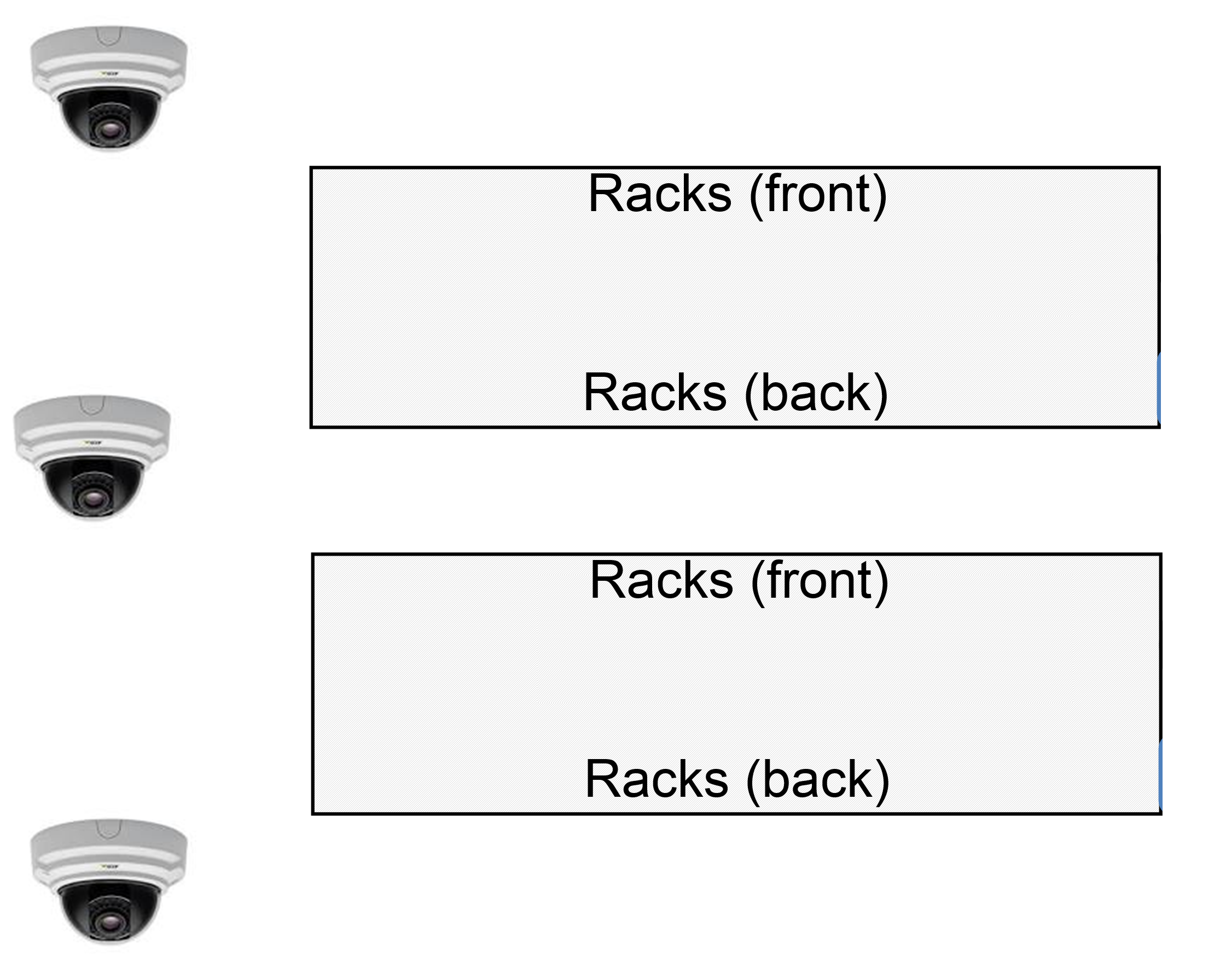
## Isolation

Devices in the PCI DSS scope must be physically isolated from not PCI devices in the data center, using either separated and closed racks, or a special area inside the datacenter.

Entry to those PCI DSS scope areas is only possible on the presentation of an authorized badge.

## Video cameras

Accesses to the racks are monitored by videos cameras positioned as follows:



Cameras must support:

* Infrared visibility up to 20 meters
* Minimum resolution of 720p

Cameras must be positioned in a way that prevents unauthorized tampering or disabling. For example, a camera could be enclosed in protective glass, or fixed to the roof, or both.

The recording is either 24/7 a day, or automatically started when movement is detected.

By French law, data from the video cameras is stored for a maximum of one month.

## Network access

In Accor central datacenters, all network jacks related to the PCI DSS environment must be enclosed in a PCI DSS rack to prevent unauthorized access.

Wireless access points are forbidden in this environment. A quarterly review is performed by Accor Security Team to detect the presence of unauthorized access points.

## Visitor Procedures

Procedures vary depending on the data center since the primary one is managed by a third-party company.

### Primary datacenter (Elancourt)

* IT Operations Services team must issue an IT request that identifies the person/role and specifies the duration of the visit.
* At the building entry, an ID check is performed by Thalès teams, and the visitor is required to complete and sign the check-in entry in the visitor log.

*Note: For all new person, a background check is mandatory for Thalès to gain access to the data center.*

* Non-Accor employees must always be accompanied by an Accor staff member, who is responsible for accompanying the visitor throughout the visit.
* **Access to PCI racks:** If access to a PCI rack is necessary, an additional check-in / check-out procedure is performed just before the server room entry. A PCI badge is given to the Accor employee by Thalès. Badge number, time and date, employee name and signature are kept in a specific visitor log.

When leaving the server room, the PCI badge must be given back to the Thalès employee and the visitor log must be signed again.

* On termination of the visit, the visitor completes and signs the check-out entry in the visitor log before getting back his ID.

**Visitor logs that contain the record of all visits must be retained for a minimum of three months.**

### Backup datacenter (Evry)

Access to the backup data center is only allowed to Accor staff members (Accor employees or long-term consultants) using a nominative badge. External visitors must always be accompanied by an Accor staff member.

Note: generic badges used by the “environment de travail” teams exist but are only attributed to specific technical interventions (ex: air conditioning, fire safety, etc.). A log (“registre de sécurité”) must be filled for any use of these generic badges.

### Badge management (Evry)

After being hired, Accor employees in Evry receive a nominative badge.

This badge only allows access to the offices.

Access to the data center is allowed after the following procedure:

* Email request to *Pascal GENDARME* [*Pascal.Gendarme@accor.com*](mailto:Pascal.Gendarme@accor.com), *Laurent BRUYNOOGHE* [laurent.bruynooghe@accor.com](mailto:laurent.bruynooghe@accor.com) and *HA Cong-Ming* <Cong-Minh.HA@accor.com> (requester must put his direct manager in copy)
* Once agreed by both the manager and the IT Operations Services team, server room access is added to the requester badge
* The direct manager is responsible for requesting server room access removal when such access is not needed anymore by the requester (example: job modification)
* A quarterly review process is performed by the IT Operations Services and security team to detect accesses that should have been terminated.

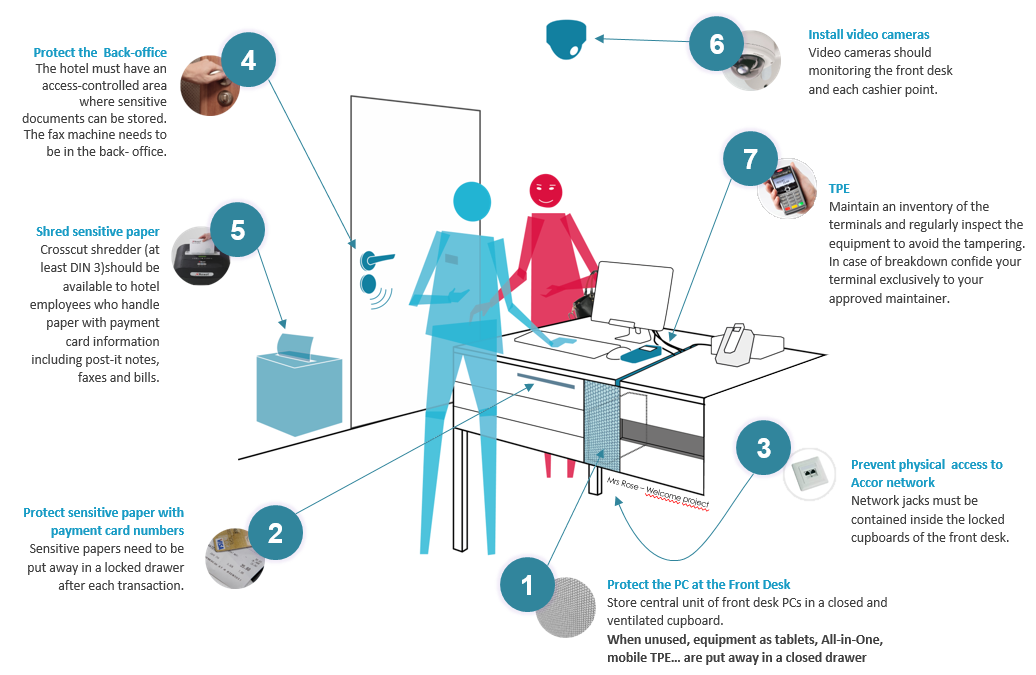
When an employee leaves the company, the nominative badge must be given back to the HR department (Talent & Culture). This is a mandatory step before receiving the last payroll.

## Datacenter review

Every quarter, a data center security review must be performed to control the presence of rogue WIFI access points, media storage security and to check the list of people authorized to access the data center.

# Procedures for hotels

The following picture illustrates physical security recommendations for hotels.



## Protect the PC at the front desk

The PCI-DSS norm requires controlled access to all systems that store, transmit or process payment card data.

This includes PCs (computers) at the front desk. They must be protected against unauthorized physical access and theft.

The basic recommendation here is: to store the central unit of your front-desk PC in a closed cupboard. It must be a secure cupboard, with some form of *access control* (a metal key, a magnetic key, RFID, PIN code, etc.).

You should also make sure that:

* **Cable Space**: There is enough space for all the required cables. This includes power cables for the computer and monitor, cables to connect the keyboard and the mouse, cables for a room key encoder, for the payment pinpad, for USB printers, etc.
* **Ventilation**: The closed cupboard where you will enclose the computer and peripherals has enough holes in it to ventilate the devices correctly. They can get quite hot, and too much heat could make them shut down unexpectedly.
* **On/Off Switch**: There is one hole positioned so that you can access the power/reset button for the computer. You must be able to turn the computer on or off without opening the cupboard.

## Protect sensitive papers with payment card numbers

Every *cashier point* should have a drawer that can be locked. The main cashier point is the reception desk, but others are located anywhere that guests can present a payment card, including the bar, the restaurant, and so on.

This drawer should have an opening (like a mailbox) to allow hotel personnel to store the sensitive documents without opening the drawer. The recommended size for this opening is A5 paper format.

## Protect access to the Accor network

Physical access to the hotel network should be protected against illegitimate access.

Ideally, network jacks should be contained inside the locked cupboard of the reception desk.

**Note**: This recommendation does not apply to the internet access network used by guests of the hotel.

## Protect the Back-office

The hotel must have an access-controlled area where you can store and archive sensitive documents that contain payment card information. Ideally, a safe box should be available in this area.

The fax machine used to receive booking guarantees should be located in this controlled area.

## Shred sensitive paper

Crosscut shredders should be available to hotel employees who handle paper with payment card information, including post-it notes, faxes, and bills.

At a minimum, these shredders should be compliant with the **DIN 3** (Deutsches Institude Für Norming) standard.

Accor selected three references available through referenced supplier LYRECO.

## Install video cameras

Anywhere that payment card information is handled or stored; a video camera should be in place for monitoring entry/exit points to these sensitive areas. This camera should cover back-office, front desk, archive room, etc…

Position cameras in a way that prevents unauthorized tampering or disabling. For example, a camera could be enclosed in protective glass, or fixed to the roof, or both.

Recordings should be kept at least three months (unless local law specifies shorter or longer requirements, in this case, local law applies). For more information, check with Legal Services in your country.

# Console lockout

All consoles should, and all PCI DSS consoles must be locked in the absence of the system administrator who uses them.

* On Windows systems: Windows-key + “L”
* On Unix systems Ctrl + “D”

# Media management

## General policy

Since clear-text storage of cardholder data is forbidden in the PCI environment, backup tapes should never contain clear-text card data, but may contain encrypted card data.

The following rules must be followed for all backup tapes containing encrypted data or PCI sensitive data (passwords, encryption keys, configuration files, etc.)

* Such media must be classified as “PCI” by a sticker
* An inventory must be maintained and reviewed annually
* Media must be stored securely
* Management approval is required before any media distribution

## Central systems procedures

### Primary datacenter (Elancourt)

Media inventory and classification is maintained by Thales teams.

Backup tapes are stored in a tape library room protected by badge access control.

Storage is reviewed annually during the Steering Committee between Thales and Accor ITOPS teams.

Datacenters are quarterly assessed based on the Datacenter security review process (cf. [Datacenter Security Review Procedure.pdf](http://confluence.accor.net/download/attachments/85260991/Datacenter%20security%20review%20process.pdf)).

### Backup datacenter (Evry)

Media inventory and classification is maintained by the “pupitre” team. The inventory is verified and updated monthly.

Related document : *Inventaire des sauvegardes de la Bulle PCI.xlsx*

### Media distribution

When the need arises to transport a tape, the procedure is as follows:

* Authorization (IT Operations Services management) is required
* Only authorized couriers are to be used (a list is maintained by the IT Operations Services team)
* Transport is tracked and monitored.

Defective Bands and Defective disks should be placed in the safe box.

### Media Destruction

At the time of expiry, cardholder data on electronic media must be made unrecoverable so that cardholder data cannot be reconstructed.

The appropriate destruction technique is applied.

* Servers: When destruction is needed, those PCI referenced disks are securely destroyed by **S-CUBE** after IT Operations Services Management approval at Evry Datacenter and by **Thales** at Elancourt Datacenter. A certificate of destruction must be provided to close the case
* Disks: When destruction is needed, those PCI referenced disks are securely destroyed by **S-CUBE** after IT Operations Services Management approval at Evry Datacenter and by **Thales** at Elancourt Datacenter. A certificate of destruction must be provided to close the case.
* Tapes: CHD-tapes are stored securely up to the time of the destruction of the data that they contain. When destruction is needed, those tapes that have a PCI label are securely destroyed by **S-CUBE** after IT Operations Services Management approval at Evry Datacenter and by **Thales** at Elancourt Datacenter. A certificate of destruction must be provided to close the case.

Thales Procedure: ***CSE-DIR-10-SEC-18464-A\_Procedure\_gestion\_supports\_dematerialises\_classif***

## Hotels

An inventory and classification process must be established by country IT teams adapted to the local backup process. This process must respect requirements 9.5, 9.6, 9.7, 9.8, 9.9 and 9.10.

If a third-party company is involved, the PCI DSS compliance clause must be added to the contract.

# PCI DSS requirements for physical security

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Testing procedure** | **Guidance** |
| **9.1** Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment. | **9.1** Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment.  · Verify that access is controlled with badge readers or other devices including authorized badges and lock and key.  · Observe a system administrator’s attempt to log into consoles for randomly selected systems in the cardholder environment and verify that they are “locked” to prevent unauthorized use. | Without physical access controls, unauthorized persons could potentially gain access to the building and to sensitive information, and could alter system configurations, introduce vulnerabilities into the network, or destroy or steal equipment. |
| **9.1.1** Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.  ***Note:*** *“Sensitive areas” refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.* | **9.1.1.a** Verify that video cameras and/or access control mechanisms are in place to monitor the entry/exit points to sensitive areas. | When investigating physical breaches, these controls can help identify individuals that physically access those sensitive areas storing cardholder data. Examples of sensitive areas include corporate database server rooms, back-end server room of a retail location that stores cardholder data, and storage areas for large quantities of cardholder data, |
| **9.1.1.b** Verify that video cameras and/or access control mechanisms are protected from tampering or disabling. |
| **9.1.1.c** Verify that video cameras and/or access control mechanisms are monitored and that data from cameras or other mechanisms is stored for at least three months. |
| **9.1.2** Restrict physical access to publicly accessible network jacks.  For example, areas accessible to visitors should not have network ports enabled unless network access is explicitly authorized. | **9.1.2** Verify by interviewing network administrators and by observation that network jacks are enabled only when needed by authorized onsite personnel. Alternatively, verify that visitors are escorted at all times in areas with active network jacks. | Restricting access to network jacks will prevent malicious individuals from plugging into readily available network jacks that may allow them access into internal network resources. Consider turning off network jacks while not in use, and reactivating them only while needed. In public areas such as conference rooms, establish private networks to allow vendors and visitors to access Internet only so that they are not on your internal network. |
| **9.1.3** Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines. | **9.1.3** Verify that physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is appropriately restricted. | Without security over access to wireless components and devices, malicious users could use your organization’s unattended wireless devices to access your network resources, or even connect their own devices to your wireless network to gain unauthorized access. Additionally, securing networking and communications hardware prevents malicious users from intercepting network traffic or physically connecting their own devices to your wired network resources.  Consider placing wireless access points, gateways and networking/ communications hardware in secure storage areas, such as within locked closets or server rooms. For wireless networks, ensure strong encryption is enabled. Also consider enabling automatic device lockout on wireless handheld devices after a long idle period and set your devices to require a password when powering on. |
| **9.2** Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible. | **9.2.a** Review processes and procedures for assigning badges to onsite personnel and visitors, and verify these processes include the following:  · Granting new badges,  · Changing access requirements, and  · Revoking terminated onsite personnel and expired visitor badges | Without badge systems and door controls, unauthorized and malicious users can easily gain access to your facility to steal, disable, disrupt, or destroy critical systems and cardholder data. For optimum control, consider implementing badge or card access system in and out of work areas that contain cardholder data.  Identifying authorized visitors so they are easily distinguished from onsite personnel prevent unauthorized visitors from being granted access to areas containing cardholder data. |
| **9.2.b** Verify that access to the badge system is limited to authorized personnel. |
| **9.2.c** Examine badges in use to verify that they clearly identify visitors and it is easy to distinguish between onsite personnel and visitors. |
| **9.3** Make sure all visitors are handled as follows: | **9.3** Verify that visitor controls are in place as follows: | Visitor controls are important to reduce the ability of unauthorized and malicious persons to gain access to your facilities (and potentially, to cardholder data). |
| **9.3.1** Authorized before entering areas where cardholder data is processed or maintained. | **9.3.1** Observe the use of visitor ID badges to verify that a visitor ID badge does not permit unescorted access to physical areas that store cardholder data. | Visitor controls are important to ensure visitors only enter areas they are authorized to enter, that they are identifiable as visitors so personnel can monitor their activities, and that their access is restricted to just the duration of their legitimate visit. |
| **9.3.2** Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as not onsite personnel. | **9.3.2.a** Observe people within the facility to verify the use of visitor ID badges, and that visitors are easily distinguishable from onsite personnel. |
| **9.3.2.b** Verify that visitor badges expire. |
| **9.3.3** Asked to surrender the physical token before leaving the facility or at the date of expiration. | **9.3.3** Observe visitors leaving the facility to verify visitors are asked to surrender their ID badge upon departure or expiration. |
| **9.4** Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor’s name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law. | **9.4.a** Verify that a visitor log is in use to record physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted. | A visitor log documenting minimum information on the visitor is easy and inexpensive to maintain and will assist, during a potential data breach investigation, in identifying physical access to a building or room, and potential access to cardholder data. Consider implementing logs at the entry to facilities and especially into zones where cardholder data is present. |
| **9.4.b** Verify that the log contains the visitor’s name, the firm represented, and the onsite personnel authorizing physical access, and is retained for at least three months. |
| **9.5** Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location’s security at least annually. | **9.5.a** Observe the storage location’s physical security to confirm that backup media storage is secure. | If stored in a non-secured facility, backups that contain cardholder data may easily be lost, stolen, or copied for malicious intent. For secure storage, consider contracting with a commercial data storage company OR, for a smaller entity, using a safe-deposit box at a bank. |
| **9.5.b** Verify that the storage location security is reviewed at least annually. |
| **9.6** Physically secure all media. | **9.6** Verify that procedures for protecting cardholder data include controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes). | Cardholder data is susceptible to unauthorized viewing, copying, or scanning if it is unprotected while it is on removable or portable media, printed out, or left on someone’s desk. |
| **9.7** Maintain strict control over the internal or external distribution of any kind of media, including the following: | **9.7** Verify that a policy exists to control distribution of media, and that the policy covers all distributed media including that distributed to individuals. | Procedures and processes help protect cardholder data on media distributed to internal and/or external users. Without such procedures data can be lost or stolen and used for fraudulent purposes. |
| **9.7.1** Classify media so the sensitivity of the data can be determined. | **9.7.1** Verify that all media is classified so the sensitivity of the data can be determined. | It is important that media be identified such that its classification status can be easily discernable. Media not identified as confidential may not be adequately protected or may be lost or stolen. |
| **9.7.2** Send the media by secured courier or other delivery method that can be accurately tracked. | **9.7.2** Verify that all media sent outside the facility is logged and authorized by management and sent via secured courier or other delivery method that can be tracked. | Media may be lost or stolen if sent via a non-trackable method such as regular postal mail. Use the services of a secure courier to deliver any media that contains cardholder data, so that you can use their tracking systems to maintain inventory and location of shipments. |
| **9.8** Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals). | **9.8** Select a recent sample of several days of offsite tracking logs for all media and verify the presence in the logs of tracking details and proper management authorization. | Cardholder data leaving secure areas without a process approved by management can lead to lost or stolen data. Without a firm process, media locations are not tracked, nor is there a process for where the data goes or how it is protected. |
| **9.9** Maintain strict control over the storage and accessibility of media. | **9.9** Obtain and examine the policy for controlling storage and maintenance of all media and verify that the policy requires periodic media inventories. | Without careful inventory methods and storage controls, stolen or missing media could go unnoticed for an indefinite amount of time. |
| **9.9.1** Properly maintain inventory logs of all media and conduct media inventories at least annually. | **9.9.1** Obtain and review the media inventory log to verify that periodic media inventories are performed at least annually. | If media is not inventoried, stolen or lost media may not be noticed for a long time or at all. |
| **9.10** Destroy media when it is no longer needed for business or legal reasons as follows: | **9.10** Obtain and examine the periodic media destruction policy and verify that it covers all media, and confirm the following: | If steps are not taken to destroy information contained on hard disks, portable drives, CD/DVDs, or paper prior to disposal, malicious individuals may be able to retrieve information from the disposed media, leading to a data compromise. For example, malicious individuals may use a technique known as “dumpster diving,” where they search through trash cans and recycle bins looking for information they can use to launch an attack.  Examples of methods for securely destroying electronic media include secure wiping, degaussing, or physical destruction (such as grinding or shredding hard disks). |
| **9.10.1** Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed. | **9.10.1.a** Verify that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. |
| **9.10.1.b** Examine storage containers used for information to be destroyed to verify that the containers are secured. For example, verify that a “to-be-shredded” container has a lock preventing access to its contents. |
| **9.10.2** Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed. | **9.10.2** Verify that cardholder data on electronic media is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing). |