

# Requirement 9: Restrict Physical Access to Cardholder Data

---



**John Elliott**

PRIVACY, PAYMENTS, SECURITY AND RISK SPECIALIST

@withoutfire [www.withoutfire.com](http://www.withoutfire.com)



## Requirement 9



**Physical access controls**

**Managing visitors**

**Secure and manage physical media**

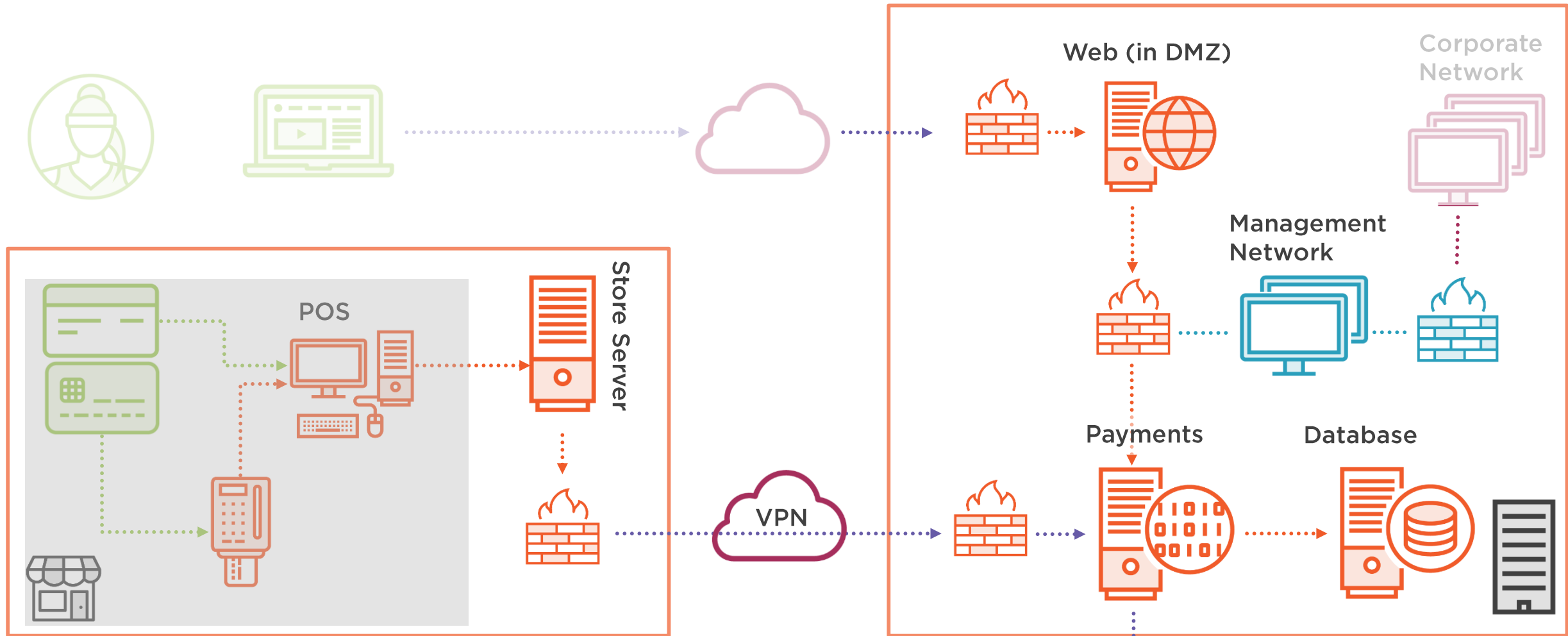
- Paper, disks, tapes

**Secure destruction of media**

**Protect card-reading devices**

**Policies and procedures**





- Cardholder's card and systems
- Stores, processes or transmits
- Connected to or security affecting
- Out of scope of PCI DSS

- Unencrypted cardholder data
- Encrypted cardholder data
- Physical card read
- Management network
- Corporate network



# Definitions



## ***Requirement 9: Restrict physical access to cardholder data***

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, “onsite personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity’s premises. A “visitor” refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. “Media” refers to all paper and electronic media containing cardholder data.

PCI DSS Requirements	Testing Procedures	Guidance
<b>9.1</b> Use appropriate facility entry controls to limit and monitor physical access to	<b>9.1</b> Verify the existence of physical security controls for each computer room, data center, and other physical areas with	Without physical access controls, such as badge systems and door controls, unauthorized persons



# Onsite Personnel

Full-time and part-time employees, temporary employees, contractors, and consultants who are physically present on the entity's premises.



# Visitor

Vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day.



# Media

All paper and electronic media containing cardholder data.



# Sensitive Areas

... data center, server room, or any area that houses systems that store, process, or transmit cardholder data.

This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.







## Requirement 9.1

Control physical access to systems in the cardholder data environment





## Requirement 9.1

Use appropriate **facility entry controls** to limit and monitor physical access to systems in the cardholder data environment.



## Requirement Guidance

- Without physical access controls, such as badge systems and door controls, unauthorized persons could potentially gain access to the facility to steal, disable, disrupt, or destroy critical systems and cardholder data.
- **Locking console login screens prevents unauthorized persons from gaining access** to sensitive information, altering system configurations, introducing vulnerabilities into the network, or destroying records.



# 9.1 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Physical security controls at the perimeter of the CDE System consoles</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>-</b>	





# Requirement 9.1.1

Monitor and log physical access





### Requirement 9.1.1

Use either **video cameras** or **access control** mechanisms (or both) 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.




### Requirement Guidance

- When investigating physical breaches, these controls can help identify the individuals that physically accessed the sensitive areas, as well as when they entered and exited.
- Criminals attempting to gain physical access to sensitive areas will often attempt to disable or bypass the monitoring controls. To protect these controls from tampering, video cameras could be positioned so they are out of reach and/or be monitored to detect tampering. Similarly, access control mechanisms could be monitored or have physical protections installed to prevent them being damaged or disabled by malicious individuals.

# “PCI DSS does not supersede local or regional laws, government regulations, or other legal requirements.”

## PCI DSS 3.2.1 | Bottom of Page 5



### Introduction and PCI Data Security Standard Overview

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD). Below is a high-level overview of the 12 PCI DSS requirements.

#### PCI Data Security Standard – High Level Overview

<b>Build and Maintain a Secure Network and Systems</b>	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
<b>Protect Cardholder Data</b>	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
<b>Maintain a Vulnerability Management Program</b>	5. Protect all systems against malware and regularly update anti-virus software or programs
	6. Develop and maintain secure systems and applications
<b>Implement Strong Access Control Measures</b>	7. Restrict access to cardholder data by business need to know
	8. Identify and authenticate access to system components
<b>Regularly Monitor and Test Networks</b>	9. Restrict physical access to cardholder data
	10. Track and monitor all access to network resources and cardholder data
<b>Maintain an Information Security Policy</b>	11. Regularly test security systems and processes
	12. Maintain a policy that addresses information security for all personnel

This document, *PCI Data Security Standard Requirements and Security Assessment Procedures*, combines the 12 PCI DSS requirements and corresponding testing procedures into a security assessment tool. It is designed for use during PCI DSS compliance assessments as part of an entity's validation process. The following sections provide detailed guidelines and best practices to assist entities prepare for, conduct, and report the results of a PCI DSS assessment. The PCI DSS Requirements and Testing Procedures begin on page 15.

PCI DSS comprises a minimum set of requirements for protecting account data, and may be enhanced by additional controls and practices to further mitigate risks, as well as local, regional and sector laws and regulations. Additionally, legislation or regulatory requirements may require specific protection of personal information or other data elements (for example, cardholder name). **PCI DSS does not supersede local or regional laws, government regulations, or other legal requirements.**

Payment Card Industry (PCI) Data Security Standard, v3.2.1  
© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Page 5  
May 2018



## 9.1.1 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Video cameras or access control systems</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>Y</b>	<b>Recordings from video cameras or data from access control systems</b>
<b>Interview people</b>	<b>-</b>	





## Requirement 9.1.1

Use either **video cameras** or **access control** mechanisms (or both) 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.



## Requirement Guidance

- When investigating physical breaches, these controls can help identify the individuals that physically accessed the sensitive areas, as well as when they entered and exited.
- Criminals attempting to gain physical access to sensitive areas will often attempt to disable or bypass the monitoring controls. To protect these controls from tampering, video cameras could be positioned so they are out of reach and/or be monitored to detect tampering. Similarly, access control mechanisms could be monitored or have physical protections installed to prevent them being damaged or disabled by malicious individuals.







Requirement 9.1.1



Requirement Guidance

**... To protect these controls from tampering, video cameras could be positioned so they are out of reach and/or be monitored to detect tampering. Similarly, access control mechanisms could be monitored or have physical protections installed to prevent them being damaged or disabled by malicious individuals.**



The PCI DSS requirements  
do not apply to the  
video recording or  
access control systems





## Requirement 9.1.2

Restrict access to publicly accessible network jacks.



## Requirement 9.1.2

Implement **physical** and/or **logical** controls to restrict access to **publicly accessible** network **jacks**.



## Requirement Guidance

- Restricting access to network jacks (or network ports) will prevent malicious individuals from plugging into readily available network jacks and gain access into internal network resources.
- Whether logical or physical controls, or a combination of both, are used, they should be sufficient to prevent an individual or device that is not explicitly authorized from being able to connect to the network.

## 9.1.2 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Locations of publicly accessible network jacks</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>Y</b>	<b>Responsible people</b>





## Requirement 9.1.3

Protect physical networking equipment





### Requirement 9.1.3

Restrict **physical access** to **wireless access points, gateways, handheld devices, networking / communications hardware, and telecommunication lines.**



### Requirement Guidance

- Without security over access to wireless components and devices, malicious users could use an organization's unattended wireless devices to access network resources, or even connect their own devices to the 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 wired network resources.



## 9.1.3 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Physical access to [various kit]</b>
<b>Examine documentation</b>	<b>!</b>	<b>Polices and risk assessment</b>
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>-</b>	







## Requirement 9.2

Make visitors and  
onsite personnel easily identifiable



## Requirement 9.2

Develop procedures to easily **distinguish between** onsite **personnel** and **visitors**, to include:

- Identifying onsite personnel and visitors (for example, assigning badges)
- Changes to access requirements.
- Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).



## Requirement Guidance

- Identifying authorized visitors so they are easily distinguished from onsite personnel prevents unauthorized visitors from being granted access to areas containing cardholder data.

## 9.2 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Identification methods, access to identification methods</b>
<b>Examine documentation</b>	<b>Y</b>	<b>Documented process for identifying people</b>
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>-</b>	





## Requirement 9.3

Physical role based access  
and least privilege





### Requirement 9.3

Control physical access for onsite personnel to sensitive areas as follows:

- **Access** must be **authorized** and based on individual **job function**.
- **Access is revoked immediately upon termination**, and all **physical** access mechanisms, such as keys, access cards, etc., are **returned or disabled**.



### Requirement Guidance

- Controlling physical access to sensitive areas helps ensure that only authorized personnel with a legitimate business need are granted access.
- When personnel leave the organization, all physical access mechanisms should be returned or disabled promptly (as soon as possible) upon their departure, to ensure personnel cannot gain physical access to sensitive areas once their employment has ended.



## 9.3 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Access control lists, people accessing sensitive areas</b>
<b>Examine documentation</b>	<b>!</b>	
<b>Examine records</b>	<b>Y</b>	<b>Terminated ons personnel</b>
<b>Interview people</b>	<b>Y</b>	<b>Responsible people</b>





## Requirement 9.4

Identify and authorize visitors.





## Requirement 9.4

Implement procedures to identify and authorize visitors.

Procedures should include 9.4.1 through 9.4.4:



## Requirement Guidance

- Visitor controls ensure visitors are identifiable as visitors so personnel can monitor their activities, and that their access is restricted to just the duration of their legitimate visit.
- Ensuring that visitor badges are returned upon expiry or completion of the visit prevents malicious persons from using a previously authorized pass to gain physical access into the building after the visit has ended.
- A visitor log documenting minimum information on the visitor will assist in identifying physical access to a building or room, and potential access to cardholder data.



## 9.4 Testing Procedures

<b>Observe/examine systems and settings</b>	-	<b>Visitor authorization and access controls: 9.4.1 through 9.4.4</b>
<b>Examine documentation</b>	-	
<b>Examine records</b>	-	
<b>Interview people</b>	-	





#### Requirement 9.4.1

**Visitors** are **authorized before entering**, and **escorted** at all times within, areas where cardholder data is processed or maintained.



#### Requirement Guidance

- Visitor controls ensure visitors are identifiable as visitors so personnel can monitor their activities, and that their access is restricted to just the duration of their legitimate visit.



## 9.4.1 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Visitor badges</b>
<b>Examine documentation</b>	<b>Y</b>	<b>Visitor procedures</b>
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>Y</b>	<b>Responsible people</b>





## Requirement 9.4.2

**Visitors** are **identified** and given a **badge** or other identification that **expires** and that **visibly distinguishes** the **visitors** from onsite personnel.

*Verify that visitor badges or other identification expire.*



## Requirement Guidance

- Ensuring that visitor badges are returned upon expiry or completion of the visit prevents malicious persons from using a previously authorized pass to gain physical access into the building after the visit has ended.

## 9.4.2 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Observe people's badges, examine badge expirations</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>-</b>	





**Remember, QSAs are typically visitors**





### Requirement 9.4.3

**Visitors** are asked to **surrender the badge** or identification before leaving the facility or at the date of expiration.



### Requirement Guidance

- Ensuring that visitor badges are returned upon expiry or completion of the visit prevents malicious persons from using a previously authorized pass to gain physical access into the building after the visit has ended.

## 9.4.3 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Observe visitors leaving</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>-</b>	







#### Requirement 9.4.4

A **visitor log** is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted.

**Document** the **visitor's name, the firm, and the onsite personnel authorizing physical access.**

**Retain** this log **for** at least **three months**, unless otherwise restricted by law.



#### Requirement Guidance

- A visitor log documenting minimum information on the visitor will assist in identifying physical access to a building or room, and potential access to cardholder data.



## 9.4.4 Testing Procedures

<b>Observe/examine systems and settings</b>	-	
<b>Examine documentation</b>	-	
<b>Examine records</b>	Y	Visitor log
<b>Interview people</b>	-	





## Requirement 9.5

Physically secure all media

- paper and electronic media





## Requirement 9.5

Physically secure all media.



## Requirement Guidance

- Controls for physically securing media are intended to prevent unauthorized persons from gaining access to cardholder data on any type of media. 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.

## 9.5 Testing Procedures

<b>Observe/examine systems and settings</b>	-	
<b>Examine documentation</b>	Y	Physical media control procedures
<b>Examine records</b>	-	
<b>Interview people</b>	-	





## Requirement 9.5.1

Store media backups in a securely, preferably off-site facility.





### Requirement 9.5.1

Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility.

Review the location's security at least annually.



### Requirement Guidance

- If stored in a non-secured facility, backups that contain cardholder data may easily be lost, stolen, or copied for malicious intent.
- Periodically reviewing the storage facility enables the organization to address identified security issues in a timely manner, minimizing the potential risk.



## 9.5.1 Testing Procedures

<b>Observe/examine systems and settings</b>	-	
<b>Examine documentation</b>	-	
<b>Examine records</b>	Y	<b>Evidence of annual reviews</b>
<b>Interview people</b>	-	







## Requirement 9.6

Control distribution of physical media





## Requirement 9.6

Maintain **strict control** over the **internal** or **external distribution** of **any** kind of **media**, including the following:

See 9.6.1 through 9.6.3



## Requirement Guidance

- 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.

## 9.6 Testing Procedures

<b>Observe/examine systems and settings</b>	-	
<b>Examine documentation</b>	Y	<b>Distribution of media policies and procedures</b>
<b>Examine records</b>	-	
<b>Interview people</b>	-	





## Requirement 9.6.1

**Classify media** so the sensitivity of the data can be determined.



## Requirement Guidance

- It is important that media be identified such that its classification status can be easily discernible. Media not identified as confidential may not be adequately protected or may be lost or stolen.
- ***Note:** This does not mean the media needs to have a “Confidential” label attached; the intent is that the organization has identified media that contains sensitive data so it can protect it.*

It does not mean this



... There is no requirement to physically label media. Instead, companies must have processes to classify and identify all media containing cardholder data that is sensitive or confidential and ensure appropriate protection is applied to that media. ...

**<https://www.pcisecuritystandards.org/faqs> | FAQ 1129**



## 9.6.1 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Classification of media</b>
<b>Examine documentation</b>	-	
<b>Examine records</b>	-	
<b>Interview people</b>	-	





### Requirement 9.6.2

Send the **media** by **secured courier** or other delivery method that can be **accurately tracked**.



### Requirement Guidance

- Media may be lost or stolen if sent via a non-trackable method such as regular postal mail. Use of secure couriers to deliver any media that contains cardholder data allows organizations to use their tracking systems to maintain inventory and location of shipments.

# Own Distribution Network





## 9.6.2 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>-</b>	
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>Y</b>	<b>Tracking logs</b>
<b>Interview people</b>	<b>Y</b>	<b>Responsible people</b>





### Requirement 9.6.3

Ensure **management approves** any and all **media** that is **moved** from a secured area (including when media is distributed to individuals).



### Requirement Guidance

- Without a firm process for ensuring that all media movements are approved before the media is removed from secure areas, the media would not be tracked or appropriately protected, and its location would be unknown, leading to lost or stolen media.



## 9.6.3 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>-</b>	
<b>Examine documentation</b>	<b>!</b>	<b>Documented procedures</b>
<b>Examine records</b>	<b>Y</b>	<b>Tracking logs &amp; management authorization</b>
<b>Interview people</b>	<b>Y</b>	<b>Responsible people</b>





## Requirement 9.7

Validate media logs/inventories  
with the physical media



### Requirement 9.7

Maintain **strict control** over the **storage** and **accessibility** of **media**.



### Requirement Guidance

- Without careful inventory methods and storage controls, stolen or missing media could go unnoticed for an indefinite amount of time.
- If media is not inventoried, stolen or lost media may not be noticed for a long time or at all.

## 9.7 Testing Procedures

<b>Observe/examine systems and settings</b>	-	
<b>Examine documentation</b>	Y	Media storage and maintenance policy
<b>Examine records</b>	-	
<b>Interview people</b>	-	





### Requirement 9.7.1

Properly **maintain inventory logs** of all media and **conduct** media **inventories** at **least** annually.



### Requirement Guidance

- Without careful inventory methods and storage controls, stolen or missing media could go unnoticed for an indefinite amount of time.
- If media is not inventoried, stolen or lost media may not be noticed for a long time or at all.

## 9.7.1 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>-</b>	
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>Y</b>	Media inventory logs Records of annual reviews
<b>Interview people</b>	<b>!</b>	People who conducted inventories







## Requirement 9.8

Securely destroy end of life media





## Requirement 9.8

**Destroy media** when it is no longer needed for business or legal reasons as follows:

See 9.8.1.through 9.8.2



## Requirement Guidance

- 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 trashcans and recycle bins looking for information they can use to launch an attack.



## 9.8 Testing Procedures

<b>Observe/examine systems and settings</b>	-	
<b>Examine documentation</b>	<b>Y</b>	<b>Media destruction policy</b>
<b>Examine records</b>	-	
<b>Interview people</b>	-	





## Requirement 9.8.1

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

**Secure storage containers** used for materials that are to be destroyed.



## Requirement Guidance

- Securing storage containers used for materials that are going to be destroyed prevents sensitive information from being captured while the materials are being collected. For example, “to-be-shredded” containers could have a lock preventing access to its contents or physically prevent access to the inside of the container.



## 9.8.1 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Materials storage containers</b>
<b>Examine documentation</b>	<b>Y</b>	<b>Materials destruction procedures</b>
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>Y</b>	<b>Responsible people</b>





## Requirement 9.8.2

**Render** cardholder **data** on electronic media **unrecoverable** so that cardholder data **cannot be reconstructed**.

Understand  
the threat  
actor



## Requirement Guidance

- Examples of methods for securely destroying electronic media include secure wiping, degaussing, or physical destruction (such as grinding or shredding hard disks).

## 9.8.2 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Electronic data destruction methods</b>
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>!</b>	<b>Media destruction records</b>
<b>Interview people</b>	<b>!</b>	<b>Who destroyed and validated destruction</b>



# That's Fine in Theory

