

7: Restrict Access to Cardholder Data by Business Need to Know



Requirement 7

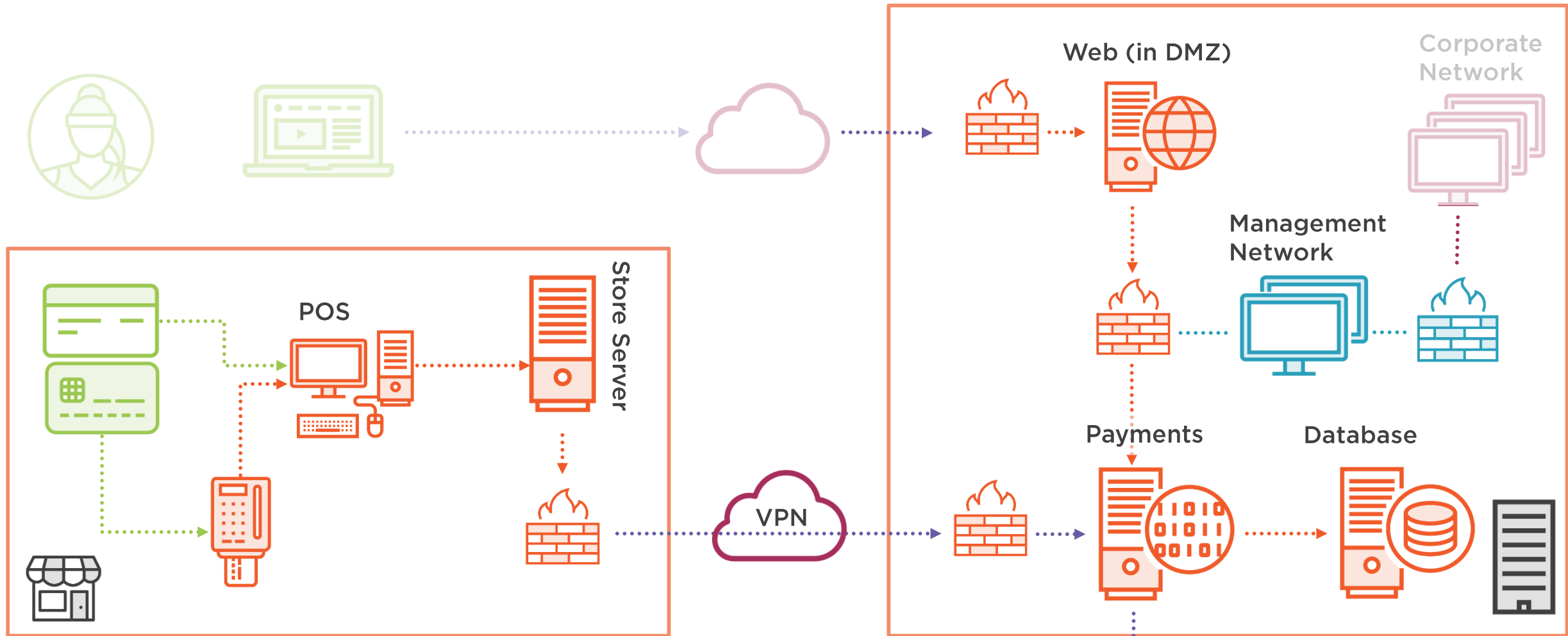


Role-based access

- Limit privileged access

Least privilege (need to know)

Policies and procedures





Requirement 7.1

Only give access to people who need it



Requirement 7.1

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



Requirement Guidance

- The more people who have access to cardholder data, the more risk there is that a user's account will be used maliciously. Limiting access to those with a legitimate business reason for the access helps an organization prevent mishandling of cardholder data through inexperience or malice.

7.1 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	Y	Access Control Policy
Examine records	-	
Interview people	-	





Requirement 7.1.1

Define roles and least privilege access



Requirement 7.1.1

Define **access** needs for each **role**, including:

System components and data resources that **each role needs** to access for their **job function**.

Level of privilege required (for example, user, administrator, etc.) for accessing resources.



Requirement Guidance

- In order to limit access to cardholder data to only those individuals who need such access, first it is necessary to define access needs for each role (for example, system administrator, call center personnel, store clerk), the systems/devices/data each role needs access to, and the level of privilege each role needs to effectively perform assigned tasks. Once roles and corresponding access needs are defined, individuals can be granted access accordingly.

7.1.1 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	Y	Role descriptions and access requirements
Examine records	-	
Interview people	-	





Requirement 7.1.2

Minimise rights given to privileged accounts

Privileged Account / User

Any user account with greater than basic access privileges.

PCI DSS Glossary





Requirement 7.1.2

Restrict access to **privileged user IDs** to **least privileges necessary** to perform job responsibilities.



Requirement Guidance

- When assigning privileged IDs, it is important to assign individuals only the privileges they need to perform their job (the “least privileges”). For example, the database administrator or backup administrator should not be assigned the same privileges as the overall systems administrator.
- Assigning least privileges helps prevent users without sufficient knowledge about the application from incorrectly or accidentally changing application configuration or altering its security settings. Enforcing least privilege also helps to minimize the scope of damage if an unauthorized person gains access to a user ID.

7.1.2 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	-	
Examine records	-	
Interview people	Y	People responsible for assigning access Management





Requirement 7.1.3

Assign access based on roles





Requirement 7.1.3

Assign **access** based on individual personnel's **job classification** and **function**.



Requirement Guidance

- Once needs are defined for user roles (per PCI DSS requirement 7.1.1), it is easy to grant individuals access according to their job classification and function by using the already-created roles.



7.1.3 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	-	
Examine records	-	
Interview people	Y	People with management responsibilities





Requirement 7.1.4

All rights granted must be explicitly authorized



Requirement 7.1.4

Require **documented approval** by **authorized parties** specifying **required privileges**.



Requirement Guidance

- Documented approval (for example, in writing or electronically) assures that those with access and privileges are known and authorized by management, and that their access is necessary for their job function.

7.1.4 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	-	
Examine records	Y	Records of approval
Interview people	-	





Requirement 7.2

Use an “access control system”

Active Directory, LDAP etc



Requirement 7.2

Establish an **access control system(s)** for systems components that restricts access based on a **user's need to know**, and is set to “**deny all**” unless specifically allowed.

This access control system(s) must include 7.2.1 through 7.2.3



Requirement Guidance

- Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. Access control systems automate the process of restricting access and assigning privileges. Additionally, a default “deny-all” setting ensures no one is granted access until and unless a rule is established specifically granting such access. Entities may have one or more access controls systems to manage user access.





Requirement 7.2.1

Coverage of **all** system components.



Requirement Guidance

- Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. Access control systems automate the process of restricting access and assigning privileges. Additionally, a default “deny-all” setting ensures no one is granted access until and unless a rule is established specifically granting such access.
Entities may have one or more access controls systems to manage user access.



Requirement 7.2.2

Assignment of privileges to individuals based on **job classification** and function.



Requirement Guidance

- Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. Access control systems automate the process of restricting access and assigning privileges. Additionally, a default “deny-all” setting ensures no one is granted access until and unless a rule is established specifically granting such access. Entities may have one or more access controls systems to manage user access.





Requirement 7.2.3

Default “deny-all” setting.



Requirement Guidance

- Without a mechanism to restrict access based on user’s need to know, a user may unknowingly be granted access to cardholder data. Access control systems automate the process of restricting access and assigning privileges. Additionally, a default “deny-all” setting ensures no one is granted access until and unless a rule is established specifically granting such access. Entities may have one or more access controls systems to manage user access.



7.2.1 – 7.2.3 Testing Procedures

Observe/examine systems and settings	Y	System settings
Examine documentation	Y	Vendor documentation
Examine records	-	
Interview people	-	





Requirement 7.3

Have policies and procedures



Requirement 7.3

Ensure that **security policies** and operational **procedures** for restricting access to cardholder data are **documented, in use,** and **known** to all affected parties.



Requirement Guidance

- Personnel need to be aware of and following security policies and operational procedures to ensure that access is controlled and based on need-to-know and least privilege, on a continuous basis.



7.3 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	Y	Security policies, Operational procedures
Examine records	-	
Interview people	Y	Responsible people and people who need to know



That's Fine in Theory

