

# Requirement 12: Maintain a Policy That Addresses Information Security for All Personnel

---



**John Elliott**

PRIVACY, PAYMENTS, SECURITY AND RISK SPECIALIST

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



## Requirement 12



Security Policy

Risk Assessment

Usage policies for “critical technologies”

Defined responsibilities with some mandatory roles

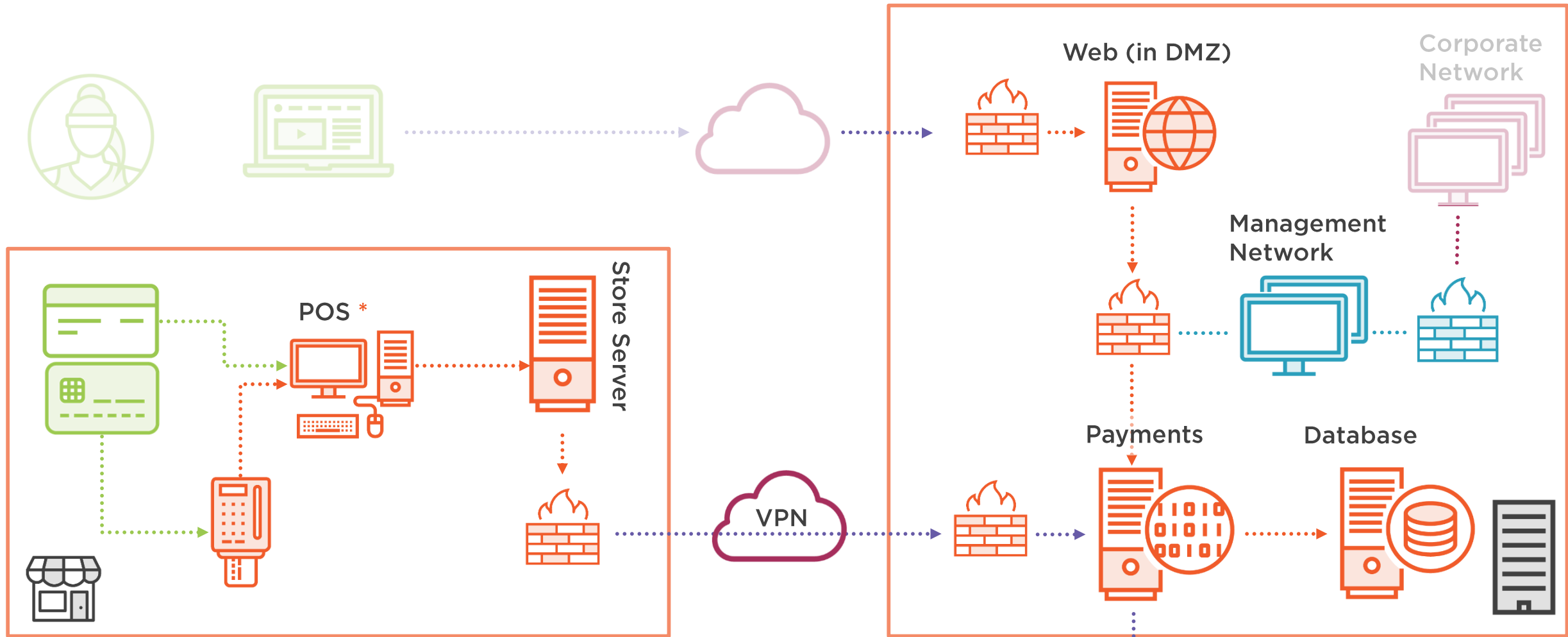
Security awareness

Personnel screening

Third party relationships

Incident response





- 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





# Requirement 12.1

Have a security policy





## Requirement 12.1

Establish, publish, maintain, and disseminate a **security policy**.



## Requirement Guidance

- A company's information security policy creates the roadmap for implementing security measures to protect its most valuable assets. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.

## 12.1 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>-</b>	
<b>Examine documentation</b>	<b>Y</b>	<b>Information security policy</b>
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>!</b>	<b>People who should use the policy</b>





## Requirement 12.1.1

Review the policy annually





### Requirement 12.1.1

**Review** the security policy **at least annually** and update the policy when the environment changes.



### Requirement Guidance

- Security threats and protection methods evolve rapidly.  
Without updating the security policy to reflect relevant changes, new protection measures to fight against these threats are not addressed.



## 12.1.1 Testing Procedures

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





## Requirement 12.2

Conduct an annual risk assessment



## Requirement 12.2

Implement a risk-assessment process that:

- Is performed at least **annually** and upon **significant changes** to the environment
- **Identifies** critical **assets**, **threats**, and **vulnerabilities**, and
- Results in a **formal, documented** analysis of risk



## Requirement Guidance

- A risk assessment enables an organization to identify threats and associated vulnerabilities with the potential to negatively impact their business.
- Resources can then be effectively allocated to implement controls that reduce the likelihood and/or the potential impact of the threat being realized.
- Performing risk assessments at least annually and upon significant changes allows the organization to keep up to date with organizational changes and evolving threats, trends, and technologies.



PLURALSIGHT

Products ▾

Courses ▾

View plans

Resources ▾

Call us +441173741780



# Defending Against JavaScript Keylogger Attacks on Payment Card Information



By John Elliott and Troy Hunt

In this course, you'll learn how about the most common attack now used to steal payment card data and the possible defences.

START A FREE 10-DAY TRIAL

▶ PLAY COURSE OVERVIEW





## Requirement 12.2

Implement a risk-assessment process that:

- Is performed at least **annually** and upon **significant changes** to the environment
- **Identifies** critical **assets**, **threats**, and **vulnerabilities**, and
- Results in a **formal, documented** analysis of risk



## Requirement Guidance

- A risk assessment enables an organization to identify threats and associated vulnerabilities with the potential to negatively impact their business.
- Resources can then be effectively allocated to implement controls that reduce the likelihood and/or the potential impact of the threat being realized.
- Performing risk assessments at least annually and upon significant changes allows the organization to keep up to date with organizational changes and evolving threats, trends, and technologies.

## 12.2 Testing Procedures

<b>Observe/examine systems and settings</b>	-	
<b>Examine documentation</b>	Y	<b>Policies and procedures, documentation</b>
<b>Examine records</b>	-	
<b>Interview people</b>	-	





## Requirement 12.3

Usage policies for *critical* technologies



# Critical Systems / Technologies

A system or technology that is deemed by the entity to be of particular importance. For example, a critical system may be essential for the performance of a business operation or for a security function to be maintained. Examples of critical systems often include security systems, public-facing devices and systems, databases, and systems that store, process, or transmit cardholder data.

**PCI DSS Glossary**





# ~~Critical Technologies~~ End-user Technologies

Which if not correctly used can  
cause security vulnerabilities



# “Critical” Technologies



**Note:** Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.



### Requirement 12.3

Develop **usage policies** for critical technologies and define proper use of these technologies.

Ensure these usage policies require the following:  
(12.3.1 thru 12.3.10):

**Remember that this only applies to people and technologies in scope of PCI DSS**



### Requirement Guidance

- Personnel usage policies can either prohibit use of certain devices and other technologies if that is company policy, or provide guidance for personnel as to correct usage and implementation.  
If usage policies are not in place, personnel may use the technologies in violation of company policy, thereby allowing malicious individuals to gain access to critical systems and cardholder data.





### Requirement 12.3.1

Explicit approval by authorized parties.



### Requirement Guidance

- Without requiring proper approval for implementation of these technologies, individual personnel may innocently implement a solution to a perceived business need, but also open a huge hole that subjects critical systems and data to malicious individuals.



### Requirement 12.3.2

Authentication for use of the technology



### Requirement Guidance

- If technology is implemented without proper authentication (user IDs and passwords, tokens, VPNs, etc.), malicious individuals may easily use this unprotected technology to access critical systems and cardholder data.



### Requirement 12.3.3

A list of all such devices and personnel with access.



### Requirement Guidance

- Malicious individuals may breach physical security and place their own devices on the network as a “back door.” Personnel may also bypass procedures and install devices. An accurate inventory with proper device labeling allows for quick identification of non-approved installations



#### Requirement 12.3.4

A method to accurately and readily determine owner, contact information, and purpose  
(for example, labeling, coding, and/or inventorying of devices)



#### Requirement Guidance

- Malicious individuals may breach physical security and place their own devices on the network as a “back door.” Personnel may also bypass procedures and install devices. An accurate inventory with proper device labeling allows for quick identification of non-approved installations.
- Consider establishing an official naming convention for devices, and log all devices with established inventory controls. Logical labelling may be employed with information such as codes that can correlate the device to its owner, contact information, and purpose.



### Requirement 12.3.5

Acceptable uses of the technology



### Requirement Guidance

- By defining acceptable business use and location of company-approved devices and technology, the company is better able to manage and control gaps in configurations and operational controls, to ensure a “back door” is not opened for a malicious individual to gain access to critical systems and cardholder data.







### Requirement 12.3.6

Usage policies must require acceptable network locations for the technologies



### Requirement Guidance

- By defining acceptable business use and location of company-approved devices and technology, the company is better able to manage and control gaps in configurations and operational controls, to ensure a “back door” is not opened for a malicious individual to gain access to critical systems and cardholder data.



### Requirement 12.3.7

List of company-approved products



### Requirement Guidance

- By defining acceptable business use and location of company-approved devices and technology, the company is better able to manage and control gaps in configurations and operational controls, to ensure a “back door” is not opened for a malicious individual to gain access to critical systems and cardholder data.





### Requirement 12.3.8

Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity



### Requirement Guidance

- Remote-access technologies are frequent "back doors" to critical resources and cardholder data.
- By disconnecting remote-access technologies when not in use (for example, those used to support your systems by your POS vendor, other vendors, or business partners), access and risk to networks is minimized





### Requirement 12.3.9

Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use



### Requirement Guidance

- Remote-access technologies are frequent "back doors" to critical resources and cardholder data.
- By disconnecting remote-access technologies when not in use (for example, those used to support your systems by your POS vendor, other vendors, or business partners), access and risk to networks is minimized





## Requirement 12.3.10

Be careful with remote access to cardholder data

- copy and move only with policy





### Requirement 12.3.10

For personnel accessing **cardholder data via remote-access technologies**, **prohibit** the **copying**, **moving**, and **storage** of it onto local hard drives and removable electronic media, **unless explicitly authorized for a defined business need**. Where there is a need, the usage policies must require the data be protected in accordance to all applicable PCI DSS Requirements.



### Requirement Guidance

- To ensure all personnel are aware of their responsibilities to not store or copy cardholder data onto their local personal computers or other media, your policy should clearly prohibit such activities except for personnel that have been explicitly authorized to do so. Storing or copying cardholder data onto a local hard drive or other media must be in accordance with all applicable PCI DSS requirements.

## 12.3 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Remote access</b>
<b>Examine documentation</b>	<b>Y</b>	<b>Usage policies</b>
<b>Examine records</b>	<b>Y</b>	<b>Authorizations</b>
<b>Interview people</b>	<b>Y</b>	<b>Responsible people</b>





It's perfectly acceptable to have a policy that says:

“technology XYZ is not permitted to be used in the cardholder data environment”







## Requirement 12.4

Define information security responsibilities



#### Requirement 12.4

Ensure that the **security policy** and procedures clearly define **information security responsibilities** for all personnel



#### Requirement Guidance

- Without clearly defined security roles and responsibilities assigned, there could be inconsistent interaction with the security group, leading to unsecured implementation of technologies or use of outdated or unsecured technologies.

## 12.4 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>-</b>	
<b>Examine documentation</b>	<b>Y</b>	<b>Information security policies</b>
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>Y</b>	<b>Responsible people</b>





## Requirement 12.4.1

For service providers only

Assign overall accountability for PCI DSS compliance



## Requirement 12.4.1

### *Service providers only:*

Executive management shall establish **responsibility** for the protection of CD and a PCI DSS compliance program to include:

1. **Overall accountability** for maintaining PCI DSS compliance
2. **Defining a charter for a PCI DSS compliance program** and communication to **executive management**



## Requirement Guidance

- *Note: Only applicable when the entity being assessed is a service provider.*
- Executive management assignment of PCI DSS compliance responsibilities ensures executive level visibility into the PCI DSS compliance program and gives the opportunity to ask questions to determine the effectiveness of the program and influence strategic priorities. Overall responsibility may be assigned to individual roles and/or business units.
- The detail provided to executive management should be appropriate for the particular organization and the intended audience.





“We the organization commit to achieving and maintaining compliance with PCI DSS by the following activities...”

*John Hancock*



“Executive management may include C-level positions, board of directors, or equivalent. The specific titles will depend on the particular organizational structure.”

**Guidance to requirement 12.4.1**



## 12.4.1 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>-</b>	
<b>Examine documentation</b>	<b>Y</b>	<b>Accountability documentation PCI DSS charter</b>
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>!</b>	<b>The accountable person</b>







## Requirement 12.5

Assign five specific information security management responsibilities





### Requirement 12.5

Assign to an individual or team the following information security management responsibilities.



### Requirement Guidance

- Each person or team with responsibilities for information security management should be clearly aware of their responsibilities and related tasks, through specific policy. Without this accountability, gaps in processes may open access into critical resources or cardholder data. Entities should also consider transition and/or succession plans for key personnel to avoid potential gaps in security assignments, which could result in responsibilities not being assigned and therefore not performed.

# Requirement 12.5 Testing Procedure



**Examine information security policies and procedures to verify:**

- 1. The formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management.**
- 2. The following information security responsibilities are specifically and formally assigned:**



### Requirement 12.5.1

Establish, document, and distribute security policies and procedures.



### Requirement Guidance

- Each person or team with responsibilities for information security management should be clearly aware of their responsibilities and related tasks, through specific policy. Without this accountability, gaps in processes may open access into critical resources or cardholder data. Entities should also consider transition and/or succession plans for key personnel to avoid potential gaps in security assignments, which could result in responsibilities not being assigned and therefore not performed.





### Requirement 12.5.2

Monitor and analyze security alerts and information, and distribute to appropriate personnel.



### Requirement Guidance

- Each person or team with responsibilities for information security management should be clearly aware of their responsibilities and related tasks, through specific policy. Without this accountability, gaps in processes may open access into critical resources or cardholder data. Entities should also consider transition and/or succession plans for key personnel to avoid potential gaps in security assignments, which could result in responsibilities not being assigned and therefore not performed.



### Requirement 12.5.3

Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.



### Requirement Guidance

- Each person or team with responsibilities for information security management should be clearly aware of their responsibilities and related tasks, through specific policy. Without this accountability, gaps in processes may open access into critical resources or cardholder data. Entities should also consider transition and/or succession plans for key personnel to avoid potential gaps in security assignments, which could result in responsibilities not being assigned and therefore not performed.





#### Requirement 12.5.4

Administer user accounts, including additions, deletions, and modifications



#### Requirement Guidance

- Each person or team with responsibilities for information security management should be clearly aware of their responsibilities and related tasks, through specific policy. Without this accountability, gaps in processes may open access into critical resources or cardholder data. Entities should also consider transition and/or succession plans for key personnel to avoid potential gaps in security assignments, which could result in responsibilities not being assigned and therefore not performed.



### Requirement 12.5.5

Monitor and control all access to data.



### Requirement Guidance

- Each person or team with responsibilities for information security management should be clearly aware of their responsibilities and related tasks, through specific policy. Without this accountability, gaps in processes may open access into critical resources or cardholder data. Entities should also consider transition and/or succession plans for key personnel to avoid potential gaps in security assignments, which could result in responsibilities not being assigned and therefore not performed.





## 12.5 Testing Procedures

<b>Observe/examine systems and settings</b>	-	
<b>Examine documentation</b>	Y	<b>Information security policies and procedures</b>
<b>Examine records</b>	-	
<b>Interview people</b>	-	





# Requirement 12.6

## Security awareness

Requirement 12 | Maintain a policy that addresses information security for all personnel





### Requirement 12.6

Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.



### Requirement Guidance

- If personnel are not educated about their security responsibilities, security safeguards and processes that have been implemented may become ineffective through errors or intentional actions.



## 12.6 Testing Procedures

<b>Observe/examine systems and settings</b>	-	
<b>Examine documentation</b>	Y	Security awareness program, procedures and documentation
<b>Examine records</b>	-	
<b>Interview people</b>	-	





### Requirement 12.6.1

Educate personnel upon hire and at least annually.

***Note:** Methods can vary depending on the role of the personnel and their level of access to the cardholder data.*



### Requirement Guidance

- If the security awareness program does not include periodic refresher sessions, key security processes and procedures may be forgotten or bypassed, resulting in exposed critical resources and cardholder data

**Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web-based training, meetings, and promotions).**



## 12.6.1 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>-</b>	
<b>Examine documentation</b>	<b>Y</b>	<b>Security awareness program</b>
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>Y</b>	<b>Sample of trained people</b>





### Requirement 12.6.2

Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.



### Requirement Guidance

- Requiring an acknowledgement by personnel in writing or electronically helps ensure that they have read and understood the security policies/procedures, and that they have made and will continue to make a commitment to comply with these policies.

## 12.6.2 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>-</b>	
<b>Examine documentation</b>	<b>Y</b>	<b>Security awareness program</b>
<b>Examine records</b>	<b>!</b>	<b>Records of attestation &amp; understanding</b>
<b>Interview people</b>	<b>-</b>	







## Requirement 12.7

Screen personnel before hiring



## Requirement 12.7

Screen potential personnel prior to hire to minimize the risk of attacks from internal sources.

***Note:** For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.*



## Requirement Guidance

- Performing thorough background investigations prior to hiring potential personnel who are expected to be given access to cardholder data reduces the risk of unauthorized use of PANs and other cardholder data by individuals with questionable or criminal backgrounds.



# Screening



**You decide what screening is appropriate**

**It's not mandatory for people who process a single card at a time**

**Local laws may apply and take precedence over PCI DSS**



## 12.7 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>-</b>	
<b>Examine documentation</b>	<b>!</b>	<b>Policies and the risk assessment</b>
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>Y</b>	<b>HR department management</b>



# That's Fine in Theory

