more security. usd

ConCardis

Hotel Payment Card Security

How PCI DSS Secures Your Business Operations Long-Term

ConCardis GmbH
Helfmann-Park 7
65760 Eschborn
Germany

www.concardis.com

Table of Contents

1. Attack Target: Payment Card Information

1.1. Why PCI DSS?

Payment card data are a very sought after target for criminals. They can be stolen easily especially from smaller companies and turned into money with relatively little effort. The hotel industry is a particularly frequent victim of payment card theft. Whether the attacks are made by professional hackers or malicious insiders, the criminals are usually optimally organized, and the business with stolen payment card information is flourishing.

Discovery of a theft of payment card information initially leads to a series of costly investigations. These investigations are followed by claims for damages and penal fines. Finally, publication of the incident by the press results in a loss of reputation that is extremely difficult to recover. Customer confidence dwindles, and your business suffers for a longer period of time.

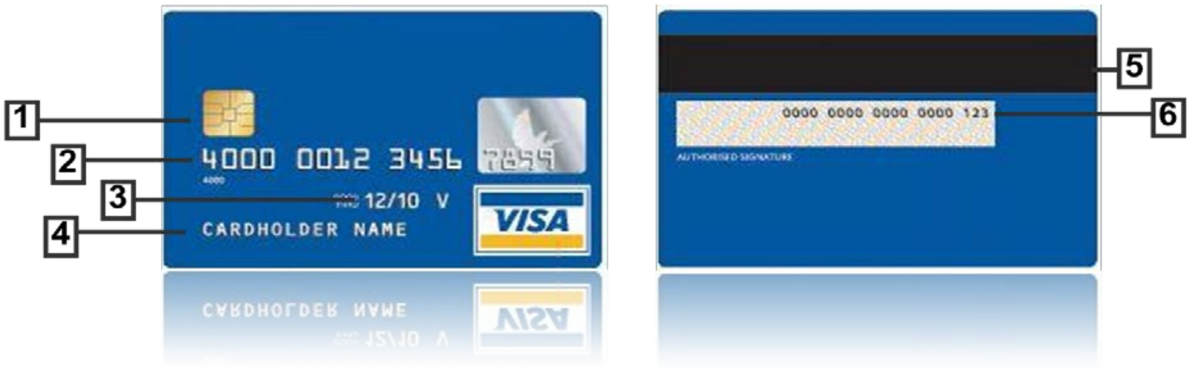
To counteract this development, the large payment card companies teamed up and founded the Payment Card Industry Security Standards Council (PCI SSC). The PCI Data Security Standard (PCI DSS) was developed by standardizing the security guidelines of the individual companies. It provides the basis for a standardized approach to protecting payment card data and includes both technical and organizational measures. If these measures have been implemented, they interact to provide a minimum level of security of payment card information.

Proof of the PCI DSS conformity of your company can significantly influence the question of liability in case a payment card theft is detected. However, you must provide evidence that you had implemented and complied with all measures specified by the PCI standard at the time of the incident.

Nevertheless, if nothing else, you as a hotel operator must remember that by ensuring the security of the payment card data of your customers, you are also securing your own source of income.

1.2. What are criminals targeting?

Payment card data are located on the card in the form of an inscription, on the chip and on the magnetic strip. The following illustration shows the structure of a typical payment card:



1. Chip
2. Card number (Primary Account Number, PAN)
3. Validity date
4. Cardholder name
5. Magnetic strip
6. Card validation code, card verification number

Criminals are most interested in obtaining the following payment card data: the payment card number (PAN) and the card verification number (CVC2/CVV2/…), as well as the complete magnetic strip so that they can produce an illegal copy of the card. This information can be relatively easily turned into money on the thriving black market for stolen payment cards. The risk of being caught is comparatively low for the criminals. They are usually optimally organized and operate internationally. It is almost impossible to trace their activities.

But what value does this stolen information have? Stolen credit cards can be used without problems to conduct payment transactions for which the payment card must not be physically available, for example, for online purchases in the Internet. The goods are then delivered to or sold by go-betweens using sophisticated channels.

When using payment terminals, there is the risk that such terminals have been manipulated so that the magnetic strip can be “copied.” The magnetic strip data is read out during the payment transaction and transmitted to the attacker. The attacker can then copy the stolen data on a “blank” payment card and physically use this card for payments.

The PCI DSS measures focus on potential attack channels and thereby offer a minimum level of protection for payment card information.

2. The Path to PCI DSS Conformity

2.1. How to get started?

We recommend that you first make a list of where and how payment card information is processed in your hotel. In doing so, you should consider the entry point and the channels through which payment card information enters the hotel, the channels through which it is transmitted within the hotel and, if applicable, how the information leaves the hotel again.

Business Process	Area	Medium that contains the payment card data	Further processing of payment card data
Customer pays the costs of the hotel stay with a payment card and hands over the payment card to the employee at the reception desk	Reception Desk	Paper	Reception desk employee pulls the card through the terminal, then returns it to the customer and retains a paper voucher that is stored in a lockable cabinet or drawer
Paper vouchers collected at the reception desk during the day are forwarded to the accounting department	Reception Desk/ Accounting Department	Paper	Accounting department receives the paper vouchers and checks payment receipt. Paper vouchers are then archived for the statutory record retention period (in a lockable archive)
Service provider picks up the paper vouchers for disposal following expiration of the statutory record retention period	Accounting Department/ Archive	Paper	Service provider properly disposes of paper vouchers
Customer sends a reservation query per e-mail including his/her payment card information (although this is actually not desired)	Reception Desk/Reservation Dept.	Digital	E-mail is printed out and directly deleted from the mailbox
…			

Such a list provides you with an overview of potential risk and serves at the same time as a starting point for the measures to be implemented. The above list shown is certainly not complete and should only be considered as an example.

You should pay particular attention to the sections in the list where payment card data is available in electronic (digital) form. Information stored on computers is easy prey for hackers. If they succeed in gaining access to a hotel's internal network, they can steal large quantities of payment card data. As hackers don't have to be physically present on-site, the risk of being discovered is relatively small for them.

Due to the high risk to which digitally stored payment card data is exposed, the PCI Security Standard foresees very comprehensive measures to appropriately protect such data. You can significantly reduce the scope of measures to be implemented to protect payment card information and thereby the cost of achieving PCI DSS conformity by refraining from using any kind of electronic data storage!

That's why in this connection you must clarify the question of whether you really need to store payment card information in electronic form or whether you can do without such storage.

For example, hotels frequently receive e-mails from customers that contain payment card data. If you do not immediately delete such e-mails, then you are considered to be electronically storing payment card data. You can avoid such problems by printing out questionable e-mails and further processing the payment card data only in paper form. Then you can completely delete the e-mail from your computer directly following print-out thereof. You must also empty your trash basket / “deleted object folder”!

As a general policy: You should always forego electronic storage of payment card data unless it is necessary!

2.2. Why is proof of your PCI DSS conformity important?

In many cases of payment card theft, subsequent investigations repeatedly determine that one or more of the required PCI DSS measures had not been implemented. The consequences of such incidents include, among others, claims for damages, penal fines, a loss of reputation and a corresponding loss of customers

As you can see, such an incident can cause significant damage and lead to long-term adverse effects on your business.

2.3. Proof of PCI DSS conformity based on Self-Assessment Questionnaires

The Self-Assessment Questionnaires (SAQ) offer small companies a practicable and efficient method of verifying their PCI DSS conformity. The SAQ have been adapted to meet a company’s specific requirements in line with its business model. You must fill out and submit the SAQ once per year. This enables you to check the measures you implemented and/or to adapt them to suit possible changes in your business processes that were made and, if necessary, to select a new appropriate SAQ category.

2.4. Selecting the appropriate SAQ

Your business processes determine which SAQ is appropriate for you. Five SAQ categories have been established to enable you to adequately self-assess the PCI DSS conformity of your own business environment. The criteria on which the various categories are based are shown in the right column of the table below. Electronic storage of payment card data is a key influencing factor. If this is the case, you must always use SAQ Category D.

You can obtain the SAQ that you must fill out on the ConCardis PCI DSS Platform that supports you on the way to achieving PCI DSS conformity. After you register on the platform, the SAQ Selection Assistant will help you in selecting the appropriate SAQ.

You can register on the ConCardis PCI DSS Platform under the following link:
https://www.pciplatform.concardis.com/

Please remember that you must have received your initial login data from ConCardis prior to registration.

As an alternative, you can also obtain the appropriate SAQ from your merchant bank or as a download from the PCI SSC website at: https://www.pcisecuritystandards.org/security_standards/documents.php.

Example: Payments are made in my hotel with payment cards using two ISDN terminals. One terminal is located at the reception desk, the other in the dining hall area. These devices do not store payment card data but generate a paper voucher once payment has been completed. Thereafter, we only use the paper voucher for further processing (in the accounting department, etc.). We immediately delete e-mails that contain payment card information from our incoming mail and our trash basket / “deleted object folder.” That means that we have to fill out the Category B SAQ.

SAQ Category	Scope	Target Group/Characteristics
A	13 Questions	▪ All payment card functions have been outsourced ▪ No physical presence of payment cards (that is, only E-commerce or mail order business)
B	29 Questions	▪ Only terminals with dial-up connection (ISDN or analog) are used for payment card payments ▪ No electronic storage of payment card data (also not by the terminal!!)
C-VT	51 Questions	▪ Payment handling is only made using web-based virtual terminals ▪ The computer on which the virtual terminal is used may not be connected with any other merchant system ▪ No electronic storage of payment card data
C	80 Questions	▪ Payment card terminals and/or payment application systems that are connected with the Internet are used ▪ The payment card terminals and/or payment application systems may **only** be connected with the Internet and **with no other** merchant system ▪ No electronic storage of payment card data
D	288 Questions	▪ All that are not contained in the descriptions for SAQ A through C ▪ All service providers

2.5. Important Supplementary Information about Selection of the Correct SAQ

Frequently, selection of the SAQ to be applied is suboptimal due to a lack of detailed knowledge about the requirements of the PCI DSS Security Standard. As a result, Category D SAQ is selected for application although classification in a different category would certainly be possible by making minor changes. This is primarily due to improper conduct of employees and the existing infrastructure. However, these could be adapted relatively easily to enable application of a Category A, B. or C SAQ. By taking this approach, you benefit from the significantly narrower scope of the security measures to be implemented to comply with the PCI DSS Security Standard.

We describe below a number of frequently observed scenarios that require application of the Category D SAQ. We also provide concise guidance for each of these scenarios for circumventing the applicability of SAQ D to significantly simplify achievement of your PCI DSS conformity.

Payment card information is available in electronic form

It frequently happens that payment card data is electronically stored in different locations, for example, in the files of word processing or table calculation programs, but the associated risks thereof are not recognized. In addition, e-mails that contain payment card information are frequently not deleted in electronic mailboxes. You can print out e-mails and further process them on paper. If you delete e-mails immediately after printing them out, and delete them also from your trash basket and the “deleted object folder,” then you are not considered to be using electronic storage in the sense of PCI DSS. If you are not certain whether payment card data is stored in electronic form in your systems, special software can help you to find out. We recommend that you conduct an initial check of your current systems. Your IT service provider should be able to support you in doing so.

SAQ D becomes immediately applicable if you store payment card information in electronic form in your hotel! That's why we would like to repeat again here that you should forego all forms of electronic storage of payment card data insofar as such storage is not absolutely necessary!

Lack of Network Segmentation

The PCI DSS Security Standard requires that systems that process payment card data be separated from systems that do not need to access this information. In particular, isolation of payment card data processing systems is a mandatory prerequisite for application of SAQ C. Payment card terminals and/or payment application systems may only be connected with the Internet and with no other merchant system. This is intended to reduce the risk of a theft of payment card information.

The use and suitable configuration of firewalls and routers can prevent communication between systems that process payment card data and other hotel systems to achieve the desired segmentation. The objective is to prevent access of systems that do not process payment card data to systems that work with payment card data. Your IT service provider should be able to support you with the implementation.

If isolation of the payment card data processing systems is not in place, then you must implement comprehensive measures for your entire network to protect these systems. That means that you have to apply SAQ D!

Secure Access during Remote Maintenance

Software providers frequently offer their customers the option of remote maintenance to be able to efficiently solve problems. An inadequately secured remote access harbors a significant risk potential and can enable a hacker to steal security-critical information.

If you provide remote access to your systems to your IT service provider or a manufacturer in connection with maintenance and support work, you must adequately secure such access. Only encrypted communications may be used. In addition, you may only grant access via an account that has been established especially for remote access. This account may only be active when it is needed. It must not provide a permanent access capability. Remote access must be monitored during use. Your IT service provider or respective software supplier should be able to assist you in implementing the necessary measures.

You must apply SAQ D if you allow remote access to your systems without the corresponding security measures!

In most cases, you can avoid applicability of SAQ D by following our recommendations and thereby achieve your PCI DSS conformity in a more efficient way.

3. Measures to achieve PCI DSS Compliance for Hotels (SAQ B)

- Payment card data are processed only by ISDN terminals and on paper vouchers.
- No electronic storage of payment card information.

3.1. Application Area

The information provided below corresponds with that of Category B SAQ. That means they refer to a business environment in which payment card data are only processed on paper and with payment terminals via ISDN lines. No data are stored electronically. If these characteristics do not apply to the business processes in your hotel, you should recheck in Section 2.4 above “Selecting the appropriate SAQ” which SAQ category would apply for you or check with your merchant bank. It is important that you as a first step determine the correct category for your hotel as the measures described below are only complete for Category B business environments.

You can obtain the SAQ that is appropriate for your business processes from your merchant bank (acquirer) or download it from the PCI SSC website at http://de.pcisecuritystandards.org/minisite/en/saq-v2.0-documentation.php.

3.2. Access to Payment Card Information

Potential Risk

You should only grant access to payment card data to those employees that require such access for their work. The risk that such data goes astray obviously increases the greater the number of people who have access to such sensitive data. This must not necessarily be due to a malicious insider. It can simply result from a lack of knowledge about how sensitive information must be handled.

Measures

As a consequence thereof, you should only grant access rights in such a way that each employee only has the access rights needed for his/her job tasks. This includes access to computers as well as physical access to cabinets, drawers and offices. You should only give a computer access password to those employees that need such access for their work. Analogously, you should only give keys for payment card information storage locations to those employees that need this for their work. In doing so, you should consider all data storage locations, for example, the cabinets in the back office and in the accounting department as well as the drawer at the reception desk. If an employee is no longer employed by the hotel, you must check whether this employee had special access rights. You must change the password if he/she had access to a computer. Of course, you must also demand the return of keys that you had given to such employees.

Tasks to be completed from this section

Review access rights (Who has access to computers/data storage locations?) □

Make necessary modifications, if applicable □

3.3. Handling E-Mails

Potential Risk

Customers frequently, send an e-mail containing their payment card data to a hotel, for example, to make a reservation. This means anyone can read such an e-mail that has access to the respective computer.

Note: In this section, we describe only the case in which customers send reservation e-mails to you containing payment card information from time to time although this is unwanted. However, if you solicit/accept e-mails containing payment card information as part of a standard business process, then you should stop processing this list of measures here. You must then fill out the Self-Assessment Questionnaire D and implement significantly more comprehensive security measures. In this case, you should request professional security support from your merchant bank (acquirer).

Measures

You should delete the e-mail immediately following receipt thereof. You must ensure that such e-mails are also deleted from the trash basket/“deleted object folder” and that no copies of such e-mails are stored for archiving purposes on a central e-mail server. If you need the information, then we recommend that you print out the e-mail and further process the data in paper form. We describe how to handle print-outs containing payment card information in the next section.

Tasks to be completed from this section

Instruct employees that have computer access how to handle e-mails □

3.4. Handling Print-Outs and Paper Vouchers

Potential Risk

You can typically find payment card information on several different kinds of documents in a hotel. These documents include mainly print-outs, faxes and payment terminal vouchers. If you carelessly handle these documents, the payment card information they contain are easy prey for a malicious employee.

Measures

You must store paper documents containing payment card information in lockable cabinets or drawers wherever such information is processed. You should, for example, never stack print-outs and vouchers at the reception desk where they could be seen by others. As a general rule, you should classify such documents as confidential and train employees that handle such documents regarding the sensitivity of the information they contain.

PCI DSS forbids any kind of storage of so-called sensitive authentication data that in the case of payment cards also includes among other data the card verification number and PIN. However, hotel operators normally never have access to the PIN. Nevertheless, if a customer e-mail contains, for example, a card verification number, then you must also make this number illegible (blacken it out) on the print-out. You must also make sure that only those employees have access to the vouchers who need them to complete their work tasks. That's why you must strictly control and document in writing the names of those employees that have keys to the data storage locations.

When disposing of print-outs, vouchers and other paper documents containing payment card data, you must confirm that these documents have actually and irretrievably been destroyed. They belong in the shredder and not just in the paper basket. Documents can be shredded in such a way that they cannot be reconstructed by using a cross cut/particle cut shredder. That means that if you shred documents in-house, you should check whether the shredder you purchase provides this kind of shredding.

The DIN Standard 32757-1 defines five security levels. The standard recommends a shredder of at least Security Class 3 for reliable destruction of sensitive information.

If you engage a service provider for document disposal, you must ensure that the service provider accepts responsibility for proper destruction of the documents. You should include a clause covering this subject in the written agreement with your respective service provider. Frequently, documents are not immediately destroyed in such a situation but are first collected. That means that the container in which these documents are stored must be protected against access by unauthorized persons. For instance, if documents are stored in a cabinet, you should at least secure the cabinet with a lock.

Tasks to be completed from this section

Store print-outs, faxes and vouchers with payment card information in a locked-up location. □

Blacken out highly sensitive information on print-outs □

Inform employees about how to properly handle print-outs and paper vouchers □

Ensure that payment card data is irretrievably destroyed during disposal □

Ensure that your service provider correctly disposes of documents and assumes responsibility for doing so □

3.5. The Payment Terminal

Potential Risk

As a general rule, you should refrain from electronically storing payment card information unless such storage is absolutely necessary. The (SAQ Category B) measures described in this section are based on the assumption that you do not store payment card data in digital form. However, it is possible that payment card data is stored on older devices. Normally, this should not be the case with more modern card terminals. Modern payment devices should also be tamper-proof. You can frequently find a corresponding security seal affixed to such a payment terminal. Security seals were introduced in response to thefts of payment card information via manipulated card terminals that occurred in the past.

Measures

You should contact the service provider who delivered your payment terminal if you are not certain whether the terminal is tamper-proof or stores card data. Ask your service provider whether this device complies with the payment card security standards. You can also check whether your card terminal has been validly certified according to PCI PTS (PIN Transaction Security) on the PCI Council website. If this is the case, then you can assume that the device complies with PCI DSS requirements. You can find a list of certified card terminals under the following link:
https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

Tasks to be completed from this section

Contact the service provider or manufacturer of the card terminal you use

(or verify certification of the device on the PCI Council website) □

Clarify whether your card terminal complies with the payment card security standards □

Clarify whether your card terminal is tamper-proof □

Clarify whether your card terminal stores payment card data □

If yes: Clarify whether this data can be securely deleted □

3.6. Security Documents

The PCI standard requires that you prepare and keep certain types of documents up-to-date to help you keep track of compliance of the various measures. In addition, written documentation is the best method of subsequently verifying your PCI conformity vis-à-vis third parties. We therefore recommend that you prepare/keep updated concise and pragmatic documentation on the following subjects:

Information Security Guideline

An information security guideline should describe the handling of all security-critical issues within your hotel. PCI DSS does not require at this point that you prepare a complex reference work, but the guideline should contain a short description of all security-relevant topics. Key topics include secure handling of payment card information and also secure handling of computers and the software installed on them. It is particularly important that you instruct your employees that payment card information should never be sent by unprotected e-mail.

People often use so-called “messaging technologies for end-users” to communicate with each other. However, with these technologies you cannot suitably protect the data to be transmitted. That's why you should never use these technologies to transmit payment card data. The term end-user technologies includes in general unencrypted e-mails, Instant Messenger and chat programs such as ICQ or Skype. These messages can be easily intercepted and read using software that is freely available in the Internet. Most of these programs do not offer any way to encrypt such messages. You should refrain entirely from communicating via software that can only transmit unencrypted messages due to the increased risk involved. We recommend that you prepare a work instruction that prohibits the use of risky technologies as this is the best way to resolve this problem. You should inform your employees about the associated risks so that they understand why they should not use these technologies.

You must sensitize your employees about the fact that the security of the payment card data of your customers is a critical, long-term key success factor for your business and that ensuring this security is in their own interest. You should offer your employees a security training course, if possible. You can also sensitize your employees, for example, by using posters or screensavers at their workplaces to remind them of data security requirements.

You should also distribute a copy of your information security guideline to each employee and have the employee confirm by signature on a form that he/she has read and understood the guideline.

You should review the guideline annually to ensure that it is up-to-date, and modify it, if applicable, to reflect changes that have been made.

Work Instruction for Employees with Access to Payment Card Data

A work instruction for employees that handle payment card data should remind employees that they are handling sensitive information and inform them how to correctly handle such information. This includes information from the Sections “Handling E-Mails” and “Handling Print-Outs and Paper Vouchers.”

List of Computer Access and Data Storage Location Access Authorizations

The list of computer access and data storage location access authorizations should include those employees that use the computer with its electronic mailbox and/or have a key to the print-out and paper voucher storage locations. This list and your duty roster enable you to reconstruct who had access to payment card information at a given point in time.

List of External Service Providers

If you have agreements with external service providers that come into contact with payment card data, then you must properly inform them regarding the sensitivity of such data. You should include a clause in your contractual agreement that specifies that the service provider bears co-responsibility for the security of payment card data which applies as soon as the service provider comes into contact with such data. For example, a service provider who has been engaged to destroy payment card data must be clearly aware that he/she is responsible for proper disposal of such data. A list containing all your external service providers helps you to keep track of the above.

The large payment card companies maintain their own lists in which you can confirm the PCI DSS conformity of service providers and manufacturers involved with the payment card business. These lists are published on the respective websites and are accessible to the general public.

You can find the MasterCard list under the following link:
http://www.mastercard.com/us/company/en/whatwedo/compliant_providers.html

You can find the Visa Europe list of certified service providers under the following link:
http://www.visaeurope.com/en/businesses__retailers/payment_security/service_providers.aspx

In particular, if you process payment card data with payment applications and thus fall under the applicability of SAQ C, you can verify whether the software you use complies with the requirements of the PCI Payment Application Data Security Standard (PCI PA-DSS) on the PCI Council website. You can simplify implementation of measures to achieve your PCI DSS conformity by using certified software. You can check whether and which version of a payment application is certified according to PCI PA-DSS under the following link to the PCI Council website:
https://www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php

You can also find out whether the card terminal you use is certified under the following link to the PCI Council website:
https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

You must check the PCI DSS conformity status of service providers once per year.

Tasks to be completed from this section

Prepare an information security guideline □

Prepare a work instruction for employees with access to payment card data □

Prepare a list of computer access and data storage location access authorizations □

Prepare a list of external service providers □

Review the PCI DSS conformity status of service providers □

3.7. Successfully Securing Payment Card Data Over Time

The measures we describe in this section provide a minimum level of protection of payment card data for business models that exclusively involve payment card processing via terminals with a dial-up connection and paper vouchers. You can implement all measures and achieve basic protection in an efficient and practicable way by foregoing electronic storage of payment card information.

You must fill out the SAQ once per year and, if applicable, submit it to your merchant bank to maintain your PCI conformity. This enables you to check the measures you implemented and/or to adapt them to suit changes that may have been made in your business processes and, if necessary, to select an appropriate SAQ category.

However, achievement/proof of PCI conformity alone is not sufficient to sustainably protect payment card data. You can only achieve effective, ongoing protection if you and your employees truly internalize the measures. All persons involved must work together to do so.

Bottom line, you should protect customer data not only considering possible liability claims but also to secure the future and competitiveness of your business long-term.

3.8. Attachment A: Checklist

Are you familiar with the payment card handling flow in your hotel?	□
Do you only handle payment cards via a terminal with a dial-up connection (ISDN or analog) and otherwise only process payment card information on paper?	□
Do only those employees have access to payment card data that need such access to complete their work tasks?	□
Do only those employees have access to a computer that need it?	□
Do only those employees have keys to the payment card data storage locations that need such access?	□
Have you trained your employees regarding secure handling of e-mails containing payment card data?	□
Have you trained your employees regarding secure handling of print-outs and paper vouchers containing payment card data?	□
Are your employees aware of the sensitivity of payment card information?	□
Do you store print-outs, faxes and vouchers containing payment card information in a locked-up location?	□
Do you blacken-out or otherwise make highly sensitive information on print-outs illegible?	□
Have you taken measures to ensure that payment card data is irretrievably destroyed during their disposal?	□
Have you contractually agreed with your service provider that he/she will properly dispose of documents containing payment card data and will assume responsibility for doing so?	□
To be clarified with your service provider: Does the card terminal you use comply with payment card security standards? (Alternatively, have you verified the certification of the device on the PCI Council website?)	□
Does the card terminal store payment card data?	□
If yes: Can this data be securely deleted?	□
Is the card terminal tamper-proof?	□
Do you have an information security guideline?	□
Do all employees understand the contents of the guideline?	□

Do you have a work instruction for employees with access to payment card data?	□
Do you have a list of computer access and data storage location access authorizations?	□
Have you concluded a contractual agreement with service providers that come into contact with payment card data?	□
Do you have a list of these service providers?	□
Review of the PCI DSS conformity status of your service providers	□
Have you sensitized your service providers regarding handling of payment card data?	□
Do you review the measures and documents once per year to ensure that they are up-to-date?	□

3.9. Attachment B: Checklist – Payment Card Processing Areas

Business Process	Area	Medium that contains the payment card data	Further processing of payment card data

4. Measures to achieve PCI DSS Compliance for Hotels (SAQ C)

- Payment card data are processed using terminals or payment applications with an Internet connection.
- No electronic storage of payment card information.

4.1. Application Area

The measures we have described up to this point correspond with those of a business model in which payment card data are exclusively processed via terminals with a dial-up connection and paper vouchers. This information is not stored electronically. Category C SAQ applies to you if you process payment card data via terminals or payment applications that are connected with the Internet. Prerequisites for using Category C are that no payment card information is stored electronically, and that the payment card terminals and/or payment application systems are only connected with the Internet and are not connected with any other system in your hotel. Using the Internet to transmit payment card data offers criminals an additional target that you should not underestimate. This means that you must implement further measures in addition to those described in the above section to appropriately respond to the higher risk potential.

The measures we describe below are mostly of a very technical nature. They encompass many components of your IT infrastructure, including, among others, computers, your Internet access and the networking of different workplace computers with one another. If you do not operate your own IT infrastructure, you should ask your IT service provider whether the measures described have been implemented and, if not, instruct your service provider to implement these measures.

4.2. Securing the Network

Potential Risk

Inadequately secured networks frequently give a hacker easy access to individual computers operated within the networks. If a network does not have control checks that monitor data traffic, this may lead to undesired communication with and thereby unwanted access to your computers. Criminals particularly target and exploit network vulnerabilities. Skilled placement of a WLAN access point can also enable a hacker to steal payment card data without being noticed.

Measures

A firewall regulates permissible incoming and outgoing data traffic based on definable rules. It enables you to limit external access to computers in your hotel. It also regulates communication between systems in your hotel. Your payment card terminals and/or payment application systems may only be connected with the Internet. You must ensure that such terminals/payment application systems cannot communicate with other systems in your hotel such as your merchandise planning and control system. You can isolate the corresponding systems as required for SAQ C applicability by using and suitably configuring firewalls. A firewall must offer the functionality described in “Tasks to be completed from this section” to efficiently protect the payment card data processed in your hotel.

You must monitor the network to prevent access by unauthorized persons. WLAN access points that have been placed unnoticed in your network can be detected, for example, by physical control, an assessment of all network access possibilities and by security scans using software tools. Due to the high risk level they involve, you should always separate WLANs from systems that work with payment card data by a firewall.

The measures to protect WLANs we describe here and in the following sections only apply to WLANs that are used to transmit payment card data. However, we recommend that you also implement these measures for other WLANs. Other network vulnerabilities can be detected by so-called vulnerability scans. You must eliminate such vulnerabilities following the scans. A distinction is made between internal and external scans. Internal scans address the scenario of a criminal who has already penetrated your internal network. External scans address the scenario of a hacker who is trying to gain access to your network via the Internet. The PCI Security Standard requires that external vulnerability scans be performed by a scanning vendor who has been accredited by the PCI Council, a so-called “Approved Scanning Vendor” (ASV). Internal scans can also be performed by your IT service provider.

You should discuss the following points with your IT service provider and have him/her confirm that the required measures have been implemented in your daily business operations.

Tasks to be completed from this section

Ensure that your firewall and router configurations limit communication between payment card processing systems and the Internet □

Ensure that your payment card terminals and/or payment applications are only connected with the Internet □

Ensure that your WLAN is separated from payment card processing systems by a firewall □

Ensure that this firewall regulates all data traffic between your WLAN and payment card processing systems □

Limit incoming and outgoing system data traffic containing payment card data to the required minimum □

Ensure that every other kind of incoming and outgoing data traffic is banned (“Deny All”) □

Ensure that direct communication between payment card processing systems and the Internet is not possible (All connections must be made via the firewall) □

Ensure that every kind of outgoing data traffic from payment card processing systems must be explicitly released □

Ensure that your firewall supports “stateful inspection” □

Ensure that a quarterly search is conducted for unauthorized WLAN access points □

Ensure that quarterly internal vulnerability scans are performed by qualified personnel □

Eliminate vulnerabilities detected and have a repeat scan performed to check this □

Perform quarterly external vulnerability scans via an ASV □

Perform internal and external vulnerability scans after each significant change in your network (for example, after start-up of additional systems, changes in firewall rule sets or changes in your network structure) □

Repeat external scans until no vulnerabilities with a CVSS Base Score of more than 4.0 are detected □

4.3. Securing Your Systems

Potential Risk

The general threat posed by viruses, worms and trojans is an ever-present risk for the operation of your computers. This so-called malware can significantly limit the usability of or even completely disable your computers. Malware can also control access to your computers and thereby enable theft of sensitive information such as payment card data.

Measures

Antivirus programs and virus protection software are intended to protect your systems against malware that focuses on exploiting known vulnerabilities and security gaps. As virus protection software can only be effective against malware that it “knows,” it is absolutely essential that you always keep your antivirus programs up-to-date.

Malware usually attempts to exploit security gaps in the software installed on your computers. Normally, software manufacturers try to eliminate security gaps once they are detected. As a rule, manufacturers try do so by issuing a patch. A patch is a “piece of software” that is installed at a later date to eliminate a security gap. That's why, in addition to keeping your antivirus programs up-to-date, it is equally important that you install critical manufacturer security patches for your operating system (Windows Updates) and the applications you use (e.g. Acrobat Reader) within one month after release.

We would like to remind you in this context that malware can infect your employees’ computers not only via an Internet connection but also in other ways. Due to their mobility and related wide range of uses, mobile data storage devices such as USB sticks and portable hard disk drives represent a risk that should not be underestimated. We recommend that you deactivate the USB interfaces on your employees’ workplace computers if they are not needed for daily business operations.

Please check, if applicable, with your IT service provider, whether the following points have been implemented in your systems:

Tasks to be completed from this section

Ensure that antivirus programs/virus protection software have been installed on all your computers □

Keep the above programs/software active and up-to-date and ensure they protocol suspicious incidents □

Ensure they offer protection against every known type of malware (for example, viruses, trojans, worms, spyware, adware, rootkits) □

Preset automatic updates of all virus signatures and routine, complete virus scans (if available, also in your master installation) □

Ensure that the latest manufacturer security patches are installed at least once per month □

4.4. Default Manufacturer Settings

Potential Risk

Newly purchased software and hardware are usually delivered with certain default settings that have been set as standard by the manufacturer. This is a normal procedure that is intended to simplify the start-up process. However, these default settings are frequently kept relatively uncomplicated. As a result, they only offer an insufficient level of security. This is especially true in the case of default access data such as user names and passwords. Furthermore, additional manufacturer-specific default settings are public knowledge and are freely available in the Internet. For example, a hacker will try to find out what kind of software or device he/she is dealing with. If you don't change default passwords, you make a hacker attack much easier as the hacker will then try out the known standard passwords.

Measures

Hackers can frequently easily figure out or guess access data such as the user name and password of products that have been delivered with default manufacturer settings. That's why you should always change these settings.

The PCI Security Standard requires that you make the following changes to default manufacturer settings if your payment application or payment terminal is connected to the Internet via WLAN. If applicable, please clarify with your IT service provider whether the following measures have been implemented in your WLAN environment:

Tasks to be completed from this section

Change default manufacturer settings during installation (Change standard passwords, ban/deactivate unnecessary accounts that implement security measures specified in the manufacturer’s user manual) □

Note: Refrain, if possible, from transmitting payment card data via WLAN

Check the WLAN you use for payment card data transmission for compliance with the following requirements:
Ensure that standard encryption settings have been changed □

Change the key whenever an employee who knows the key is no longer employed by your hotel □

Ensure that standard SNMP community character strings been changed □

Ensure that the standard password for your WLAN access point has been changed □

Ensure that your firmware is kept up-to-date □

Insofar as applicable, ensure that all other security-relevant default settings have been changed □

Ensure that only services, protocols and daemons are active in your systems that you really need (and that all others have been deactivated) □

4.5. Secure Transmission of Payment Card Data

Potential Risk

It is relatively easy for attackers to intercept payment card data during transmission if you use public networks to electronically transmit such data. Criminals utilize a variety of software programs that are freely available in the Internet to tap data during its transmission. If you have not encrypted this data, it can be read by anyone including those persons who have intercepted it without authorization. Especially WLANs with weak encryption make it relatively simple for criminals to intercept such data without being detected.

Measures

It is important that you encrypt such data for transmission to protect it against misuse. This data can still be intercepted by hackers, but encryption makes it illegible and therefore of no use to them.

Encryption mechanisms play a central role in this context. These mechanisms must be robust enough to thwart hacker attacks. A mechanism is considered to be “strongly encrypted” if it can successfully ward off such hacker attacks. This is the case because only strong encryption is effective and provides the required level of protection of sensitive data. As a result, you should clarify with your IT service provider whether the protective mechanisms listed below have been implemented:

Tasks to be completed from this section

Ensure that your systems utilize strong encryption and security protocols

(for example, SSL/TLS, SSH or IPSEC) □

Only use trustworthy certificates (for example, from VeriSign, Thawte etc.)

Ensure that insecure protocols (for example, SSL v2.0 or SSH v1.0) are not used □

Ensure that HTTPS appears as part of your browser URL when using SSL □

Only work with payment card data if HTTPS is displayed as part of the URL and only permit HTTPS logins on login pages □

Comply with WLAN industry standards (i.e. use strong encryption for data transmission and authentication) □

4.6. Working in a Home Office

Potential Risk

From a technological point of view, working from a home office has long since become an established practice without problems thanks to laptops and the Internet. However, you must ensure that only those persons can externally access sensitive data such as payment card data stored in your hotel network who are truly authorized to do so. Otherwise, a criminal could pretend to be a person with access authorization and then try to access and steal payment card data.

Measures

In addition to securing all your communication channels, you must also ensure that only authorized persons can externally access your hotel network. You must use a so-called two-factor authentication to “prove” that the person who claims to have access authorization truly has such an authorization.

Normally, three factors must be considered in confirming a person's identity:

1. Something that the person knows: This is normally a password.

2. Something that the person possesses: For example, a chip card.

3. A personal characteristic: This applies to biometric characteristics, for example, a fingerprint scan.

Use of a single factor twice is not considered to be a two-factor authentication. The security level is not increased, for example, by requesting two different passwords one after the other. Only the combination of at least two different factors can provide higher security. The more factors you combine to identify a person, the more difficult you make it for criminals to imitate that person's identity. That's why persons who are trying to externally access a hotel network are required to prove their own identity via two of the three above-described factors. Your IT service provider should be able to assist you in implementing the above.

Tasks to be completed from this section
Ensure that proof of identity is provided using at least two factors to enable external access to your hotel network. □

4.7. Administrative Access and Remote Systems Maintenance

Potential Risk

Whenever systems are administered without using a directly connected console, a poorly secured remote access can enable a hacker to obtain security-critical information. In case of weak or even a lack of encryption, the criminal could, for example, obtain passwords that would enable him/her to access your systems and thereby payment card data at a later date.

Measures

System access for administrative purposes that is not conducted via a monitor directly connected to the computer must be secured using strong encryption. The login process is particularly risky so you must ensure that encryption mechanisms are activated before a password is queried.

If you provide remote access to your systems to an IT service provider or a manufacturer in connection with maintenance and support work, you must adequately secure such access. In addition, you may only grant access via an account that has been established especially for remote access. This account may only be active when it is needed. The account may not provide a permanent access capability. Remote access must be monitored during use.

Tasks to be completed from this section

Protect non-console administrative accesses with strong encryption (for example, with SSH, VPN or SSL/TLS) □

Call up strong encryption methods before entering an administrator password □

Utilize strong encryption also during administrator access to web-based management interfaces □

Prevent insecure remote login procedures (for example, Telnet or rlogin) □

Ensure that remote accesses of your service provider or a manufacturer can only be made using the accounts established for that purpose □

Ensure that these accounts are only active when they are needed □

Ensure that the activities of the service provider/manufacturer are monitored during remote access □

4.8. Supplementary Information in the Security Documents

The explanations given in the previous chapter about an information security guideline also apply to the Category C SAQ. However, we must provide some supplemental information to inform you about the additional risks that arise due to the characteristics and functionality of the technologies used.

Information Security Guideline

You should supplement your information security guideline with the following contents:

- Authentication is required to prove that the respective person actually has access authorization. Criminals could relatively easily access systems if you do not implement identity verification mechanisms.
- “Acceptable Network Locations” must be specified. These are the locations where computers that can access payment card data should ideally be installed. For example, you could specify that monitors must be installed in such a way that third parties cannot view them. Specifying such locations will help you to keep track of things and identify possible security gaps.
- Technologies that permit access from home office workplaces to the hotel network are especially risky. That's why the PCI Security Standard provides that these kinds of technologies be configured in such a way that connections are automatically interrupted after a specified period of inactivity (15 minutes) and that a repeated login with a password is required.
- Special measures must be implemented if you grant remote access to hotel network systems to external service providers or to a manufacturer to enable maintenance and support activities. This kind of access capability represents a kind of “backdoor” that provides access to sensitive data. That's why it is very important that such access is only active when it is needed and is inactive at other times.
- A search for unauthorized WLAN access points must be conducted on a quarterly basis. You should include a description of how the above is to be performed. Alternatively, you can inspect all locations that provide access to the hotel network or conduct an automated scan. Employees should be instructed about how to deal with unauthorized WLANs access points they discover during their routine daily work. They should delete such access points and inform hotel management about such an incident.

Work Instruction for Employees with Access to Payment Card Data

Be sure to supplement the work instruction for employees having access to payment card data with information about those special items describing PCI-compliant handling of the technologies used. You can achieve the required acceptance for measures to be implemented by explaining to your employees the action to be taken, how this should be done and the reasons for doing so. This helps to ensure that your employees implement these measures and limits the risks of improper conduct.

You should ensure that the following points are included in the work instructions depending on the types of technologies you use:

- Employees authorized to grant remote access to your hotel's computers to an external service provider or manufacturer to enable maintenance support work must be familiar with the handling of such access technologies. They must be fully aware that they must deactivate such access immediately after the support activity has been concluded and how this is to be handled in practice.

- If an employee discovers an unauthorized WLANs access point, then he/she must delete it and report the incident to hotel management.

List of Computer Access and Data Storage Location Access Authorizations

The list of computer access and data storage location access authorizations must also specify which employees have access in what ways to computers that process payment card data. In this context, the list should also clearly indicate which employees know the corresponding passwords and whether they can access hotel systems from their workplace computers in the hotel or from their home offices. The list must also include the names of those employees authorized to grant access to the hotel network to a service provider or manufacturer.

List of External Service Providers

External service providers who may be granted remote access to hotel network systems during the course of maintenance and support work should be marked accordingly on the list of external service providers.

Tasks to be completed from this section

Supplement the Information Security Guideline □

Supplement the Work Instruction for Employees with Access to Payment Card Data □

Supplement the List of Computer Access and Data Storage Location Access Authorizations □

Supplement the List of External Service Providers □

4.9. Successfully Securing Payment Card Data Over Time

The measures we describe in this section provide a minimum level of protection of payment card data for business models that utilize terminals or payment applications with an Internet connection to process payment cards. You can implement all measures and achieve basic protection in an efficient and practicable way by foregoing electronic storage of payment card information.

If you have implemented the measures described in this handbook in your hotel, you may answer the questions contained in the Category C SAQ with “yes” to prove your PCI conformity. Of course, you must not implement measures applicable to technologies that you don't use. In the case of such SAQ questions, you should fill in the answer “not applicable” in the “Special” column and briefly explain in the attachment why this question does not apply to your hotel. If, for example, remote access to your systems from outside the hotel is prohibited in general and impossible, then you must not deal with security measures for such remote access.

You must fill out the SAQ once per year and, if applicable, submit it to your merchant bank to maintain your PCI conformity. This enables you to check the measures you implemented and/or to adapt them to suit changes that may have been made in your business processes and, if necessary, to select an appropriate SAQ category.

However, achievement/proof of PCI DSS conformity alone is not sufficient to sustainably protect payment card data. You can only achieve effective, ongoing protection if you and your employees truly internalize the measures. All persons involved must work together to do so.

Bottom line, you should protect customer data not only considering possible liability claims but also to secure the future and competitiveness of your business long-term.

4.10. Attachment C: SAQ Checklist – Category C

Are you familiar with the payment card handling flow in your hotel?	□
Do you only handle payment cards via a terminal with a dial-up connection (ISDN or analog) and otherwise only process payment card information on paper?	□
Do only those employees have access to payment card data that need such access to complete their work tasks?	□
Do only those employees have access to a computer that need it?	□
Do only those employees have keys to the payment card data storage locations that need such access?	□
Have you trained your employees regarding secure handling of e-mails containing payment card data?	□
Have you trained your employees regarding secure handling of print-outs and paper vouchers containing payment card data?	□
Are your employees aware of the sensitivity of payment card information?	□
Do you store print-outs, faxes and vouchers containing payment card information in a locked-up location?	□
Do you blacken-out or otherwise make highly sensitive information on print-outs illegible?	□
Have you taken measures to ensure that payment card data is irretrievably destroyed during their disposal?	□
Have you contractually agreed with your service provider that he/she will properly dispose of documents containing payment card data and will assume responsibility for doing so?	□
Have you clarified with your service provider whether the card terminal you use complies with payment card security standards? (Alternatively, have you verified the certification of the device on the PCI Council website?)	□
Does the card terminal store payment card data?	□
If yes: Can this data be securely deleted?	□
Is the card terminal tamper-proof?	□
Do your firewall and router configurations limit communication between payment card processing systems and the Internet?	□

Is your WLAN separated from payment card processing systems by a firewall?	□
Does your firewall regulate all data traffic between your WLAN and payment card processing systems?	□
Have you limited incoming and outgoing system data traffic containing payment card data to the required minimum?	□
Have you banned every other kind of incoming and outgoing data traffic (“Deny All”)?	□
Have you ensured that direct communication between payment card processing systems and the Internet is impossible (All connections must be made via the firewall)?	□
Are your payment card terminals and/or payment applications only connected with the Internet and with no other system in your hotel?	□
Must every kind of outgoing data traffic from payment card processing systems be explicitly released?	□
Does your firewall support “stateful inspection”?	□
Do you search for unauthorized WLAN access points on a quarterly basis?	□
Are quarterly internal vulnerability scans performed by qualified personnel?	□
Are detected vulnerabilities eliminated, and do you have a repeat scan performed to verify this?	□
Are quarterly external vulnerability scans performed by an ASV?	□
Do you perform internal and external vulnerability scans after each significant change in your network (for example, after start-up of additional systems, changes in firewall rule sets or changes in your network structure)?	□
Are external scans repeated until no vulnerabilities with a CVSS Base Score of more than 4.0 are detected?	□
Have you installed antivirus programs/virus protection software on all your computers?	□
Are these programs/software active and up-to-date and do they protocol suspicious incidents?	□
Do they protect against every known type of malware (for example, viruses, trojans, worms, spyware, adware, rootkits)?	□
Have you preset automatic updates of all virus signatures and routine, complete virus scans (if available, also in your master installation)	□
Do you install the latest manufacturer security patches at least once per month?	□

Do you install security-relevant patches within one month of release?	□
Do you change manufacturer default settings during installation (i.e. change standard passwords, ban/deactivate unnecessary accounts, among other changes)?	□
Does the WLAN used to transmit payment card data comply with the following?	
▪ Did you change the standard encryption settings?	□
▪ Do you change keys whenever an employee who knows the keys is no longer employed by your hotel?	□
▪ Did you change the standard SNMP community character strings?	□
▪ Did you change the standard password for your WLAN access point?	□
▪ Is your firmware up-to-date?	□
▪ Insofar as applicable, have you changed all other security-relevant default settings?	□
Are only services, protocols and daemons active in your systems that are really needed (and have you deactivated all others)?	□
Do you use strong encryption and security protocols to transmit payment card data (for example, SSL/TLS, SSH or IPSEC)?	□
Do you only use trustworthy certificates (for example, from VeriSign, Thawte etc.)?	□
Have you ensured that insecure protocols (for example, SSL v2.0 or SSH v1.0) are not used?	□
Is the prefix “HTTPS” displayed in your browser URL when you use SSL?	□
Do you only work with payment card data if HTTPS is displayed as part of the URL?	□
Do you comply with WLAN industry standards (i.e. use strong encryption for data transmission and authentication)?	□
Have you ensured that proof of identity using at least two factors is absolutely necessary to enable external access to your hotel network?	□
Are non-console administrative accesses protected with strong encryption (for example, with SSH, VPN or SSL/TLS)?	□
Do you call up strong encryption methods before entering an administrator password?	□
Do you utilize strong encryption also during administrator access to web-based management interfaces?	□
Do you prevent use of insecure remote login procedures (for example, Telnet or rlogin)?	□

Have you ensured that remote accesses of your service provider or a manufacturer can only be made using the accounts established for that purpose?	□
Are these accounts only active when they are needed?	□
Do you monitor the activities of the service provider/manufacturer during remote access?	□
Do you have an information security guideline containing the information required by SAQ B and C?	□
Do you distribute this guideline to all employees that come into contact with payment card data?	□
Do your employees understand the contents of the guideline?	□
Do you have a work instruction for employees with access to payment card data?	□
Do you have a list of computer access and data storage location access authorizations?	□
Are your employees familiar with the handling of the technologies you use?	□
Do your employees know what to do if they discover unauthorized WLAN access points?	□
Are employees that work with payment card data aware of the sensitivity of this data?	□
Have you concluded a contractual agreement with service providers that come into contact with payment card data?	□
Which service providers and manufacturers have been granted remote access to your hotel network?	□
Do you have a list of these service providers?	□
Have you reviewed the PCI DSS conformity status of your service providers?	□
Have you sensitized your service providers regarding handling of payment card data?	□
Do you review the measures and documents once per year to ensure that they are up-to-date?	□