Cross Keys Hotel Chatteris

Information Security Policy

Responsible Person *(Employer or other person having control of the relevant premises)*	David Leaning
Address of Premises	Cross Keys Hotel 12-16 Market Hill Chatteris Cambridgeshire
Postcode	PE16 6BA
Assessor:	David Leaning
Date of Information Security Policy	26th April 2021
To be reviewed on an annual basis unless any pertinent event or change warrants a review sooner.	
Subsequent Review Dates	

Reviewed by		**Date**	By 26 APRIL 22
Reviewed by		**Date**	
Reviewed by		**Date**	

Information Security Policy

Contents

Information Security Policy 1

INTRODUCTION

This Policy Document encompasses all aspects of security surrounding confidential company information and must be distributed to all company employees. All company employees must read this document in its entirety and sign the form confirming they have read and understand this policy fully. This document will be reviewed and updated by Management on an annual basis or when relevant to include newly developed security standards into the policy and distribute it all employees and contracts as applicable.

The Cross Keys Hotel handles sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organisation.

The Cross Keys Hotel commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end management are committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.

We each have a responsibility for ensuring our company's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from David or

Rebecca Leaning.

I. PURPOSE AND SCOPE

The purpose of this Policy, which has a global scope, is to establish the information security framework used in the activities developed by Cross Keys Hotel, Chatteris and its Group (hereinafter CKH). This framework lies on internationally recognised best practices used in the management of Information Security in order to ensure confidentiality, integrity and availability of the information being processed at all times and in any of its business areas.

The content of this Policy is set as minimum standards, without prejudice to additional and specific regulations that may be approved regarding the topic, and without prejudice to any specific legal regulations that may be applicable in any of the countries in which the Company or any entity of its Group may develop its activities.

This Policy sets the security objectives and identifies its treatment resources to ensure compliance with the degree of protection required, and reflects the commitment in regards to the need to establish the precise mechanisms aimed at ensuring the confidential treatment and integrity of information, in line with CKH's business strategy.

II. FRAMEWORK OF APPLICATION

This Policy is framed and approved according to, among others, the commitments contained in the GDPR policy of the Cross Keys Hotel both in relation to our clients (commitment to protect the information and data that customers entrust to us), as well as to our shareholders and investors (ensuring maximum reliability and accuracy of our accounting and financial records).

III. GUIDING PRINCIPLES

CKH acknowledges the need to create a culture of information security that operate in all areas of business, both internal (in relation to all staff) and external (in relation to stakeholders, potential residents, etc.), and with the global perspective of a company with an international footprint.

Acceptable Use Policy

The Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to The Cross Keys Hotel established culture of openness, trust and integrity. Management is committed to protecting the employees, partners and The Cross Keys Hotel from illegal or damaging actions by individuals, either knowingly or unknowingly. The Cross Keys Hotel will maintain an approved list of technologies and devices and personnel with access to such devices.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies

- Employees should take all necessary steps to prevent unauthorised access to confidential data which includes card holder data.
- Employees should ensure that technologies should be used and setup in acceptable network locations
- Keep passwords secure and do not share accounts.
- Authorised users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Because information contained on portable computers is especially vulnerable, special care should be exercised.
- Postings by employees from a Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of The Cross Keys Hotel, unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

PHYSICAL SECURITY

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data, this includes CCTV system access.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
- Employees should ensure that technologies should be used and setup in acceptable network locations
- A list of devices that accept payment card data should be maintained.
- The list should include make, model and location of the device
- The list should have the serial number or a unique identifier of the device
- The list should be updated when devices are added, removed or relocated
- POS devices surfaces should be periodically inspected to detect tampering or substitution.
- Personnel using the devices should be trained and aware of handling the POS devices
- Personnel using the devices should verify the identity of any third party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.
- Personnel using the devices should be trained to report suspicious behaviour and indications of tampering of the devices to the appropriate personnel.

- A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.
- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. “Employee” refers to full-time and part-time employees, temporary employees and personnel, and consultants who are “resident” on The Cross Keys Hotel sites. A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Network Jacks located in public and areas accessible to visitors must be disabled and enabled when network access is explicitly authorised.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Strict control is maintained over the external or internal distribution of any media containing card holder data and has to be approved by management
- Strict control is maintained over the storage and accessibility of media
- All computer that store sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorised use.

Access to the sensitive cardholder data

All Access to sensitive cardholder should be controlled and authorised. Any Job functions that require access to cardholder data should be clearly defined.

- Any display of the card holder should be restricted at a minimum of the first 6 and the last 4 digits of the cardholder data.
- Access rights to privileged user ID’s should be restricted to least privileges necessary to perform job responsibilities
- Privileges should be assigned to individuals based on job classification and function (Role based access control)
- Access to sensitive cardholder information such as PAN’s, personal information and business data is restricted to employees that have a legitimate need to view such information.
- No other employees should have access to this confidential data unless they have a genuine business need.
- If cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained as detailed in Appendix B.
- The Cross Keys Hotel will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the for the cardholder data that the Service Provider possess.
- The Cross Keys Hotel will ensure that a there is an established process including

proper due diligence is in place before engaging with a Service provider.

- The Cross Keys Hotel will have a process in place to monitor the PCI DSS compliance status of the Service provider.

Employees handling Sensitive cardholder data should also ensure:

- Handle Company and cardholder information in a manner that fits with their sensitivity;
- Limit personal use of The Cross Keys Hotel information and telecommunication systems and ensure it doesn't interfere with your job performance;
- The Cross Keys Hotel reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;
- Do not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Do not disclose personnel information unless authorised;
- Protect sensitive cardholder information;
- Keep passwords and accounts secure;
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval;
- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended;
- Information security incidents must be reported, without delay, to the individual responsible for incident response locally – Please find out who this is.

Information Security Policy 2

As this environment is a global and changing scenario, information security must be perceived as a continuous improvement process that allow us to achieve even more advanced security levels, and with a primary goal of ensuring compliance with current legislation and complying with all other legal or regulatory requirements that may be applicable in each country. In this regard, special attention will be given to the following aspects:

•Personal data protection

The security of the personal information of our clients and stakeholders is a priority for CKH, for which the structures, security plans and control mechanisms are set in order to align with the existing regulations on this matter in each country.

• Safe and responsible treatment of credit card data and payment methods

We will make every effort to make it impossible to compromise or leakage. The Company and its employees commit themselves to diligently use the available resources at their disposal when processing the information associated with credit card data by using all the means that guarantee maximum security and confidentiality of the data to avoid the fraudulent use of any means, as well as by ensuring the compliance with existing legislation and regulations at any moment. Among the measures taken, the Company complies with the standards of the payment industry (PCI / DSS) after having adopted the security standards (PCI /

DSS) required to merchants in order to ensure a proper protection and confidentiality of their customers' information.

• Installation or unauthorized use of computer assets that may harm intellectual and industrial property.

• The awareness and sensitization of employees in the abstention of the unauthorised use of computer assets will be actively promoted, in accordance with current regulations.

• Computers and IT equipment damage
The Company and its employees must preserve the correct use of the equipment, systems and software available to them by acting according to security, confidentiality and efficiency criteria, as well as by preventing any action that is unlawful or contrary to existing regulations in each country or which may cause any damage to the Company's IT systems or to any third party related to them. For this purpose, the Company performs, among other things, a preventive activity aimed at detecting malicious software.

• Business continuity
The Company and its employees will develop plans and processes that guarantee the normal functioning and continuity of operations in case of computer-related incidents.

Information Security Policy 3

• Rights relating to privacy and unauthorised access
The Company has the necessary technical, human and organisational resources to ensure the confidentiality of information and the implementation of access control systems to information repositories, such as identities administration or user accounts.

For all the aspects listed above, CKH has the technical, physical and organisational control and monitoring systems that are necessary to provide the confidentiality, integrity and availability of the information managed within the Company in an effective way.

The safety objectives therefore operate at the highest levels of the Company, as they are a critical element for the achievement of its strategic objectives.

All of the foregoing, without prejudice to all other legal or regulatory requirements not clearly included in this Policy and that might be applicable in each country, on matters that affect in any way the businesses managed by CKH.

The existence of standards, processes, procedures and manuals is essential for this purpose, as well as the commitment to keep all of them permanently updated in order to ensure the validity and timing of controls and their adequacy to the specific needs of CKH at all times.

Moreover, direct involvement of all members of the Company is actively encouraged by promoting a proactive, critical and constructive attitude in a constant search for improvement and quality in the treatment, evolution, security and safeguard of information.

The Company is committed to provide the necessary means for the achievement of the established security objectives, relies on the collaboration of all employees and assumes the responsibility of motivating and training them so they can know and fully fulfil this Policy.