INFORMATION SECURITY POLICY

Approving Authority	Board of Directors of Chalet Hotels Limited ("the Company")
Approval Date	January 29, 2025
Effective Date	This shall come into effect from the date of its approval, i.e. adoption at the meeting of the Board of Directors.
Classification	Public
Version	1.0

Purpose and Objectives

Chalet Hotels Limited is a part of K Raheja Corp group. Chalet Hotels Limited network has adopted the ISO 27001 security standards which apply a risk-based approach to protect information assets. The ISO is internationally renowned and provides the best practices for managing information security, risks, and controls within the framework of an information security and risk management program to support the Information Security Policy and business objectives.

Objectives

The specific objectives of the "Information Security Policy" are:

- To prevent unauthorized disclosure of information stored or processed on Chalet Hotels Limited's information systems (Confidentiality)
- To prevent accidental or unauthorized deliberate alteration or deletion of information (Integrity)
- To ensure that information is available to authorized person whenever required (Availability)

The policy will provide guidance to ensure that Chalet Hotels Limited's information systems comply with relevant laws and regulations, industry leading practices and recognized international standards on information security management system.

Scope

Information Security Management Systems (ISMS) applies to IT Infrastructure and its associated services namely, IT Delivery, Infrastructure, & Security Operations along with support functions HR and Admin to provide secured and quality services to its customers.

Policy Framework

The ISMS is committed to satisfying applicable requirements relating to Information Security and is committed to continual improvement of Information Security. Information assets are critical to the success of our business. We shall, therefore, ensure the confidentiality, integrity, availability and legality of the information and information processing assets of our customers and our company by deploying appropriate people, processes, and technology.

1.1 All employees of Chalet Hotels Limited's network and third-party users shall be responsible for adhering to and remain in compliance with the ISMS in accordance with the policies and procedures.

1.2 This Information Security Policy shall be communicated to all employees through onboarding and periodic training as well as by storing it in some shared location or publishing it on the website of the Company.

1.3 Information Security Policy should be communicated to all interested parties.

Policy Statement

Information Security Risk Assessment (ISRA)

ISRA provides necessary directions to identify and assess risks and to reduce the exposure to the security risks. It also minimizes the overall impact on the IT environment (existing and emerging) to an acceptable level.
This assessment applies to any form of data, including paper documents and digital data stored on any type of media. It applies to all the organization’s employees, as well as to third-party agents authorized to access the data.

Human Resource and Security Policy (HRSP)

This policy refers to implementing ISMS security controls to ensure that employees understand their roles and responsibilities for which they are considered.

Access Control Management (ACM)

ACM defines an acceptable usage of assets for users while accessing organization computing resources. A clearly defined and enforced Asset Usage policy (AUP) is critical to maintain information security requirements. Establishes a standard for creating strong passwords, the protection of those passwords and the frequency of change.
ACM applies to all employees having access to the organization’s information and systems, internet access and electronic communication services.

Operations Security

Operations security procedure ensures that periodically audits are conducted for validating controls implemented in the ISMS for consistencies and to identify areas of the ISMS for continuous improvement.

Vulnerability Management Policy

This policy is committed towards the protection of IT infrastructure including servers, applications, network, databases and security devices with security, reliability, and stability. The technical vulnerabilities of Information Systems and infrastructure shall be identified and evaluated to ensure adequate measures are taken to address the associated risks. All discovered vulnerabilities are assigned a Common Vulnerability Scoring System (CVSS) and shall be reported and addressed appropriately to mitigate the identified risks within specified timelines.

Supplier Management

The purpose of this policy is to ensure that the Company's suppliers, vendors and third-party contracts follow information security requirements while accessing and managing the Company's information assets for service delivery and/or during service delivery.

Information Security Incident Management (ISIM)

A security incident is defined as any event which affects confidentiality, integrity or availability of data in the enterprise. Security incidents can be successfully managed by having a clear incident management policy in place.

a. Information Security Incident Management Policies

The purpose of this policy is to define standard methods for identifying, tracking, promptly responding and remediating IT Security Incidents.

ISIM applies to all physical, network and computing assets owned and/or administered in the enterprise. All Employees of the Company are required to follow this procedure for reporting Information Security weaknesses and incidents.

b. Business Continuity Program (BCP)

BCP focuses on continuity of critical business processes. Each document shall be updated on a periodic basis and records of the same shall be maintained. This policy enforces a consistent way to maintain, evaluate and update the Business Continuity Management (BCM) documentation and ensure that changes to the documents are performed in a controlled and systematic manner.

The incident response plan shall be used in the event of system compromise addressing specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies. The plan is tested periodically, and appropriate training shall be provided for staff with security breach response responsibilities.

All documents are prepared in accordance with ISO 27001:2022.

Compliance

The information systems should be regularly reviewed for compliance with the information security policies and standards & IT Act.

All assets shall be checked for technical compliance with their documented configuration requirements periodically. This includes periodic penetration testing of all websites and Internet-facing applications and connectivity.

Definitions

Terms	Definition
Asset	Anything tangible or intangible that can be owned controlled and produce value through its use.
Availability	Property of being accessible and usable on demand by an authorized entity.
Backup	The saving of files onto alternate storage or other offline mass storage media for preventing loss of data in the event of equipment failure, destruction, or accidental deletions.
Business Continuity	The company's ability to ensure operations and core business functions are not severely impacted by disaster or unplanned incidents that take critical systems offline.
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Copyright	Copyright is a legal right that protects the expression of ideas.
Cryptography	The science of secret writing that enables storage and transmission of data in a form that is available only to the intended individuals
Devices	The device includes all servers, network devices and endpoints.
Document	A document is something that is being currently worked upon and is therefore subject to editing and change.
Encryption	The transformation of plain text into unreadable cipher text.
External Network	Any network including the Internet, outsourced suppliers, and business partners.
Information Systems	Knowledge or information that is retained in electronic form (such as emails, documents, etc.) or physically tangible material (such as printed documents, etc.) for industrial control systems or set of applications, services, information technology assets, or other information-handling components.
Information Security Event	The identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that can be security relevant.
Information Security Management System	Is a management system based on a systematic business risk approach to establish, implement, operate, monitor, review, maintain, and improve information security.
Information Security Incident	Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
Integrity	Property of accuracy and completeness of the information.
Password	A protected word or string of characters which serves as an authentication of a person's identity, or which may be used to grant or deny access to private or shared data.
Review	The activity was undertaken to determine the suitability, adequacy, and effectiveness of the subject matter to achieve established objectives.
Risk	A potential event or action that would harm the organization.
Risk assessment	The overall process of risk identification, risk analysis and risk evaluation.
Suppliers	Any third-party service providers, vendors, contractors, and their sub-contractors are referred to as supplier.
System	Any machine used for computation which includes endpoints, servers, application.
Third-Party	Third parties include suppliers including advisors, consultants, service providers (contractors and their sub-contractors), vendors and other personnel having access to the company's information systems.
Virus	A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its code.
Vulnerability	Vulnerability is a weakness with an organization's assets that have the potential to allow a threat to occur with higher frequency, more significant impact, or both.

Violation of Policy

All employees are obligated to report violations of this policy to IS-Head / COO immediately. The ISMS Forum must approve any exceptions to this policy in advance.

Enforcement and Escalation

Failure to comply with this policy may result in:

- Withdrawal, without notice, of access to information and/or information resources.
- Disciplinary action, up to and including termination.
- Civil or criminal penalties as provided by law.

References

This policy refers to ISO/IEC 27001:2022 standard.

Note

The Company's operational hospitality assets shall follow the guidelines stated in their respective brand IT policies and procedures.