

Information Security Policy

S. No.	Type of Information	Document Data
1	Document Title	VHL_IT_POL_33_One Pager Information Security Policy
2	Document No.	VHL_IT_POL_33
3	Date of Supersede Version	03-04-2026
4	Date of Approval	25-06-2026
5	Date of Release	30-06-2026
6	Document Revision No	1.2
7	Document Owner	ISGC
8	Document Approver	ISGC
9	Document Authors	Saarth Infosec
10	Next Review Date	05-04-2027

Version Control

Version History					
Version	Summary of Changes	Last Updated	Prepared by	Reviewed by	Approved by
1.0	Initial Document	03-04-2026	IBM	Arjun Kumar Yenishetti	Rajkumar Sharma
1.1	Final Document	25-06-2026	Saarth Infosec	Arjun Kumar Yenishetti	Rajkumar Sharma
1.2	Published Document	30-06-2026	Saarth Infosec	Arjun/Rajkumar	ISGC



Information Security Policy

Vision

To provide secure, reliable, and innovative hospitality solutions by protecting information assets and maintaining trust among customers, partners, employees, and stakeholders.

Mission

To establish and maintain an effective information security framework that safeguards organizational information, supports business operations, and enables secure delivery of hospitality services.

Information Security Commitment

Ventive Hospitality Limited is committed to protecting its information assets, systems, and business processes by ensuring:

Confidentiality

Information is accessible only to authorized individuals and protected against unauthorized disclosure.

Integrity

Information is accurate, complete, and safeguarded against unauthorized modification, alteration, or destruction.

Availability

Information systems, applications, and services remain accessible and operational to support business and customer requirements.

Scope

This policy applies to all employees, contractors, consultants, third-party service providers, business partners, and any individual or entity handling or accessing information assets, systems, applications, or services of Ventive Hospitality Limited.



Security Practices

Ventive Hospitality Limited commits to implementing and maintaining the following security practices:

- Identify, classify, and protect information assets based on business and regulatory requirements
- Implement access controls based on business need-to-know and least privilege principles
- Secure networks, systems, applications, and cloud infrastructure using industry-recognized security practices
- Monitor, log, and review security events to identify and respond to threats effectively
- Maintain backup and recovery mechanisms to support business continuity and resilience
- Conduct regular information security awareness and training programs for employees
- Establish processes for timely detection, reporting, investigation, and response to information security incidents
- Assess and manage information security risks associated with suppliers, partners, and third parties
- Ensure compliance with applicable legal, regulatory, contractual, and business requirements

Responsibilities

All employees, contractors, third parties, and relevant stakeholders are responsible for protecting organizational information assets, adhering to security requirements, and promptly reporting security incidents, vulnerabilities, or suspicious activities.

Continuous Improvement

Ventive Hospitality Limited is committed to continuously reviewing, monitoring, and improving its information security controls, processes, and practices to address emerging threats, business changes, and evolving regulatory requirements.