ClubMahindra

Information Security & Customer Privacy Policy

Purpose:

Mahindra Holidays & Resorts India Limited (MHRIL) is committed to safeguarding the confidentiality, integrity, availability and privacy of its information assets and customer data. This Policy establishes the principles and responsibilities necessary to ensure secure operations, protect personal and corporate information, and comply with applicable regulatory and contractual obligations.

Scope:

This Policy applies to all employees, contractors, consultants, interns, third parties and service providers who access MHRIL's information systems or handle MHRIL's data. It covers all information assets, IT systems, networks, cloud environments, applications, digital platforms and customer data processed or stored by MHRIL.

Information Security Commitments:

1. Protection of Information Assets

MHRIL is committed to protecting the confidentiality, integrity and availability of information by implementing appropriate technical and organisational measures. All information assets will be secured against unauthorised access, misuse, alteration, loss or disclosure. Access to information will be granted based on business need and governed through strict access control, authentication and monitoring mechanisms.

2. Continuous Improvement of Information Security Systems

MHRIL follows the ISO 27001:2022 Framework and will continuously enhance its information security controls, governance systems, incident-handling mechanisms, monitoring capabilities and risk management practices. Improvements will be driven through periodic assessments, audits, corrective actions and technology upgrades.

3. Monitoring and Responding to Cybersecurity Threats

MHRIL maintains a comprehensive security monitoring environment that covers digital risk, network and cloud security, web application protection, endpoint security, data loss prevention, access violations, anomalous user behaviour and potential cyberattacks. The organisation will proactively detect, analyse and respond to cybersecurity threats, and maintain documented incident response procedures to ensure timely and effective action.

4. Integrity and Protection of Data

MHRIL ensures that information and personal data remain accurate, complete and protected from unauthorised modification or destruction. Data will be encrypted where necessary, stored securely, processed only for legitimate purposes, and handled through structured backup, recovery and business continuity processes. Network segmentation, system hardening and patch management will be maintained to reduce vulnerabilities and strengthen resilience.

5. Workforce Responsibilities

All employees and individuals working on behalf of MHRIL share responsibility for information security. They must follow secure practices, protect login credentials, comply with company-approved security procedures, promptly report incidents or suspected security weaknesses, and complete all mandatory information security and privacy trainings. Every user of MHRIL systems is accountable for safeguarding the information they access.

6. Third-Party Information Security Requirements

Suppliers, vendors, partners and service providers with access to MHRIL systems or data must comply with this Policy, implement adequate security controls, and protect information entrusted to them. MHRIL will conduct due-diligence assessments during onboarding and periodic reviews thereafter to evaluate compliance. Third-party system access will be limited, monitored and approved through defined processes, and contractual agreements will include confidentiality and data protection requirements.

Customer Privacy Commitments:

1. Transparency in Data Collection and Use

MHRIL will inform customers of the nature of personal data collected, the purpose for which it is used, and the legal basis for such collection. Customers will have visibility into how their information is processed, stored and shared. Privacy information is made available through MHRIL's digital and operational platforms, including websites and application interfaces.

2. Customer Rights and Control Over Personal Data

MHRIL provides customers with the ability to decide how their personal data is collected, used, retained and processed. Customers may exercise their right to give consent, withdraw consent, opt out of non-essential uses, access personal data, correct inaccuracies, delete information, or request that their data be transferred to another service provider. Requests will be processed in accordance with applicable regulations and MHRIL's internal procedures.

3. Data Retention and Disposal

Customer information will be retained for only as long as necessary for the purpose for which it was collected or as required by statutory and regulatory obligations. For example, financial and transactional records may be retained for periods prescribed under law. Data will be securely deleted or anonymised once the retention period has lapsed or upon valid customer request.

4. Protection of Customer Data

MHRIL employs layered security measures to protect customer data, including firewalls, web application security controls, endpoint protection, encryption, secure development standards, network segmentation, access approvals, continuous monitoring, and regular security updates. These measures ensure that personal information is protected against unauthorised access, disclosure, misuse or loss throughout its lifecycle.

5. Disclosure of Data to Third Parties

Customer data may only be shared with authorised third parties who have a legitimate business purpose and who are contractually obligated to maintain confidentiality and appropriate data protection measures. All third-party interactions involving customer information will be governed by agreements such as NDAs, service contracts and data processing clauses that specify privacy and security obligations.

6. Secondary Use of Customer Data

Any secondary or non-primary use of customer data will be communicated to customers, who will be given appropriate options to provide consent or opt-out where applicable. MHRIL will maintain internal controls to ensure that secondary data usage is limited, justified, and compliant with consent frameworks and regulatory requirements.

Incident Reporting and Response:

All employees and third parties must promptly report actual or suspected information security or privacy incidents. MHRIL will investigate incidents, take corrective and preventive action, notify stakeholders where legally required, and document learnings to strengthen controls.

Training and Awareness:

MHRIL will provide ongoing training and awareness programmes to employees and contractors on information security practices, data protection requirements, phishing awareness, secure handling of systems and applications, and responsibilities under relevant laws and corporate policies.

Governance and Review:

MHRIL will maintain an Information Security Management System aligned with ISO 27001:2022 requirements. Governance bodies will periodically review risks, compliance status, third-party security, audit findings and areas

requiring improvement. This Policy will be reviewed annually or earlier if required due to changes in technology, regulation or business needs.

Enforcement:

Non-compliance with this Policy may result in disciplinary action, suspension of access, termination of contract, or legal proceedings where applicable. MHRIL reserves the right to restrict or revoke access to systems and information where security is compromised.

Manoj Bhat
Managing Director & CEO

Date: 29th December 2025

THANK YOU!