7SEAS ENTERTAINMENT LIMITED
PERSONAL DATA BREACH AND CYBER INCIDENT RESPONSE POLICY

(Approved/Amended by the Board of Directors on 21 July 2026)

CIN: L72900TG1991PLC013074

Registered Office: 5th Floor, Plot Nos. 92, 93 and 94, Kavuri Hills, Madhapur, Hyderabad, Telangana – 500081

Classification: Internal and confidential

1. Objective and scope

This Policy establishes an integrated response to confidentiality, integrity or availability incidents affecting systems, personal data, games, applications, websites, vendors or statutory disclosures.

2. Incident-response team

The team shall include technology/security, legal, compliance, data protection, business, communications and management representatives. Contact details, deputies, external forensic support, insurers and regulator channels shall be maintained and tested.

3. Incident classification

Incidents shall be classified by data sensitivity, persons affected, system criticality, duration, geographic reach, fraud, child impact, recovery, legal exposure and likely harm. Classification shall be updated as facts develop.

4. Detection and reporting

Employees and processors shall report suspected phishing, malware, unauthorised access, data loss, service disruption, credential compromise or accidental disclosure immediately. Processor contracts shall require prompt notice and cooperation.

5. Containment and evidence

The response team shall isolate affected assets, revoke credentials, block malicious activity, preserve logs and forensic images, maintain chain of custody and avoid actions that unnecessarily destroy evidence.

6. Assessment and notifications

The team shall determine affected data, individuals, systems, cause, likely consequences and remedial measures. Notifications shall be made to affected Data Principals and the Data Protection Board under DPDP requirements, to CERT-In within applicable timelines and to other regulators, law enforcement, insurers and counterparties as required.

7. SEBI and public disclosure

The Company Secretary shall immediately assess the incident under Regulation 30. A disclosure shall not be delayed solely because investigation is incomplete; known facts, impact and mitigation may be disclosed with subsequent updates. Communications shall be accurate and coordinated.

Scaling New Heights

8. Recovery and post-incident review

Systems shall be restored from trusted sources, vulnerabilities remediated and monitoring enhanced. A root-cause report shall record timeline, decisions, control failures, costs and actions. Material incidents shall be reported to the Audit Committee/Board.

9. Preparedness

Backups, restoration, incident exercises, vendor drills, vulnerability management, access reviews and awareness training shall be conducted periodically. Lessons from exercises and incidents shall update plans and controls.

10. Interpretation and overriding effect

Terms not specifically defined in this Policy shall have the meanings assigned to them under the Companies Act, 2013, the rules made thereunder, the applicable SEBI regulations and other governing law. References to statutes and regulations include amendments, clarifications, circulars and re-enactments. If any provision of this Policy conflicts with applicable law, the law shall prevail and this Policy shall be read as modified to the minimum extent necessary.

11. Administration and responsibility

The Board shall retain overall responsibility for this Policy. The committee or officer identified in this Policy shall administer it, maintain evidence of compliance and report material deviations. Every director, officer, employee, consultant and service provider within scope shall provide information and cooperation reasonably required for implementation.

12. Records, training and assurance

The Company Secretary/Compliance Officer shall ensure that approvals, registers, declarations, notices, reports, training records and supporting documents are retained for the period prescribed by law and the Company's document-retention schedule. Periodic awareness and role-based training shall be conducted. Internal audit or an independent reviewer may test compliance and recommend corrective action.

13. Review and amendment

This Policy shall be reviewed at least annually and earlier upon a material change in law, business model, organisation, risk profile or regulatory guidance. Material amendments shall be placed before the competent committee and the Board. The Managing Director and Company Secretary/Compliance Officer may jointly make clerical, contact-detail and statutory-reference corrections that do not alter substantive rights or obligations, subject to reporting to the Board.

For 7Seas Entertainment Limited
Company Secretary / Compliance Officer

Scaling New Heights