ORIENT INSURANCE P.S.C.

United Arab Emirates

DATA BREACH RESPONSE POLICY

&

INCIDENT RESPONSE TEAM (IRT) CHARTER

Document Reference:	**Data Breach Response Policy & IRT Charter**
Version:	Version 1.2
Effective Date:	1st April 2026
Review Cycle:	Annual / Upon Material Change
Approved By:	Data Protection Office - Orient
Classification:	**CONFIDENTIAL — Internal Use Only**

PART I — DATA BREACH RESPONSE POLICY

1. Purpose and Scope

1.1 Purpose

This Data Breach Response Policy ("Policy") establishes the framework, procedures, and accountabilities governing Orient Insurance P.S.C.'s ("Orient Insurance" or "the Company") detection, containment, investigation, remediation, and notification of actual or suspected personal data breaches. The Policy ensures compliance with applicable UAE legislation, Abu Dhabi regulatory requirements, and international information security standards.

Orient Insurance, as a licensed insurance company operating across the UAE and handling Protected Health Information (PHI) in connection with medical insurance products, recognises the heightened sensitivity of the data it processes and is committed to the highest standards of data protection and cybersecurity.

1.2 Scope

This Policy applies to:

- All employees, contractors, consultants, temporary staff, and third-party service providers — including Third Party Administrators (TPAs), brokers, and technology vendors — who process personal data on behalf of Orient Insurance.
- All personal data processed by Orient Insurance whether held electronically, in cloud environments, on portable media, or in paper-based records.
- All systems, networks, applications, and data repositories owned, operated, or managed by or on behalf of Orient Insurance, including systems connected to the Abu Dhabi Health Information Exchange (Malaffi) portal.
- All categories of personal data including: Policyholder PII; Protected Health Information (PHI) including medical history, claims, diagnoses and treatment data; financial and payment data; and employee personal data including Emirates ID and biometric data.

1.3 Regulatory and Standards Framework

This Policy is developed in compliance with and with reference to:

- UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (UAE PDPL) and its implementing regulations - including the mandatory 72-hour notification obligation to the UAE Data Office.
- Abu Dhabi Healthcare Information and Cyber Security Standard Version 2.0 (ADHICS V2, effective August 2024), issued by the Department of Health (DoH) Abu Dhabi - including incident classification (P1–P4), SIMDB maintenance, and mandatory notification to the Abu Dhabi Health Security Operations Centre (AD Health SOC).
- ISO/IEC 27001:2022 - Information Security Management Systems, Annex A Controls A.5.24 to A.5.28 (Information Security Incident Management).
- UAE Federal Law No. 2 of 2019 on the Use of Information and Communications Technology in Health Fields.
- Central Bank of the UAE (CBUAE) has regulatory requirements applicable to licensed insurance entities.

2. Definitions

Term	Definition
Personal Data	Any information relating to an identified or identifiable natural person ("Data Subject") as defined in UAE PDPL Article 1.
Special Category Data / PHI	Sensitive personal data including health/medical data, biometric data, financial information, and national identity numbers. Includes Protected Health Information (PHI) as defined under ADHICS V2.
Data Breach	A security incident resulting in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed by or on behalf of Orient Insurance.
Data Controller	Orient Insurance P.S.C., which determines the purposes and means of processing personal data.
Data Processor	A third party that processes personal data on behalf of Orient Insurance pursuant to a formally executed Data Processing Agreement (DPA).
DPO	Data Protection Officer - the designated individual responsible for overseeing data protection compliance and serving as the primary regulatory liaison.
CISO	Chief Information Security Officer - responsible for Orient Insurance's overall information and cyber security posture.
IRT/ SOC	Incident Response Team - the cross-functional body activated to manage data breach response.
CSIRT/SOC	Computer Security Incident Response Team - the technical sub-group of the IRT that conducts root cause analysis, containment, and eradication, as required under ADHICS V2 Section 11.
SIMDB	Security Incident Management Database - the centralised repository for recording and tracking all security incidents, mandated by ADHICS V2.
AD Health SOC	Abu Dhabi Health Security Operations Centre (DoH) - the authority to which Orient Insurance must report health-related security incidents within ADHICS-prescribed timeframes.
UAE Data Office	The UAE Supervisory Authority for personal data protection. Notifiable breaches must be reported within 72 hours under UAE PDPL.

3. Breach Classification and Severity Levels

Orient Insurance adopts the incident priority classification framework specified in ADHICS V2 (Section 11, Policy Appendix) and aligns it with UAE PDPL risk thresholds. The CISO, in consultation with the Security operation SOC, DPO, shall classify all confirmed breaches within two (2) hours of confirmation.

Priority	Level	Description	Examples	ADHICS V2 — AD Health SOC Notification SLA
P1	Critical	Malicious cyber activity that will disrupt, destroy, or degrade health information systems; total or near-total compromise; active zero-day exploit targeting Orient systems.	Ransomware on claims/medical database; mass exfiltration of PHI or policyholder PII.	Acknowledge: 30 min | Notify SOC: 2 hrs. | Updates: Near Real-Time
P2	Severe	Targeted intrusion or focused attack on systems holding health or financial data; law enforcement involvement triggers automatic High classification.	Phishing-led credential compromise on medical portal;	Acknowledge: 1 hr. | Notify SOC: 4 hrs. | Updates: Every 1 hr.
P3	Elevated	Potential or suspected compromise; known exploitable vulnerability; limited-service degradation.	Misdirected email with policy data; lost unencrypted device; insider access anomaly.	Acknowledge: 1 hr | Notify SOC: 24 hrs | Updates: Every 2 hrs
P4	Normal	General concern: non-critical systems affected; no PHI or financial data at material risk.	Policy number in unsecured internal email; minor misconfiguration with no confirmed exposure.	Acknowledge: 1 hr | Notify SOC: 48 hrs | Updates: Every 24 hrs

4. Data Breach Response Procedure

Phase 1 — Detection and Reporting

All Orient Insurance employees, contractors, and third-party service providers are obligated to report any known, suspected, or potential data breach immediately upon discovery to the Information Security Department via the designated breach reporting channel or IT Help Desk, or directly to the Data protection office or CISO if the Information Security Department is unavailable.

Upon receipt, the Information Security Department shall:

- Record the incident in the SIMDB within one (1) hour, capturing: description and timestamp; identity of the reporting party; assets and systems affected; damages observed; incident status; method of detection; prior similar incidents; supporting evidence; remedial steps already taken; and initial classification.
- Conduct a preliminary analysis to validate whether the event constitutes a confirmed data breach.
- Classify the incident under the P1–P4 framework within two (2) hours of confirmation.

Phase 2 - Activation of the Incident Response Team

Upon confirmation of a P1 or P2 breach - or at the CISO's and SCO discretion for P3/P4 - the IRT shall be formally activated. The CISO shall constitute the CSIRT from permanent IRT members and designated representatives of affected business units and shall immediately notify: the CEO and Board Risk Committee (P1/P2); the DPO to assess regulatory notification obligations; and affected business unit heads.

Phase 3 - Containment

The CSIRT shall implement containment measures proportionate to incident severity:

- Short-term containment: Isolate affected systems; revoke compromised credentials; block malicious IPs or connections; preserve forensic evidence. Third-party network connections shall be terminated where the breach is attributable to a third party, per ADHICS V2 Third Party Security Policy.
- Long-term containment: Apply security patches; strengthen access controls; implement network segmentation; ensure integrity of backup systems.

All containment actions shall be documented in SIMDB with precise timestamps.

Phase 4 - Investigation and Root Cause Analysis

The CSIRT shall conduct a thorough investigation to determine: the full scope of the breach; data categories and volume of records affected; identity of Data Subjects impacted; root cause; and risk to individuals. Evidence shall be retained for a minimum of one (1) year from the date of the incident per ADHICS V2, or longer if required for legal proceedings.

Phase 5 - Notification and Communication

5a. Internal Notification

Senior management and the iGRC team shall be briefed within the timeframes set out in Section 3. The IRT shall provide regular situation updates in accordance with the ADHICS V2 Incident Reporting Matrix throughout the active incident.

5b. UAE Data Office (UAE PDPL - 72-Hour Rule)

Where the breach is likely to result in a risk to the rights of Data Subjects, Orient Insurance shall notify the UAE Data Office within seventy-two (72) hours of becoming aware, specifying: the nature of the breach; categories and approximate number of affected individuals and records; contact details of the DPO; likely consequences; and measures taken or proposed.

5c. AD Health SOC (ADHICS V2)

For breaches involving health information or systems connected to the Abu Dhabi healthcare ecosystem, Orient Insurance shall notify the AD Health SOC strictly within the ADHICS V2 priority SLAs (see Section 3). Notification shall be submitted by the designated Entity Point of Contact via Email (primary) and Phone <TBU> (secondary).

5d. Data Subject Notification

Where a high risk to individuals is identified, affected Data Subjects shall be notified without undue delay in plain language, stating: the nature of the breach; DPO contact details; likely consequences; measures taken; and protective steps they may take.

5e. Third-Party and Contractual Notification

TPAs, reinsurers, brokers, and IT service providers shall be notified as required under their Data Processing Agreements and service contracts. The anonymity of any employee who reported a suspected incident shall be maintained unless the matter is referred to a court of law, per ADHICS V2 Section 11.

Phase 6 — Remediation and Recovery

The CSIRT shall: implement permanent fixes for the root cause; restore affected systems from verified clean backups ensuring data integrity per ADHICS V2 Continuity Policy; verify restored data completeness before return to production; strengthen access controls; and resume operations with enhanced monitoring.

Phase 7 — Post-Incident Review

Within fourteen (14) calendar days of incident closure, a Post-Incident Report shall be prepared and submitted to the CISO and CEO, covering: incident chronology; root cause; effectiveness of the response; quantified trends and costs; corrective and preventive actions (CAPA); and recommended policy updates. All incident documentation is classified CONFIDENTIAL by default, irrespective of severity, per ADHICS V2 Section 11.

5. Breach Register (SIMDB) - Mandatory Fields

Field	Detail Required
Incident Reference Number	Unique identifier assigned at logging
Date and Time of Discovery / Confirmation	Exact timestamps
Incident Priority Level	P1 / P2 / P3 / P4 per ADHICS V2
Nature of Breach	Confidentiality / Integrity / Availability
Data Categories Affected	PHI, PII, Financial, Employee data, etc.
Approximate Number of Records / Data Subjects	Volume
Systems / Assets Affected	Specific applications, infrastructure, media
Root Cause	Technical, human, third-party, or physical
Containment Actions (with timestamps)	Steps taken
Regulatory Notifications Made	UAE Data Office, AD Health SOC - date, time, channel, content summary
Data Subject Notifications	Whether made, date, method, content summary
Remediation Steps	Permanent fixes implemented
Closure Date	Date formally closed in SIMDB
Evidence Retention Date	Minimum 1 year from incident date per ADHICS V2

6. Training, Testing, and Awareness

In accordance with ADHICS V2 and ISO/IEC 27001:2022 Annex A.6.3:

- All IRT members shall undergo annual incident response training and tabletop simulation exercises.
- All staff shall complete mandatory data breach awareness training upon onboarding and annually thereafter.
- Orient Insurance shall participate in DoH ADHICS awareness programs and e-learning initiatives.
- Simulated breach exercises shall be conducted at least annually; findings shall be incorporated into policy updates and the CAPA plan.

7. Policy Compliance and Disciplinary Measures

All employees and engaged third parties must comply with this Policy. Non-compliance may result in: formal disciplinary proceedings under Orient Insurance's HR Disciplinary Procedure (considering nature and gravity of violation, business impact, whether a repeat offence, awareness, and UAE law); termination of employment or contract; and/or civil or criminal liability under UAE PDPL, the UAE Cybercrime Law, and other applicable legislation. Access to systems shall be revoked with immediate effect upon issuance of a termination order, per ADHICS V2 HR Security Policy.

8. Policy Review

This Policy shall be reviewed annually, or upon any material change in applicable law or regulation; a significant breach or near-miss incident; or substantial changes to Orient Insurance's systems or organisational structure.

The DPO and CISO shall coordinate each review. Revisions shall be approved by the CEO and communicated to all relevant personnel.

CROSS-FUNCTIONAL INCIDENT RESPONSE TEAM (IRT) CHARTER

1. CHARTER PURPOSE & AUTHORITY

This Incident Response Team (IRT) Charter (the "Charter") formally establishes the cross-functional team responsible for leading, coordinating, and executing Orient Insurance PJSC's response to data breaches and information security incidents. The IRT derives its authority from the Data Breach Response Policy (OI-INFOSEC-001) and is accountable to the Executive Committee and Board of Directors.

The IRT is empowered to make binding operational decisions during an active incident, including the authority to isolate systems, engage external specialists, suspend third-party services, and initiate mandatory notifications to regulators and affected individuals.

2. IRT STRUCTURE & COMPOSITION

The IRT is structured across two tiers to ensure appropriate response capacity for incidents of all severity levels:

Tier 1: Core IRT (Always Activated)

Activated for all Level 2 (Medium) and above incidents.

Role	Department	Primary Responsibilities	Decision Authority
Incident Commander (IC)	CISO / IT Security	Overall command of the IRT; coordinates all workstreams; final operational decision-maker; owns breach timeline and documentation; reports to CEO and Board.	Full operational authority during active incident
Data Protection Officer (DPO)	Legal / Compliance	Regulatory compliance lead; determines notification obligations under UAE PDPL; owns all regulatory correspondence with UAE Data Office; maintains Breach Register.	Regulatory notification decisions; Breach Register authority
IT Security Lead	IT Security	Technical investigation lead; system forensics; containment and eradication; evidence preservation; vulnerability root cause analysis; system recovery oversight.	Technical containment and system isolation
Legal Counsel	Legal	Legal risk assessment; review and approval of all external communications; contractual obligations review; regulatory correspondence support; evidence admissibility guidance.	External communication approval; legal hold authority
Compliance Officer	Risk & Compliance	Regulatory framework adherence; internal audit liaison; breach classification validation; insurance regulatory notification assessment	Compliance assessment and regulatory escalation

		(CBUAE); policy compliance monitoring.	
HR Business Partner	Human Resources	Employee-related breaches; disciplinary process management; employee communications; training remediation; witness statement coordination.	HR investigation and disciplinary process
PR / Communications Lead	Corporate Communications	External stakeholder messaging; media management; brand protection; customer and partner communications; social media monitoring and response.	External public communications (with CEO approval)
Operations Lead	Business Operations	Business continuity coordination; operational impact assessment; third-party vendor liaison; claims and policy servicing continuity; customer service escalation.	Operational continuity decisions

Tier 2: Extended IRT (Activated for Level 3–4 Incidents)

The following roles are activated at the discretion of the Incident Commander for high-severity or critical incidents:

Extended Role	Activation Trigger & Role
Chief Executive Officer (CEO)	Activated for Level 3–4 incidents. Provides executive oversight; approves regulatory notifications and public communications; briefs the Board of Directors.
Chief Financial Officer (CFO)	Activated when financial data is compromised or significant financial exposure arises. Manages insurance claims, financial impact assessment, and cyber insurance notification.
External Cybersecurity Forensics Firm	Engaged by the CISO for Level 3–4 incidents requiring specialist forensic investigation, malware analysis, or threat actor attribution.
External Legal Counsel (Data Privacy Specialist)	Engaged for complex regulatory exposure, multi-jurisdictional breaches, or potential litigation.
Reinsurance / Actuarial Liaison	Activated where policyholder data involving reinsured portfolios is implicated. Manages reinsurer notification obligations.

3. DEPARTMENTAL RESPONSIBILITIES IN DETAIL

3.1 IT Security Department

The IT Security Department serves as the technical backbone of the IRT. Its responsibilities encompass:

- Continuous monitoring of Orient Insurance systems through Security Information and Event Management (SIEM) tools, Intrusion Detection/Prevention Systems (IDS/IPS), and Data Loss Prevention (DLP) solutions;
- First-line detection and triage of security alerts and anomalies;
- Execution of technical containment measures including network segmentation, account suspension, and firewall rule deployment;
- Forensic image acquisition and digital evidence preservation in a manner admissible for regulatory and legal proceedings;
- Malware analysis, vulnerability root cause identification, and threat actor attribution;

- System restoration from verified clean backups and post-recovery integrity validation;
- Post-incident hardening of technical controls and infrastructure.

3.2 Legal Department

The Legal Department provides the critical legal risk management function during an incident:

- Real-time assessment of the Company's notification obligations under UAE PDPL and applicable regulatory frameworks;
- Review and written approval of all external communications including regulatory notifications, data subject letters, media statements, and third-party correspondence;
- Issuance of legal hold notices to preserve documents and electronic records relevant to the incident;
- Advice on contractual breach notification obligations in data processing agreements and insurance contracts;
- Management of any attendant litigation risk or regulatory investigation;
- Coordination with external data privacy legal counsel where required.

3.3 Compliance Department

The Compliance Department ensures the Company's breach response meets all regulatory and internal policy standards:

- Validation of the breach severity classification assigned by the CISO;
- Assessment of reporting obligations to the CBUAE and other applicable UAE insurance regulators;
- Liaison with the Company's internal audit function and external auditors;
- Monitoring of compliance with prescribed response timelines under UAE PDPL and ISO 27001;
- Integration of breach findings into the Company's risk register and compliance monitoring framework.

3.4 Human Resources Department

The Human Resources Department manages the people dimension of the breach response:

- Leading the investigation and disciplinary process where the breach involves employee negligence, misconduct, or insider threat;
- Coordinating employee communications with the PR team to ensure accurate and consistent messaging;
- Managing remedial training requirements identified as a result of the incident;
- Providing guidance on employment law obligations in respect of employee-related data exposures;
- Facilitating the collection of employee witness statements in coordination with Legal.

3.5 Public Relations / Corporate Communications

The PR/Communications function protects Orient Insurance's reputation and manages information flow to external stakeholders:

- Developing and obtaining CEO approval for all external public communications, including press releases, social media statements, and customer communications;
- Monitoring media and social media channels for breach-related commentary and coordinating the Company's response;
- Preparing holding statements for immediate deployment in the event of public disclosure;
- Advising the IRT on reputational risk implications of proposed response actions;
- Managing communications to brokers, agents, and business partners in coordination with Operations.

3.6 Operations Department

The Operations Department ensures business continuity and manages the operational impact of the breach:

- Assessing the operational impact of containment measures on policyholder services, claims processing, and underwriting activities;
- Activating and managing the Business Continuity Plan (BCP) where operations are materially disrupted;
- Coordinating with third-party vendors, TPAs, and brokers to manage service continuity and breach notifications;
- Maintaining customer service operations and managing escalated customer enquiries relating to the breach;
- Tracking and reporting on operational recovery milestones to the Incident Commander.

4. IRT ACTIVATION & COMMUNICATION PROTOCOLS

4.1 Activation Triggers

- The IRT shall be activated by the CISO or DPO upon confirmation or reasonable suspicion of a data breach at Level 2 severity or above.
- The CISO may activate the IRT at Level 1 severity at their discretion where circumstances warrant.
- Activation shall be communicated to all Core IRT members via the secure IRT Communication Channel (primary: encrypted group messaging platform; secondary: direct phone contact).

4.2 Communication Protocols During Active Incident

- All IRT communications shall be conducted through designated secure channels to prevent inadvertent disclosure of breach details;
- A daily IRT situation report (SitRep) shall be issued by the Incident Commander to all active IRT members during the response period;
- No information regarding the breach shall be shared externally by any IRT member without prior approval of the Incident Commander and Legal Counsel;
- All IRT decisions and actions shall be contemporaneously documented in the Breach Register;
- IRT meetings shall be conducted at minimum daily during an active Level 3–4 incident and as determined by the Incident Commander for Level 2 incidents.

4.3 Escalation Path

Severity	Escalates To	Timeline	Board Notification
Level 1	CISO / DPO	Within 24 hours	Not required
Level 2	CISO, DPO, Legal	Within 4 hours	Summary report at next meeting
Level 3	CEO, CISO, DPO, Legal, HR	Within 2 hours	Within 24 hours
Level 4	CEO, Board, Full IRT	Immediate	Immediate emergency session

5. IRT PERFORMANCE METRICS & KPIS

The IRT's effectiveness shall be measured against the following Key Performance Indicators, reviewed quarterly by the CISO and annually by the Executive Committee:

KPI Metric	Target	Measurement Method
Mean Time to Detect (MTTD)	< 4 hours	SIEM alert-to-IRT notification time

Mean Time to Contain (MTTC)	< 12 hours (Level 3–4)	IRT activation to containment confirmation
Regulatory Notification Timeliness	100% within 72 hours	DPO submission records vs. breach discovery timestamp
Data Subject Notification Timeliness	< 5 business days (high risk)	Notification dispatch records
Post-Incident Review Completion	100% within 20 business days	PIR report dates vs. breach closure
IRT Training Completion Rate	100% annually	HR training records
Tabletop Exercise Frequency	Minimum 1x per year	Exercise completion records

6. CHARTER GOVERNANCE

- This Charter shall be reviewed annually by the CISO and DPO, with approval from the Executive Committee.
- IRT membership shall be reviewed upon any organisational restructuring, senior personnel change or following a post-incident review that identifies structural gaps.
- IRT members who are unavailable during an incident shall designate a qualified alternate who has received equivalent IRT training.
- This Charter shall be distributed to all IRT members and maintained in the Company's Document Management System under restricted access.

IRT CHARTER APPROVAL & ACKNOWLEDGEMENT

All IRT members are required to sign this Charter to confirm understanding of and commitment to their roles and responsibilities.

IRT Role	Name & Signature	Date
Incident Commander	_____	_____
Data Protection Officer (DPO)	_____	_____
IT Security Lead	_____	_____
Compliance Officer	_____	_____
HR Head	_____	_____
PR / Communications Lead	_____	_____
Operations Lead	_____	_____

— END OF DOCUMENT —