Security incident management policy

Company Name	Origen Technologies
Document Title	Origen Security incident management policy
Document Index	CSA-LAC-008
Document Owner	Chief Information Security Officer
Version	1.1
Effective Date	06 July 2026
Review Frequency	Annual review required, or earlier upon material changes to systems, services, regulations, or access control processes.
Next Scheduled Review	08 July 2027

Document Revision History

Version	Date	Description of Change	Author/Owner	Approval
1.0	2026-01-01	**Baseline Release:** Initial formalization of the Disaster Recovery Framework aligned with GDPR and ISO 27001 standard practices.	InfoSec & Delivery Leadership	approval
1.1	2026-07-08	Audit Optimization & Integration: Consolidated core incident management lifecycles into a unified response framework. Integrated explicit PII data classification references from Global Privacy guidelines for enhanced regulatory alignment. Added structural tables mapping containment protocols and post-incident forensic activities.	Security Program Office / CISO	Approval

ORIGEN CLOUD SOLaaS
(Solution as a Service) SECURITY ADDENDUM

This policy defines Origen Tech's formal framework for protecting personal, confidential, and business-critical data in the event of an incident or operational disruption. The primary objective is to guarantee data availability, system integrity, confidentiality, and statutory regulatory compliance during and after security events.
The scope encompasses:

- All production and non-production environments (Cloud and On-Premise infrastructure).

- Enterprise solutions including ERP systems (SAP), CRM platforms, and Data Warehouses.
- All internal employees, contractors, systems, and third-party integrations handling corporate or customer content.

This framework is strictly aligned with GDPR (Articles 32, 33, and 34), ISO/IEC 27001 (Annex A.5, A.8, A.12, A.17), and SOC 2 Trust Services Criteria (Security, Availability, Confidentiality).

1. Roles, Responsibilities & Contacts

Operational accountability during a high-pressure security or disaster recovery event is distributed as follows:

- Executive Management: Approves the overall disaster recovery strategy, establishes risk appetite boundaries, and authorizes critical business funding.
- Chief Information Security Officer (CISO) & Security Office: Leads the enterprise information security program, reviews corporate security controls, and approves any exceptions regarding elevated workspace or production infrastructure permissions.
- Delivery Head (Disaster Recovery & Incident Owner): Retains end-to-end operational ownership over plan
- Delivery Ambassadors: Represent delivery excellence across product suites, ensuring that technical disaster recovery controls are implemented consistently across all production tiers.
- Data Protection Officer (DPO): Oversees statutory data privacy compliance, initiates GDPR breach impact assessments, and coordinates formal communications with supervisory authorities.
- IT & Security Operations Team: Executes technical backup strategies, handles direct containment measures, performs log aggregation/monitoring, and conducts mandatory quarterly backup verifications.

2. Incident Classification & Prioritization

Infrastructure assets, corporate solutions, and security events are prioritized using an objective matrix based on operational impact and data sensitivity classifications (including Personally Identifiable Information - PII).

System Classification	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)	Operational Impact Definition
Mission Critical	4 Hours	15 Minutes	Complete failure or compromise of a production system affecting vital business operations with no immediate workaround

System Classification	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)	Operational Impact Definition
			(e.g., primary SAP outage or validated severe security breach).
Business Critical	8 Hours	1 Hour	Serious disruption that degrades operational capacity or renders major individual features unusable, but permits core business tracking to continue.
Standard Systems	24 Hours	24 Hours	Minor or localized operational anomalies with low business impact, general queries, or failures entirely isolated to testing and non-production tiers.

3. Incident Analysis

A rigorous analytical methodology is applied to eliminate diagnostic errors and identify affected perimeters promptly:

- Detection & Triage: Automated alerting engines aggregate operational logs. Upon security team validation, an event is classified under standard severity tiers within 1 hour.
- Data Privacy Scope: If customer content or confidential database perimeters are breached, a formal privacy assessment is initiated immediately under the direction of the DPO.
- Regulatory Timelines: A comprehensive data impact review must be finalized within 24 hours of identification to assess the probability of a personal data breach under GDPR criteria.

4. Containment & Escalation Protocols

Containment procedures are triggered immediately to minimize blast radiuses and protect adjacent environments:

- Isolation Procedures: Technical actions include immediate environment segmentation, network traffic rerouting via firewall perimeter adjustments, and disabling compromised administrative access privileges.
- Session and Account Constraints: Workstation security safeguards enforce a strict 15-minute inactivity timeout. Standard accounts are restricted to non-administrative

privileges, and any emergency access granted during containment is automatically revoked post-incident.

- Internal Escalation: Mandatory internal escalations and management briefings to Executive Leadership and Corporate Security Functions must be executed within **1 hour** of incident confirmation.

5. Recovery & Privacy Safeguards

System restoration activities must protect data integrity and privacy throughout the recovery lifecycle:

- **Backup Restoration:** Replications utilize daily automated snapshots. Backups are natively encrypted using Advanced Encryption Standard (AES) 256-bit protocols and distributed via geo-redundant storage.
- **Data Protection In-Transit:** Web and application communication sessions utilized during recovery environments strictly enforce Transport Layer Security (TLS 1.2+) by default.
- **Forensic Auditing:** Immutable logging and tamper-proof audit trails remain fully active during all recovery procedures to document actions taken for subsequent compliance verification.

6. Notification Flow (External)

- **Regulatory Notification:** In the event of a verified Personal Data Breach impacting data subjects, Origen Tech is bound by regulatory frameworks to notify the competent supervisory authorities within **72 hours**.
- **Customer Notification:** Affected clients and partners are notified without undue delay, strictly conforming to the communication timelines and requirements detailed in individual enterprise service contracts. All public statements must be coordinated and pre-approved by the Corporate Legal and Data Protection functions.

7. Post-Incident Activity & Continuous Learning

Origen Tech treats every incident as an opportunity to strengthen structural resilience and update corporate knowledge bases:

- **Root Cause Analysis (RCA):** For all critical or high-severity events, technical teams must execute a comprehensive After-Action Review (AAR) to isolate root technical and process failures.
- **Remediation Tracking:** Findings, vulnerabilities discovered, and corrective actions are formally recorded in the centralized Origen Risk Register. Progress against critical implementation milestones is monitored directly by the Origen Risk Management Committee (URMC).
- **Testing, Simulations & Training:** Tabletop exercises for executive management and technical incident response simulations are conducted **annually**. Localized delivery workshops are held periodically to refine disaster recovery runbooks, adapt to emerging regulatory standards, and optimize service delivery performance.