Incident Response Plan

ProvisionIQ Ltd — Operational Playbook for Security Incidents

Document	Incident Response Plan (IRP) — Operational
Version	1.0
Date	22 May 2026
Owner	CTO (Incident Commander)
Tested	21/05/2026
Related	Incident Response Policy · BCP · DRP · Privacy Policy
Classification	CONFIDENTIAL — IRT members and management only

Activation

This plan is activated whenever an event meets the threshold for P1 or P2 classification (see Section 1). It provides the operational detail that the Incident Response Policy summarises.

The Incident Commander has authority to deviate from this plan where circumstances require it, provided deviations are documented in the Incident Log within 30 minutes.

1. Activation Criteria and IRT Contact List

Priority	Activation Criteria
P1 CRITICAL	Activate immediately (24/7): ransomware; confirmed exfiltration of pupil data; complete platform outage; safeguarding data exposure
P2 HIGH	Activate within 30 minutes: confirmed unauthorised access to any customer data; partial platform outage affecting multiple customers; malware detected on production infrastructure

IRT Role	Contact (complete before publishing)
Incident Commander (CTO)	Liam Wheldon – liam@provisioniq.org
Deputy IC (COO.)	Jen Longden- jen@provisioniq.org

DPO	Liam Wheldon- liam@provisioniq.org
Customer Success Lead	Jen Longden- jen@provisioniq.org
Legal Counsel	Dan Howard- dan@provisioniq.org
Communications Lead (CEO)	Dan Howard- dan@provisioniq.org
Cloud Infrastructure Contact	https://aws.amazon.com/contact-us/compliance-support/
Cyber Insurance Insurer	Hiscox Insurance · Policy No: PSC10003967417 · 24hr claims line: 01206 773 791 or 0800 840 2782

2. Phase 1 — Detect and Report (0–30 min)

Minute	Action	Owner
0	Event detected / reported. First responder completes Incident Report Form (IRF). Do NOT attempt to fix or investigate independently.	Any staff member
0–5	First responder emails security@provisioniq.co.uk with: what happened, what systems/data affected, what actions taken, their contact details.	First Responder
0–10	Automated monitoring alert OR manual report reaches Head of Engineering / CTO on-call.	Automated / On-call
10–20	Incident Commander (IC) reviews IRF. Makes initial classification decision. Declares incident.	Incident Commander
20–30	IC activates IRT (P1: all roles; P2: core roles). Opens incident channel. Assigns Incident Log owner.	Incident Commander

3. Phase 2 — Classify and Contain (30 min – 4 hrs)

Time	Action	Owner
T+30 min	Full IRT on bridge call. IC briefs team. Lead Engineer confirms systems affected. Initial scope assessment.	IC + Lead Eng.
T+30–60 min	EVIDENCE PRESERVATION: memory dumps, log exports, network captures, disk images of affected systems. Hash all evidence.	Lead Engineer

T+60 min	CONTAINMENT: isolate affected systems; revoke compromised credentials; block attack IPs at WAF. Document every action in Incident Log.	Lead Engineer
T+60–90 min	DPO assesses personal data breach status: what data? How many individuals? Is it notifiable? Documents initial assessment.	DPO
T+90 min	IC approves customer communication draft (P1: within 2 hours; P2: within 4 hours). Customer Success prepares notifications.	IC + CS Lead
T+2 hrs	P1: Board notified by IC. Customer notifications sent. ICO breach assessment initiated if personal data breach suspected.	IC + DPO
T+4 hrs	Containment verified. Root cause investigation begins. Vulnerability scan of all adjacent systems.	Lead Engineer

4. Phase 3 — Investigate and Eradicate (4–24 hrs)

1. Root cause analysis: identify attack vector, vulnerability exploited, initial point of compromise, lateral movement path, data accessed or exfiltrated
2. Full scope determination: all affected systems, accounts, and data records. Update Data Controller notification with confirmed scope.
3. Threat intelligence: search for known indicators of compromise (IOCs); check threat intelligence feeds; consider sharing IOCs with NCSC
4. Eradication: remove all malware, backdoors, or unauthorised access. Patch or mitigate exploited vulnerability. Verify no persistence mechanisms remain.
5. ICO notification (if personal data breach and notifiable): DPO submits via ico.org.uk/report-a-breach. Target: within 8 hours of confirmed breach; hard deadline 72 hours.
6. Forensic report draft: Lead Engineer documents full technical timeline and findings

5. Phase 4 — Recover (24–72 hrs)

Step	Action	Criterion to Proceed
5.1	Define recovery sequence: critical services first. Agree with IC.	Root cause eradicated and verified
5.2	Rebuild / restore affected systems from known-good backups (pre-compromise). NOT from backups taken after compromise without explicit verification.	Clean backup identified and verified
5.3	Vulnerability scan and configuration check of all restored systems.	Zero critical/high findings
5.4	Functionality test: all platform features tested in staging before returning to production.	All features confirmed working

5.5	Production traffic restored in controlled phases. Monitoring on maximum sensitivity for 72 hours.	IC sign-off
5.6	All-Clear declared by IC. Customer Success notifies affected Data Controllers of restoration.	Lead Engineer confirms clean

6. Phase 5 — Post-Incident Review

Element	Standard
Timing	PIR meeting within 5 business days of All-Clear. Interim findings to Board within 24 hours for P1.
Agenda	Timeline; root cause; impact (technical, data, customer, regulatory, financial); what worked; what didn't; improvement actions
Report	Written PIR report (not blame-focused). Retained permanently. Shared with Board and insurers.
Actions	All improvement actions tracked with owner and deadline. Reviewed monthly by CTO.
Policy update	This plan updated if gaps identified. Full policy review triggered for P1 incidents.
Insurance claim	Notify cyber insurer within 24 hours of any P1 incident. Provide PIR report to insurer.

Ransomware-Specific Protocol

If ransomware is suspected: 1) ISOLATE affected systems from network immediately (unplug network cable / disable WiFi). 2) Do NOT reboot. 3) Do NOT pay the ransom without Board and Legal sign-off. 4) Preserve all evidence (encrypted files, ransom note, screenshots). 5) Contact cyber insurer immediately — many policies include ransomware negotiation services. 6) Initiate recovery from pre-compromise backups.

ProvisionIQ's backup architecture (WORM storage, separate facility, AES-256 encrypted) is specifically designed to survive ransomware. Clean backups should be available within the hourly RPO window.