ResolvX

Incident Response Plan

IR-PLAN-001 - v1.0 - 2026 - Internal - Restricted

Document Information

Document ID	IR-PLAN-001
Version	1.0
Status	Active
Classification	Internal - Restricted
Owner	GRC Lead - Derick G. Dmello
Approver	CISO
Review Cycle	Annual; after each P1/P2 incident
Next Review	Q1 2027
Framework Alignment	NIST SP 800-61 Rev 2 - ISO/IEC 27001:2022 A5.24-A5.28 SOC 2 CC7.3-CC7.5 - NIST CSF 2.0 RS Family

ResolvX - Incident Response Plan

Document ID: IR-PLAN-001 | **Version:** 1.0 | **Status:** Active
Owner: GRC Lead | **Approver:** CISO | **Classification:** Internal - Restricted

Framework Alignment: NIST SP 800-61 Rev 2 | ISO/IEC 27001:2022 A5.24-A5.28 | SOC 2 CC7.3-CC7.5 | NIST CSF 2.0 RS Family

1. Purpose and Scope

1.1 Purpose

This Incident Response Plan (IRP) establishes ResolvX's capability to prepare for, detect, contain, eradicate, recover from, and learn from information security incidents. It defines the processes, roles, responsibilities, communication protocols, and decision criteria that govern how ResolvX responds when a security incident occurs or is suspected.

The plan exists to:

- Minimise the impact of incidents on ResolvX's clients, personnel, and business operations.
- Ensure consistent, coordinated, and documented responses regardless of who is on duty.
- Meet contractual obligations to clients (SOC 2 CC7.3-CC7.5) and regulatory notification requirements (GDPR Art. 33-34, ISO A5.24-A5.26).
- Generate evidence of incident management capability for audit purposes.
- Continuously improve ResolvX's security posture through structured post-incident learning.

1.2 Scope

This plan applies to all information security incidents affecting ResolvX systems, data, personnel, or clients - including but not limited to:

- Unauthorised access to systems or data
- Malware infections (ransomware, spyware, trojans)
- Phishing attacks and social engineering
- Data breaches involving personal data or client data
- Denial of service attacks
- Insider threats
- Physical security incidents affecting information assets
- Third-party/vendor security incidents with downstream impact on ResolvX

This plan applies to all ResolvX personnel, contractors, and vendors with access to ResolvX systems.

1.3 Relationship to Other Documents

Document	Relationship
Information Security Policy (POL-001)	Parent policy; provides authority for this plan
Access Control Policy (POL-003)	Governs access revocation during incident response
Data Classification Policy (POL-004)	Determines notification obligations based on data type
Privacy Programme (POL-006)	Governs personal data breach notifications
Runbook - Phishing (IR-RB-001)	Tactical procedures for phishing incidents
Runbook - Ransomware (IR-RB-002)	Tactical procedures for ransomware incidents
Runbook - Data Breach (IR-RB-003)	Tactical procedures for data breach incidents
Incident Log Template (IR-LOG-001)	Operational record for each incident

2. Incident Classification

2.1 Severity Levels

ResolvX classifies incidents using a four-tier severity model based on NIST SP 800-61 functional impact, information impact, and recoverability criteria.

Severity	Label	Criteria	Initial Response SLA
P1	Critical	Client data confirmed exfiltrated; ransomware encrypting production systems; complete loss of critical service availability; active attacker in production environment	Immediate - within 15 minutes of detection
P2	High	Suspected data breach under investigation; malware contained but not eradicated; significant degradation of critical services; compromised privileged account	Within 1 hour of detection
P3	Medium	Single endpoint malware (contained); phishing with no confirmed credential compromise; access policy violation; minor service degradation	Within 4 hours of detection
P4	Low	Blocked phishing attempt; failed brute force with no access gained; security alert requiring investigation but no confirmed incident	Next business day

2.2 Incident vs. Event

Not all security alerts are incidents. An **event** is any observable occurrence in a system or network. An **incident** is an event that actually or potentially jeopardises the confidentiality, integrity, or availability of an information asset.

The initial responder (typically GRC Lead or on-call engineer) makes the event-to-incident determination using the criteria in Section 2.1. When uncertain, escalate - do not wait for certainty before engaging the incident response process.

2.3 Incident Categories

Category	Examples
Malware	Ransomware, spyware, trojans, cryptominers, worms
Unauthorised Access	Account compromise, privilege escalation, insider threat, physical intrusion
Data Breach	Exfiltration, accidental disclosure, third-party breach affecting ResolvX data
Denial of Service	DDoS, resource exhaustion, service disruption
Social Engineering	Phishing, spear phishing, vishing, BEC (business email compromise)
Supply Chain	Vendor breach with downstream impact; compromised software update
Physical	Stolen device, physical access to infrastructure
Policy Violation	Intentional or negligent violation of security policies

3. Roles and Responsibilities

3.1 Incident Response Team (IRT)

ResolvX does not maintain a dedicated full-time Security Operations Centre. The IRT is assembled on-demand from existing roles. Core membership:

Role	IRT Function	Contact
GRC Lead	Incident Commander - overall coordination, regulatory notifications, documentation, post-incident review	Primary IR contact
Head of Cloud Ops	Technical Lead - cloud infrastructure containment, forensic preservation, AWS-level response	On-call rotation
IT Admin	Identity Response - account revocation, MFA enforcement, endpoint isolation via Jamf	On-call rotation

DevSecOps	Application/Code Response - malware analysis, code integrity verification, secrets rotation	On-call rotation
CISO	Executive Escalation - P1/P2 notification, risk acceptance decisions, board/client communication authority	Escalation path
Legal	Legal and Regulatory - GDPR notification decisions, law enforcement liaison, evidence handling guidance	On-call for P1/P2
VP Engineering	BCM/Recovery - service restoration prioritisation, engineering resource allocation	Escalation path

3.2 Incident Commander Responsibilities

The GRC Lead acts as Incident Commander for all incidents. Responsibilities:

- Declare incident severity and open an incident log entry.
- Assemble the appropriate IRT subset for the incident type and severity.
- Maintain the incident timeline and decision log throughout.
- Coordinate internal and external communications.
- Make go/no-go decisions on containment actions with business impact.
- Determine regulatory notification obligations (GDPR 72-hour window, client SLA obligations).
- Convene post-incident review within 5 business days of resolution.

For P1 incidents where the GRC Lead is unavailable: the Head of Cloud Ops assumes Incident Commander duties and notifies the CISO immediately.

3.3 On-Call Coverage

P1 and P2 incidents require 24/7 response capability. Out-of-hours escalation path:

- Alert to #security-alerts Slack channel (auto-paged to on-call).
- Direct call to GRC Lead.
- If no response within 15 minutes: escalate to CISO.
- If CISO unavailable: escalate to CEO.

On-call rotation schedule is maintained by IT Admin and reviewed monthly.

4. Incident Response Lifecycle

ResolvX follows the NIST SP 800-61 Rev 2 four-phase lifecycle:

Preparation -> Detection & Analysis -> Containment, Eradication & Recovery -> Post-Incident Activity

4.1 Phase 1: Preparation

Preparation is ongoing - not a reactive phase. ResolvX maintains readiness through:

Technical preparation:

- AWS CloudTrail enabled across all accounts; logs shipped to centralised S3 bucket with integrity validation.
- Okta audit logs retained for 12 months; anomaly alerts configured.
- GuardDuty enabled in all AWS regions with findings routed to GRC Lead.
- Jamf remote wipe capability tested quarterly.
- Backup integrity tested monthly; offsite backup verified quarterly.
- Runbooks maintained and reviewed after each exercise or incident.

Organisational preparation:

- All personnel complete security awareness training annually (phishing simulation included).
- IRT members briefed on this plan at onboarding and after each revision.
- Emergency contact list maintained and tested quarterly.
- Out-of-band communication channel established (Signal group for IRT) for use if corporate comms are compromised.
- Legal on-call arrangement confirmed with external counsel for P1/P2 support.
- Regulatory notification templates pre-drafted (GDPR DPA, client notification, internal) - held by GRC Lead.

Documentation maintained:

- Incident Log Template (IR-LOG-001) - ready for immediate use.
- Evidence handling procedures documented in Section 5.3.
- Communication templates for each notification type (Section 6).

4.2 Phase 2: Detection and Analysis

4.2.1 Detection Sources

Incidents may be detected through:

Source	Tooling	Responsible
Cloud infrastructure alerts	AWS GuardDuty, CloudTrail, Security Hub	Head of Cloud Ops
Endpoint alerts	Jamf, EDR agent	IT Admin
Application monitoring	Datadog APM; application error rates	DevSecOps

Authentication anomalies	Okta threat intelligence; impossible travel; failed MFA spikes	IT Admin
Vulnerability scanning	Snyk; AWS Inspector	DevSecOps
Staff reports	Any channel; #security-alerts Slack	Any personnel
Vendor notifications	Vendor security bulletins; SOC 2 bridge letters	GRC Lead
External intelligence	CISA advisories; CERT alerts	GRC Lead

4.2.2 Initial Analysis Checklist

Upon receiving an alert or report, the initial responder must:

- Record the date, time, source, and nature of the alert/report in the Incident Log.
- Determine whether the activity constitutes a security event or a confirmed/suspected incident.
- If an incident: assign initial severity (P1-P4) using criteria in Section 2.1.
- Notify the GRC Lead (or Incident Commander) immediately.
- Do NOT attempt independent remediation before the IRT is assembled.
- Preserve evidence - do not power off affected systems unless directed by the Incident Commander.
- Avoid discussing details on potentially compromised channels; use out-of-band comms for P1/P2.

4.2.3 Scope Determination

The IRT must determine:

- Which systems, accounts, and data are confirmed or potentially affected.
- Whether the incident is ongoing or historical.
- The attack vector and initial access point (if determinable).
- Whether client data is involved - this triggers notification obligations.
- Whether personal data is involved - this starts the GDPR 72-hour clock.

Scope assessment is documented in the Incident Log and updated continuously as new information emerges.

4.2.4 Severity Escalation

Severity can be escalated but not de-escalated during the active incident phase. If new information indicates a higher impact than initially assessed, the Incident Commander re-classifies and notifies appropriate personnel immediately.

4.3 Phase 3: Containment, Eradication, and Recovery

4.3.1 Containment

Containment objectives: stop the spread; preserve evidence; maintain business operations where safe to do so.

Immediate containment actions by incident type:

Incident Type	Immediate Containment
Compromised account	Revoke all sessions via Okta; disable account; rotate credentials; preserve auth logs
Malware on endpoint	Isolate via Jamf (network disconnect); do not power off; notify IT Admin
Ransomware	Isolate affected systems from network immediately; disable affected AWS resources; contact Head of Cloud Ops
Data exfiltration	Block outbound traffic to destination IP/domain; revoke relevant API keys; preserve network logs
Phishing campaign	Block sender domain in email gateway; alert all staff; review for credential compromise
Compromised AWS account	Revoke IAM keys; enable AWS root MFA; contact Head of Cloud Ops; isolate affected resources

Containment decisions that affect service availability (e.g. taking down a production system) require Incident Commander approval. For P1 incidents, CISO is notified before any production shutdown.

4.3.2 Evidence Preservation

Evidence must be preserved before any remediation action. Per NIST SP 800-61 and ISO A5.28:

- Capture volatile data first: running processes, network connections, memory contents, open files.
- Take forensic disk images before wiping or rebuilding systems.
- Preserve all relevant logs with timestamps and chain-of-custody records.
- Photograph physical evidence where applicable.
- Document every action taken on affected systems with timestamp and operator name.
- Consult Legal before engaging law enforcement or discarding evidence.

Evidence is preserved for a minimum of 3 years for P1/P2 incidents, 1 year for P3/P4.

4.3.3 Eradication

After containment is confirmed:

- Identify and remove all malicious artefacts (malware files, backdoors, scheduled tasks, persistence mechanisms)
- Revoke and rotate all potentially compromised credentials, API keys, and certificates
- Patch or remediate the vulnerability exploited to gain initial access
- Verify eradication is complete before proceeding to recovery

4.3.4 Recovery

Recovery objectives: restore affected systems to verified clean state; resume normal operations; validate integrity.

Recovery steps:

- Restore from known-good backup or rebuild from verified image - do not restore from potentially compromised snapshots
- Apply all security patches before reconnecting to network
- Re-enable or re-provision affected accounts with fresh credentials
- Validate service functionality and data integrity before declaring recovery complete
- Monitor closely for 72 hours post-recovery for signs of reinfection or persistence

Recovery timeline targets by severity:

Severity	Target RTO
P1	4 hours (critical services); 24 hours (full restoration)
P2	8 hours
P3	24 hours
P4	72 hours

4.4 Phase 4: Post-Incident Activity

4.4.1 Lessons Learned Meeting

Per NIST SP 800-61 Section 3.4.1 and ISO A5.27, a lessons learned meeting must be held within 5 business days of incident resolution for P1/P2 incidents, and within 10 business days for P3. P4 incidents are reviewed in the next monthly security review.

Agenda:

- Timeline walkthrough: what happened, when, how it was detected
- Root cause analysis
- Effectiveness of the response: what worked, what did not
- Identification of control gaps or process failures
- Action items with owners and deadlines
- Updates required to this plan, runbooks, or controls

4.4.2 Post-Incident Report

A written post-incident report is required for all P1 and P2 incidents. The report covers:

- Executive summary suitable for CISO and client communication
- Detailed timeline with timestamps
- Root cause and contributing factors
- Business and data impact assessment
- Response actions taken
- Control gaps identified

- Recommendations and remediation actions with owners
- Evidence inventory

Reports are stored in the GRC Lead's evidence library, retained for 5 years.

4.4.3 ISMS Improvement

Findings from incidents must feed back into:
- Risk register (update affected risks; add new risks identified)
- Control matrix (update status of failed controls; add compensating controls)
- This IRP (update procedures where gaps were found)
- Security awareness training (add scenarios based on real incidents)

5. Communication Protocols

5.1 Internal Communication

Audience	Channel	Timing	Owner
IRT members	Out-of-band Signal group (P1/P2); Slack #security-incident (P3/P4)	Immediately on incident declaration	Incident Commander
CISO	Direct call or Signal	P1: immediately; P2: within 1 hour	Incident Commander
CEO	Direct call	P1 only; at CISO's discretion	CISO
All staff (need-to-know only)	Internal email or Slack	When containment is confirmed, if staff action required	Incident Commander + CISO

All internal incident communications are marked CONFIDENTIAL and restricted to those with a need to know.

5.2 External Notification Obligations

Obligation	Trigger	Deadline	Owner
GDPR supervisory authority (Irish DPC)	Personal data breach with risk to individuals	72 hours from becoming aware	GRC Lead + Legal
GDPR data subject notification	High risk to individuals' rights and freedoms	Without undue delay	Legal
Client notification (as data processor)	Breach affecting client data	Per DPA - typically 24-72 hours	GRC Lead + Account Manager
Law enforcement	Where criminal activity suspected	GRC Lead + Legal decision	Legal
Cyber insurer	P1/P2 incidents	Per policy terms - typically within 72 hours	GRC Lead

AWS (if infrastructure breach)	AWS-level compromise	Immediately	Head of Cloud Ops

The 72-hour GDPR clock starts from the moment ResolvX becomes **aware** of a probable breach - not from confirmation. When in doubt, notify. An early notification can be supplemented; a missed deadline cannot be undone.

5.3 Communication Restrictions

During an active incident:

- Do NOT discuss incident details on potentially compromised channels
- Do NOT post on social media or public forums
- Do NOT confirm or deny incident details to external parties without Legal approval
- All media enquiries are directed to the CEO
- Client communications require CISO approval for content before sending

6. Regulatory Notification Templates

Pre-drafted notification templates are maintained by the GRC Lead in a secure, offline-accessible location. Templates exist for:

A. GDPR supervisory authority notification (Art. 33)

Covers: nature of breach; categories and approximate number of data subjects; categories and approximate number of records; name and contact of DPO-equivalent; likely consequences; measures taken and proposed.

B. Data subject notification (Art. 34)

Plain language description of the breach; likely consequences; measures taken to address the breach; contact point for queries.

C. Client notification (data processor to controller)

Per DPA obligations: incident summary; data categories affected; preliminary root cause; immediate actions taken; next steps; GRC Lead contact.

D. Internal staff notification

For incidents requiring staff action (e.g. credential reset): what to do, what not to do, who to contact.

Templates are reviewed annually and after each P1/P2 incident.

7. Evidence Handling

Evidence management follows NIST SP 800-61 Section 3.3.2 and ISO A5.28.

Chain of custody requirements:

- Every piece of evidence is labelled with: incident ID, date/time collected, collector name, system source
- Evidence log maintained throughout the incident lifecycle
- Physical evidence stored securely with access restricted to IRT and Legal
- Digital evidence stored in write-protected format; MD5/SHA-256 hashes computed at collection

Evidence retention:

- P1/P2 incidents: 3 years minimum
- P3/P4 incidents: 1 year minimum
- Incidents involving litigation or regulatory investigation: retained until resolution plus 2 years

Law enforcement engagement:

Do not contact law enforcement without Legal approval. If law enforcement contact is initiated by a third party, refer to Legal immediately. Evidence must not be shared with law enforcement without Legal sign-off.

8. Testing and Maintenance

8.1 Plan Testing

This plan is tested through:

Test Type	Frequency	Owner
Tabletop exercise (scenario-based discussion)	Annual	GRC Lead
Functional drill (simulated phishing campaign + response)	Annual	GRC Lead + IT Admin
Communication test (out-of-band contact list verification)	Quarterly	GRC Lead
Backup restoration test	Quarterly	Head of Cloud Ops

Test results are documented and deficiencies tracked to resolution.

8.2 Plan Maintenance

This plan is reviewed and updated:

- Annually as part of the ISMS management review cycle
- Following any P1 or P2 incident (within 30 days of resolution)
- Following any significant change to ResolvX's technology stack, team structure, or regulatory environment
- Following each tabletop or functional exercise

All revisions require GRC Lead authorship and CISO approval before publication.

9. Document Control

Field	Detail
Document ID	IR-PLAN-001
Version	1.0
Status	Active
Classification	Internal - Restricted
Owner	GRC Lead – Derick G. Dmello
Approver	CISO
Review Cycle	Annual; after each P1/P2 incident
Next Review	Q1 2027
Framework References	NIST SP 800-61 Rev 2 Sections 3.1-3.4 · ISO/IEC 27001:2022 A5.24-A5.28 · SOC 2 TSC CC7.3, CC7.4, CC7.5 · NIST CSF 2.0 RS.MA, RS.AN, RS.CO, RS.MI, RS.IM
Related Documents	IR-RB-001 (Phishing), IR-RB-002 (Ransomware), IR-RB-003 (Data Breach), IR-LOG-001 (Incident Log Template)

ResolvX GRC Program - Internal Use Only - v1.0 - 2026

Authorisation

Role	Name	Date
CEO		
CISO		
GRC Lead	Derick G. Dmello	