

# VeriQuery Incident Response Plan

**Document Version:** 1.0 **Last Updated:** April 19, 2026 **Classification:** Public (Personal contact details and on-call schedules are maintained in a separate internal supplement)

## Objective

To minimise the impact of a security incident, protect user data, restore normal service as quickly as possible, and ensure compliance with legal notification requirements including GDPR (72-hour rule) and CCPA.

## 1. Severity Classification

All incidents are classified before a response is initiated.

Severity	Description	Examples	Initial Response Target
SEV-1	Critical — active breach or data exposure confirmed	Confirmed unauthorised DB access, leaked credentials in use, active exfiltration	Immediate — within 15 minutes
SEV-2	High — potential exposure or significant service impact	Suspicious access patterns, credential leak detected (not yet exploited), major service outage	Within 1 hour
SEV-3	Low — no PII exposed, limited service impact	UI bug with no data risk, failed login anomaly with no breach, minor degradation	Within 24 hours (next business day)

## 2. Roles & Responsibilities

Role	Responsibilities
------	------------------

<b>Incident Commander</b>	Declares the incident, coordinates the response, makes containment decisions, signs off on external communications
<b>Engineering Lead</b>	Leads technical investigation, implements containment and eradication steps, maintains the incident timeline
<b>Communications Lead</b>	Drafts and sends customer notifications, status page updates, and regulatory disclosures
<b>Legal / Compliance Reviewer</b>	Advises on notification obligations (GDPR DPA, CCPA AG), reviews external communications before sending

*Operational contact details, escalation chains, and on-call schedules are maintained in the internal IRP supplement, available to authorised personnel only.*

### 3. Phase 1 — Detection & Reporting

Incidents are identified via one of the following channels:

- **Automated monitoring:** Uptime, error-rate, and anomaly alerts from infrastructure tooling.
- **Internal discovery:** Engineering team identifies unexpected behaviour during normal operations.
- **External report:** A user or security researcher submits a report to [security@magicapps.dev](mailto:security@magicapps.dev).

Upon detection, the discoverer immediately notifies the Incident Commander and opens a dedicated incident channel (details in the internal supplement). All actions and observations are logged from this moment.

#### Automated Alert Response: **Veriquery\_Production\_Error**

When the `Veriquery_Production_Error` CloudWatch alarm fires, an SNS email notification is sent automatically. This is a **SEV-2** incident by default. Escalate to **SEV-1** immediately if data exposure is confirmed at any step below.

***Do not improvise.** Follow this checklist in order, log every action taken, and proceed to Phase 2 — Triage & Analysis on completion.*

1. **Acknowledge** the SNS notification email. Note the exact timestamp — this is your investigation window.
2. **Log in** to the [AWS CloudWatch Console](#).
3. **Navigate** to **Log Groups** → `veriquery-production`.
4. **Filter** log entries to the alarm timestamp ( $\pm 2$  minutes) using the CloudWatch time-range picker.
5. **Identify** the failing request(s):
  - Locate entries with `status >= 500`. Each log line is NDJSON — the `requestId` field correlates all lines for a single request.
  - Extract the `message` field and any stack trace present.
6. **Verify container health** on the VPS:

```
ssh magic@vps "docker ps"
```

Confirm the `veriquery` container is running and healthy. Note the restart count if it has cycled since the alarm fired.

7. **Record** the `requestId`, timestamp, error message, and container state in the incident channel before proceeding.
8. **Proceed to Phase 2 — Triage & Analysis** with the information gathered above.

---

## 4. Phase 2 — Triage & Analysis

---

The Engineering Lead determines the incident scope within the SEV classification above. Key questions:

1. Is the incident active (breach in progress) or historical (already occurred)?
2. What data was potentially accessed? Does it include PII?
3. What is the blast radius — how many accounts may be affected?
4. What is the attack vector?

The incident is assigned a severity level. SEV-1 escalates immediately; SEV-2 and SEV-3 follow standard business-hours response unless data exposure is confirmed.

---

## 5. Phase 3 — Containment

---

### Immediate Actions (SEV-1 / SEV-2)

- **Isolation:** Affected services or API endpoints are immediately restricted or suspended to prevent further unauthorised access.
- **Credential Rotation:** All API keys, database credentials, JWT secrets, and admin passwords are rotated immediately, regardless of whether they are confirmed as compromised.
- **Forensic Snapshot:** Before modifying affected systems, logs and relevant data are preserved to maintain chain of custody for investigation and potential legal proceedings.

### Evidence Preservation (A.5.28)

**Before remediating anything**, capture and preserve evidence. Remediation that overwrites logs or rotates credentials before evidence is secured may be irreversible.

1. **CloudWatch logs** — Export the relevant log stream(s) from the CloudWatch console to S3, or download via AWS CLI:

```
aws logs get-log-events \  
  --log-group-name veriquery-production \  
  --log-stream-name <stream-name> \  
  --output json > incident-<date>-cloudwatch.json
```

Record the SHA-256 hash of the exported file for chain-of-custody:

```
sha256sum incident-<date>-cloudwatch.json
```

2. **MongoDB Atlas audit logs** — If database compromise is suspected, export the Atlas audit log from the Atlas UI (Project → Activity Feed → Download) before any credential rotation touches the cluster.
3. **GitHub audit log** — If source code or credential exposure is suspected, capture the relevant entries from GitHub → Organisation → Audit Log before any access changes.
4. **Incident timeline** — Document every action taken with an exact timestamp in the incident channel. Do not rely on memory after the fact.

5. **Credential rotation sequencing** — Do **not** rotate credentials before evidence is captured unless an active attack makes immediate rotation necessary to stop ongoing harm. If emergency rotation is required first, document the reason explicitly in the timeline.
- 

## Temporary Mitigations

Rate-limiting, IP blocking, or feature flags may be applied to reduce attack surface while the root cause is being investigated.

---

## 6. Phase 4 — Eradication & Recovery

---

1. The root cause (vulnerable code path, leaked secret, misconfiguration) is identified and patched.
  2. If data integrity is in question, systems are restored from the most recent verified backup.
  3. Logs are reviewed to confirm no persistent backdoors, unauthorised admin accounts, or lingering attacker access remain.
  4. Affected services are restored to normal operation incrementally, with monitoring heightened for at least 48 hours post-recovery.
- 

## 7. Phase 5 — Notification (The "72-Hour Rule")

---

If the incident involves confirmed or reasonably suspected exposure of personal data:

### Customer Notification

All affected account holders will be notified by email within **72 hours** of confirming the breach. The notification will include:

- What happened (plain-language summary)
- What data was affected
- What we have done to contain it
- What affected users should do (e.g., change password)
- A contact address for questions

### Template — Customer Breach Notification Email:

**Subject:** *Important Security Notice — Your VeriQuery Account*

*Dear [Username],*

*We are writing to inform you of a security incident affecting VeriQuery that may have involved your account data.*

**What happened:** *[Brief description — e.g., "On [date], we detected unauthorised access to our database."]*

**What data was involved:** *[e.g., "Email addresses and hashed passwords. No payment information was exposed — payment data is processed exclusively by Stripe and never stored on our servers."]*

**What we have done:** *We have [contained the issue / rotated all credentials / patched the vulnerability] and taken steps to prevent recurrence. [If applicable: We have notified the relevant data protection authorities.]*

**What you should do:** *As a precaution, we recommend you [change your VeriQuery password / review your account for unexpected activity]. If you use the same password elsewhere, please change it there too.*

*We are deeply sorry for this incident. If you have any questions, please contact us at [security@magicapps.dev](mailto:security@magicapps.dev).*

*Sincerely, The VeriQuery Team*

## Public Status Notice

A notice is posted to the VeriQuery status channel within the same 72-hour window, using factual, non-speculative language.

## Regulatory Notification

If the breach meets the threshold for regulatory notification (EU personal data → GDPR supervisory authority; California residents → CCPA requirements), the Communications Lead and Legal Reviewer initiate the appropriate filing. Relevant agencies include CISA (US) and relevant EU Data Protection Authorities.

## 8. Phase 6 — Post-Mortem

Within 7 days of resolution, the Incident Commander leads a formal post-mortem review:

1. **Timeline reconstruction** — a full chronological log of events, detections, and actions.
2. **Root cause analysis** — the underlying technical or process failure.
3. **Impact assessment** — accounts affected, data exposed, service downtime.
4. **Action items** — specific technical controls to prevent recurrence, assigned with owners and due dates.
5. **Document update** — this IRP is reviewed and updated if any phase performed poorly.

Post-mortem documents are retained indefinitely as part of our audit log.

## 9. Plan Maintenance

This plan is reviewed and tested at least **annually**, or following any SEV-1 or SEV-2 incident. Tabletop exercises are conducted to validate the escalation chain and communication templates under simulated conditions.

Review Date	Version	Reviewer	Notes
April 19, 2026	1.0	Engineering Lead	Initial release
April 20, 2026	1.1	Engineering Lead	Added A.5.28 evidence preservation; added Appendix A authority contacts

## Appendix A — Regulatory Authority Contacts (A.5.5)

In the event of a confirmed breach, the Communications Lead initiates regulatory notifications within the applicable deadline. Use the contacts below. Verify URLs annually as part of the ISMS review.

Authority	Jurisdiction	When to contact	Contact
CISA (US-CERT)	United States	Significant cyber incidents	<a href="https://www.cisa.gov/report">https://www.cisa.gov/report</a>

		affecting US infrastructure or users	
<b>Irish Data Protection Commission</b>	EU / EEA (GDPR lead supervisory authority — Cloudflare EU DPA lead)	Confirmed breach involving EU/EEA personal data; notify within 72 hours (GDPR Art. 33)	<a href="https://www.dataprotection.ie/en/report-a-breach">https://www.dataprotection.ie/en/report-a-breach</a>
<b>California Attorney General</b>	California (CCPA)	Breach involving California residents' personal information	<a href="https://oag.ca.gov/privacy/databreach/reporting">https://oag.ca.gov/privacy/databreach/reporting</a>
<b>FTC (US)</b>	United States	Data security incidents affecting US consumers at scale	<a href="https://reportfraud.ftc.gov">https://reportfraud.ftc.gov</a>

**Note on GDPR lead authority:** As a SaaS product with no EU establishment, the lead supervisory authority is typically determined by the location of affected data subjects. The Irish DPC is listed above as Cloudflare's EU headquarters jurisdiction. Confirm the correct lead authority with legal counsel at the time of any actual notification.

**Annual review:** Verify all URLs and contact procedures are current as part of the annual ISMS review. Last verified: April 20, 2026.

## Attestation

I hereby certify that this Incident Response Plan represents VeriQuery's current procedures for detecting, responding to, and recovering from security incidents.

*Jacob Norr*

---

**Jacob Norr**

Founder & CEO, VeriQuery.com, MagicApps.dev

Date: April 19, 2026