Fraudfinder LTD
71-75 Shelton St
London
WC2H 9JQ
United Kingdom

Email: alexander@fraudfinderai.com

Business Continuity Plan 2025

Fraudfinder Ltd - Incident Management and Response Plan (IMRP)

Version: 1.0
Last Review: 1 February 2025
Approved by: CEO
Review Cycle: Annual

---

1. Purpose

This plan defines how Fraudfinder Ltd identifies, assesses, responds to, and communicates information-security and operational incidents. Its goals are to:

- Protect client and company data.
- Contain and remediate any incident rapidly.
- Communicate transparently with affected parties.
- Capture lessons learned and continuously improve controls.

---

2. Scope

Applies to all employees, contractors, and systems operated or managed by Fraudfinder Ltd, including:

- Core AI document-analysis platform (AWS London & Google Cloud).
- Development and collaboration tools (GitHub, Atlassian, Google Workspace, Slack).
- Any third-party integrations, such as Stripe.

---

3. Definitions

Term	Definition
Incident	Any event that compromises or could compromise the confidentiality, integrity, or availability of Fraudfinder's systems, data, or services.
Security Incident	Breach, malware, unauthorised access, data leakage, or system compromise.
Operational Incident	Outage, misconfiguration, or service disruption not caused by malicious activity.
Data Breach	Accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

---

4. Roles and Responsibilities

Role	Person	Responsibilities
Incident Lead	**Alexander Siedes (CEO)**	Owns incident coordination, decision-making, client communication, and regulatory reporting.
Technical Lead	**Andrew Kenyon (Head of Tech)**	Detect, analyse, contain, and remediate technical issues; maintain logs and evidence.
All Staff		Immediately report any suspected incident to the Incident Lead via Slack + email.

---

5. Incident Lifecycle

5.1 Detection & Reporting

- Any employee who suspects an incident must report it **immediately** to the Incident Lead and Dev Team.
- Incidents may originate from monitoring alerts, customer reports, or third-party notifications.
- All incidents are logged in the **Incident Register (Confluence → ISMS → Incident Log)**.

5.2 Classification

Severity	Example	Initial Response Target
Low	Temporary minor system bug; no data impact	Within 24 hours
Medium	Short outage or failed service affecting some users	Within 6 hours

High	Security breach or major outage; possible data exposure	Within 2 hours
Critical	Confirmed data breach or total service loss	Immediate (≤ 1 hour)

5.3 Containment

- Disable affected credentials or systems.
- Isolate compromised environments or servers.
- Suspend integrations if necessary to prevent propagation.

5.4 Eradication & Recovery

- Identify root cause and remove malicious code or misconfigurations.
- Restore from most recent verified backup (RPO 1 hour).
- Validate platform integrity before resuming services.

5.5 Communication

- **Internal:** All staff informed via Slack and email within 2 hours of classification as High or Critical.
- **Clients:** Affected clients notified within 24 hours with factual summary, mitigations, and next steps.
- **Regulators (ICO):** If personal data is involved, notify within 72 hours of becoming aware of the breach, per UK GDPR Art. 33.
- **Third Parties:** Notify vendors or partners if their systems or credentials are implicated.

5.6 Post-Incident Review

Within 7 days of closure:

- Conduct a debrief led by the CEO and Dev Team.
- Document timeline, impact, actions, and lessons learned.
- Identify preventive measures and assign owners.
- Update this plan, relevant policies, and technical controls.

---

6. Evidence & Record Keeping

- All actions, communications, and costs logged in the **Incident Register**.
- Preserve system logs, screenshots, and audit trails for at least 12 months.
- Store evidence securely in Confluence under restricted access.

---

7. Testing & Continuous Improvement

- Conduct an **annual tabletop simulation** covering a security and a service-outage scenario.
- Record results, lessons, and updates in Confluence.
- Review this plan during the annual ISMS Management Review or following any major incident.

---

8. External Contacts

Service	Contact	Purpose
AWS Support	support.aws.amazon.com	Cloud infrastructure assistance
Google Cloud Support	console.cloud.google.com/support	Data storage issues
Insurance Broker	M.Blake@sjlins.co.uk	Cyber liability claims
ICO (UK)	ico.org.uk / 0303 123 1113	Regulatory reporting

---

9. Related Documents

- Business Continuity Plan (v1.0)
- Information Security Policy
- Data Protection Policy (DPA Schedule)
- Supplier Risk Management Standard