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

Email: alexander@fraudfinderai.com

Business Continuity Plan 2025

Fraudfinder Ltd - Business Continuity Plan (BCP)

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

---

1. Aim of the Plan

This plan outlines how Fraudfinder Ltd will respond to and recover from any event that disrupts its business activities.

As Fraudfinder operates in a remote-first mode with all systems cloud-hosted, the focus is on ensuring the continuity of client services, access to systems, and data integrity following a cyber incident, system outage, or personnel loss.

---

2. Objectives

The objectives of this plan are to:

1. Provide a structured response to disruptive incidents.
2. Maintain availability of Fraudfinder's core SaaS platform and client services.
3. Ensure rapid recovery of systems and data following a disruption.
4. Protect client data, intellectual property, and business reputation.
5. Minimise operational and financial impact of incidents.

---

3. Scope

This plan applies to all employees and contractors of Fraudfinder Ltd, covering:

- Core platform and data hosted on **AWS (London)** and **Google Cloud**
- Collaboration tools (Google Workspace, Atlassian, Slack)
- Internal documentation and code repositories
- Client communication (email, LinkedIn)

There are **no physical premises or operational dependencies**; all staff work remotely using company-issued laptops.

---

4. Business Priorities and Critical Functions

Priority	Critical Function	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)	Owner
1	Platform availability and client access	12 hours	1 hour	CTO / Dev Team
2	Source code and data integrity	12 hours	1 hour	Dev Team
3	Communications with clients	24 hours	2 hours	CEO / Head of Growth
4	Business management and governance	48 hours	24 hours	CEO

---

5. Roles and Responsibilities

Role	Name	Responsibility
CEO	Alexander Siedes	Overall BCP ownership, client communications, and stakeholder management.
Head of Tech	Andrew Kenyon	Maintain system uptime, data recovery, and code repository restoration.
Head of Tech	Andrew Kenyon	Support platform restoration and system monitoring.
Head of Growth	Harry Foster	Manage customer updates and communications.

---

6. Incident Response and Recovery

6.1 Detection

- Any employee discovering an incident (system outage, security breach, data loss) must immediately report it to the CEO and Dev team via Slack and email.

6.2 Assessment

- The CEO and Dev team assess the impact:
    - **Minor:** Temporary disruption with no data loss
    - **Major:** Extended downtime or potential data compromise

6.3 Recovery Steps

1. Activate the incident response group (CEO + Dev team).
2. Identify affected systems or data.
3. Initiate data recovery using AWS or Google Cloud backups.
4. Restore platform functionality and validate integrity.
5. Notify affected clients within 24 hours if service impact is material.
6. Conduct post-incident review and update this plan.

---

7. Data Backup and Storage

- All systems are cloud-hosted on **AWS (London)** and **Google Cloud**, with automated daily backups.
- Backups are encrypted (AES-256) and monitored via automated alerts.
- Code repositories are stored in **GitHub**, replicated daily.
- Documentation is stored in **Google Drive**, version-controlled.

---

8. Alternate Working Arrangements

- All employees are remote and can work from any location with internet access.
- In the event of connectivity issues, employees may tether via mobile data or temporarily work from a co-working space.

- Company equipment (laptops) can be replaced within 24 hours via Amazon UK or Apple Business.

---

9. External Dependencies

Supplier	Service	Continuity / Backup
AWS (London)	Infrastructure hosting	Redundant cloud zones and daily backups
Google Cloud	Data storage	Multi-region redundancy
Google Workspace	Email, docs, calendar	Accessible from any device
Atlassian	Code and issue tracking	Cloud-based, replicated

---

10. Communication Plan

- **Internal:** Slack and Google Chat are primary; SMS for urgent escalations.
- **External (clients):** Email updates via Intercom or direct Gmail.
- **Regulatory/Partners:** Communication handled by CEO.
- All communications must be factual, coordinated, and approved by the CEO before release.

---

11. Testing and Review

- BCP to be tested **annually** or after any major incident.
- Test scenarios include:
    - Cloud system outage
    - Data recovery from backup
    - Simulated cyber breach communication flow
- Test results and improvements are recorded in **Confluence** under “ISMS – Business Continuity”.

---

12. Records and Documentation

All continuity records, including incident logs, tests, and corrective actions, are maintained securely in Confluence and reviewed during annual ISMS audits.

---

13. Contact List

Name	Role	Email
Alexander Siedes	CEO	alexander@fraudfinderai.com
Andrew Kenyon	Head of Tech	andrew@fraudfinderai.com