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

Email: support@fraudfinderai.com

Fraudfinder LTD - Information Security and Business Continuity Policy

Version: 1.8
Date: 22nd July 2025

This document details the Information Security Policy for Fraudfinder Ltd. (“Fraudfinder”) located at 71-75 Shelton Street, WC2H 9JQ, London, UK

Document Owner:	Alexander Siedes, CEO
Next Due for Review:	23rd January 2026
Document Classification:	Internal

Contents

Policy Objective

This is the Information Security Policy for Fraudfinder. The objectives of this Plan are as follows.

- To protect Fraudfinder's customers, staff, partners and business from harm relating to the loss of Confidentiality, Integrity or Availability of Fraudfinder systems.
- To set minimum standards of security controls to be applied in proportion to security risk.
- To define accountabilities for security processes.

Policy Governance

Roles and Responsibilities

Accountability for the implementation and enforcement of this policy rests with the Head of Engineering, who acts as the Information Security Officer.

Accountability for ensuring this policy meets all legal and regulatory requirements rests jointly with the CEO.

It is the responsibility of all employees to individually comply with all relevant aspects of this policy.

Policy Review & Approval

This policy shall be reviewed and re-approval obtained not less than annually, incorporating input from, at a minimum, the CEO, Head of Engineering and any other relevant stakeholders as required.

The Fraudfinder CEO is accountable for approval of changes to this policy.

Policy Exceptions

Exceptions to this policy may only be approved by the Information Security Officer. These must be logged, along with related mitigations, and reviewed by the CEO at least every three months for continued appropriateness.

Definitions & Policy Alignment

Incident

An unexpected event that impacts, or has the potential to impact, the confidentiality, integrity or availability of Fraudfinder services, or availability of Fraudfinder premises

Business Continuity Event

An Incident that has substantial impact on the availability of the Fraudfinder Production Services lasting more than one hour

Disaster Recovery Event
A significant Incident which results in one or more of the following:

- Incapacitation of staff
- Loss of access to physical offices
- Loss of the primary data centre hosting Production equipment

Information Classification
Information classifications exist to provide access controls to only the right individuals.

Business Continuity
A Business Continuity Plan has been defined to protect Fraudfinder's business objectives, business integrity, operational effectiveness and external obligations.

Risk Principles
The following risk management principles shall apply:

- Fraudfinder has zero appetite for material harm to either customers, partners, employees or the organisation from Information Security breaches
- Controls implemented shall be proportionate to the overall risk of harm to all stakeholders, including not just the risk of financials harm
- Fraudfinder aims to be in compliance with all regulatory expectations

Risk Management Policies

Risk Management Governance

Documentation Responsibility
The CEO is responsible for documenting and establishing control statements, procedures, organisational charts and controls for the respective area of accountability within Fraudfinder's governance framework and raising appropriate awareness.

Policy Management
Control statements, procedures, policies and controls shall be documented.

Vendor Management
When external services are procured for a task within an organisational unit, the CEO shall ensure that relevant controls are in place and regularly reviewed to safeguard Fraudfinder’s information and interests.

Contract Requirement
A legally binding contract signed by both a Fraudfinder representative and an authorised officer of the vendor shall be in place before any services are performed by a vendor.

Right to Audit

All contracts with vendors shall allow Fraudfinder the right to audit the completeness of service delivery and contractual obligations.

Compliance Management

Compliance Leadership

The CEO shall be responsible for managing compliance with Fraudfinder's legal and regulatory requirements. The CEO works closely with Fraudfinder’s external legal team, and compliance consultants, in order to carry out the compliance function effectively.

Compliance Responsibilities of Management

All managers shall be responsible for understanding legal and regulatory requirements relevant to their business and upholding business practices that align to these.

Compliance Register

The CEO shall maintain a register of all laws and regulatory requirements that Fraudfinder must comply with.

Compliance Controls

The CEO shall establish and monitor controls to ensure compliance with legal and regulatory requirements.

Compliance Strategies

The CEO shall provide advice and report directly to Fraudfinder's management on effective compliance strategies and obtain legal guidance from internal and external sources where needed.

Compliance Awareness

The CEO shall assess the need for training or awareness campaigns for legal or regulatory matters and manage execution appropriately.

Compliance Reporting

The CEO, along with relevant external help as needed, shall assess and report the current status of compliance to Fraudfinder's executives on a regular basis.

Compliance Reporting shall include at least

- Recent compliance incidents
- Status of compliance training
- Recent changes to laws or regulation
- Key compliance risks
- Complaints report, and
- Regulatory requests and issue mitigation status

Human Resources Management
Human resources management will be primarily the responsibility of the CEO, however appropriate delegation may be performed if required.

Required Background Checks
Human Resources shall ensure that sufficient background checks have been performed on new members of Fraudfinder. The depth of the background check shall be proportionate to the level of risk and responsibility related to an individual's roles & responsibilities within the organisation and include external agency checks where proportionate.

Joiners Confidentiality Agreement
The confidentiality agreement shall cover at least an agreement to abide by applicable privacy laws, an agreement preventing the disclosure of classified information outside of the organisation, and a documented understanding that the agreement remains in place indefinitely.

Technical Security Policies

Application Security
Applications includes core business applications, business tools (e.g. financial planning & development management tools), infrastructure components (e.g. middleware) and software products (e.g. MS Word)

Application Ownership
All applications shall have an assigned and recorded owner who is responsible for the operation of, changes to and the security of the Application, as well as underlying servers. This individual will have appropriate authority to approve changes.

Licencing & Support
Application owners shall ensure that applications they own are adequately licenced and that all commercially acquired software products are in-support

Application Administration
An application owner, or their delegate, shall be responsible for all administration tasks related to applications under their control.

Change Management
Each change to a production environment or network environment shall be supported by a documented business case.

Change Categories
Releases will be categorised into the following types of releases:

- Emergency Changes,

- Minor Releases,
- Major Release,
- Hotfix, and
- Go Live
- Infrastructure

Change Tracking

Traceability of all changes made to a production application shall be ensured throughout the lifecycle of each asset. The traceability will be recorded when a request for change is raised and logged in Github.

Deployment shall be approved and tracked using Rancher.

Environmental Segregation

Production environments shall be logically segregated from test and development environments using appropriate tools.

Production data shall not be used in test and development environments

Deployment

All deployment shall be reviewed and approved by the daily release manager.

Host/Endpoint Security

Patch Management

Application owners shall be responsible for ensuring that applications under their care are up to date with all relevant security patches, not less frequently than once a month.

All patches shall be subject to such tests in non-production environments as is proportionate to the risk presented by patching.

Patches shall be subject to the same Change Management process as ordinary changes, except where the patch fixes a Critical vulnerability on an externally visible system, in which case it shall be considered an emergency change.

Problem Management

Issue Management

Issues identified shall be logged on Cloudwatch, these shall be managed to resolution by the Application Owner

Incident Management

An incident is defined as an unplanned event leading to actual or potential impact on the Confidentiality, Integrity or Availability of services or data, whether through malicious actions or not.

Notification

Any employee identifying a potential incident shall immediately notify the Information Security Officer via any available means.

Roles & Responsibilities

Primary responsibility for coordinating resolution of an incident shall rest with the Information Security Officer. Should it not be possible to contact the Information Security Officer, the first available Board Member shall step into the role.

Should it not be practicable to contact a Board member in a reasonable time frame, it is the responsibility of all individuals to take necessary actions to resolve the incident.

The lead incident responder shall at all times consider whether the Incident meets the threshold for a Business Continuity or Disaster Recovery Event and execute the invocation process per the Business Continuity & Disaster Recovery Plan.

Logging

All incidents where the Confidentiality, Integrity or Availability of a system or data is compromised shall be appropriately logged utilising Sentry.

Cloudwatch shall be used on a periodic basis to analyse technical incidents. Mitigations identified from use of Cloudwatch shall be logged along with details of impact on Service Level Agreements

Post Incident Review

Logged incidents shall be reviewed by the CEO and Head of Technology within 14 days of the incident being closed, in order to identify lessons learned, including inputs appropriate to the nature of the incident.

Lessons learned shall be logged and tracked to completion.

Identity and Access Management

Identity and Access Management Leadership

The Application Owner shall be responsible for Identity and Access Management, under delegated authority from the Information Security Officer.

Least Privileged Principle

Users shall only have access required for executing their assigned tasks in line with the least privileged principle.

Unique Identities
Each person with access to Fraudfinder's IT assets shall have a permanently unique identity. The hiring manager shall be responsible for initiating the identity creation.

All accounts across all applications, whether related to business roles, communication/email suites or otherwise, shall be tied to the identity of an identifiable individual

Single Account per Identity
An identity shall only have one account per system or application associated to it.

Access for Movers
A user's move within the organisation or significant change within a user's responsibilities or position shall trigger a review of the user's assigned roles and entitlements. The user access review upon changing business positions shall be executed by the new manager.

Deprovisioning on Termination
The termination of a user's association with Fraudfinder shall result in immediate deprovisioning of all access linked to the user's identity. This activity shall be executed by the individual’s manager, with support from Application Owners

Authentication Requirements
Access to IT assets containing information classified as Confidential or Secret shall be granted only after the user has been identified and authenticated.

Authentication with Enterprise Credentials
Users shall authenticate against all Fraudfinder applications and services using their enterprise credentials.

Privileged Account Approval

All privileged access accounts shall be approved by the Application owner.

Elevated access to IT assets for administration, maintenance or configuration shall be defined as privileged accounts.

All actions undertaken by privileged accounts shall be logged and tied to an individual user.

Where it is not possible to tie a privileged account to an individual user for technical reasons (e.g. where only one account is technically possible), alternative mitigations must be identified, proportional to the risk of misuse

Business Roles
Entitlements to business applications and IT assets required to execute tasks specific to a profile within the organisation shall be defined as a business role.

Each person within Fraudfinder shall be assigned at least one role specific to assigned tasks within the organisation and these shall be centrally documented.

High Risk User Access Reviews

Access Control Lists for applications with access to Secret data or with a criticality rating of High or Critical shall be reviewed by the Application Owner at least every 3 months.

All other applications shall be reviewed at least annually.

Inactivity Management

User sessions shall time out after a fixed period of inactivity, except where such functionality is not supported.

Communication Technology

Email Service

Email and messaging communication on behalf of Fraudfinder shall use Fraudfinder's email service (currently Google G-Suite).

All users shall have 2-factor authentication enabled for access to any G-Suite functions.

Email Account Assignment

All email and messaging accounts linked to Fraudfinder's top level domain are either individual accounts, group accounts or technical accounts.

Group and Technical Accounts

Group Accounts may be set up for a group of people with a common functional need that this group requires to communicate on behalf of. Technical email accounts may be setup to allow non-human identities to send automatically generated messages.

Such accounts must be authorised by the CEO and access rights controlled as per application access.

Privacy Restriction

Privacy of messages sent through Fraudfinder's email or messaging services shall not be guaranteed, as it may be necessary to grant other employees access to the email account to ensure business continuity and fulfil contractual obligations.

Restrictions on privacy shall be outlined in employee agreements.

Password Management

Secure Password Storage

Passwords shall not be stored unprotected in physical or digital form. Passwords shall not be transmitted unencrypted.

The approved password management solution, Onepass, shall be used wherever technically feasible.

Physical Security

Security Pass

All members of Fraudfinder shall be issued with a keyless access pass that shall be required at all times to access non-public parts of the Fraudfinder office. This clause is currently not applicable to date as Fraudfinder is a remote only company as of January 2024.

Signing in Visitors

All visitors shall be formally signed in and out of all Fraudfinder facilities by an authorised member of the organisation. Visitors shall either be issued temporary passes to be returned before leaving the facility or must be accompanied by an authorised member of the organisation at all times. This clause is not applicable to date as Fraudfinder is currently a remote only company as of January 2024.

Entry and Exit Points

Entry and exit points have a receptionist and an individual access mechanism (e.g. fob enabled door access) combined with video surveillance. This clause is currently not applicable to date as Fraudfinder is a remote only company as of January 2024.

Data Centres

Fraudfinder utilises Amazon Web Services for data centre requirements.

All Fraudfinder servers hosted by Amazon Web Services shall be onshore in the European Economic Area.

Security Monitoring

Logging Information Security Events

Information security events relevant to availability, integrity and confidentiality of information shall be logged.

Automatic notifications shall be configured for indicators of key events.

Logged Items

All events must be timestamped.

Logging shall be sufficient to assign accountability for an event, establish traceability of actions and determine the effectiveness of security mechanisms

Blacklisting

Known illegal, dangerous or malicious content and nodes shall be blocked from Fraudfinder's network at a network level.

Cryptography

Security Objectives

Cryptographic measures shall be implemented to achieve the security objectives of confidentiality, authenticity, integrity and irrevocability of data. Measures deployed shall be proportionate to the risk related to the non-achievement of these objectives.

Cryptographic Measures

Cryptographic measures that must be considered shall include

- Asymmetric encryption,
- Digital signatures and certificates,
- Message authentication codes, and
- Time based one time passwords.

Cryptography Review

The Information Security Officer shall review approved cryptographic methods on a regular basis, not less than annually, and assess if the selected methods still provide sufficient protection and remain legal.

Cryptography Strength

The strength of the cryptographic method shall be proportionate to the information classification and the risk of usage through applications and devices.

The strength of a cryptographic method shall be determined by key length, known weaknesses, symmetrical versus asymmetrical encryption method, use of additional cryptographic measures for key exchange or handshake, split knowledge or dual control and implementation in hardware and / or software.

Encryption Requirements

All data representing information classified Secret or Confidential shall be protected by encryption in motion and at rest.

Key Generation

All cryptographic keys shall be randomly generated, independently from other cryptographic keys.

Key Storage
Cryptographic keys shall be securely stored to prevent unauthorised access.

Redundant Storage
Cryptographic keys shall be stored redundantly to protect from loss of keys thereby losing access to encrypted information.

Cryptography at Application Layer
Cryptography shall be applied at the database layer for application data where possible. Where this is not possible, alternative options, such as disk encryption, shall be deployed.

Key Changes and Revocation

The asset owner is responsible for revoking and changing compromised or expired cryptographic keys.

Infrastructure Management

Infrastructure Inventory

The Head of Technology shall maintain an inventory of all production IT Infrastructure elements including network diagrams as part of the IT asset inventory and shall ensure that all changes are reflected in a timely manner.

Capacity Management

Capacity monitoring shall be enabled for network components, hardware components and IT services by Amazon Web Services. Performance analyses shall be performed on a regular basis to identify capacity usage patterns and anticipate and distribute peak load.

Capacity planning shall be performed using input from IT strategy describing future developments, IT architecture describing the types of resources in demand, human resources to describe user bases and purchasing functions to describe available resources and capacity monitoring for actual usage.

Network Management

Documentation
Network architecture and configuration shall be documented and maintained as part of the Change Management Process.

Network Segmentation

Network segmentation shall be used to isolate production environments from non-production, as well as to isolate public-facing services from the internal network

Network Perimeters

All external connections and network segments shall be protected using firewalls and intrusion prevention technologies. These shall be configured in accordance with logging standards and the logs reviewed on a regular basis.

Document Control

Version	Date	Approved By	Changes
1.0	07/12/17	N/A	Initial draft for review
1.1	21/01/18	AS	Signed off
1.2	21/01/19	AS	
1.3	23/01/20	AS	Password management / Physical security
1.4	23/01/21	AS	
1.5	23/01/2022	AS	
1.6	23/01/2023	AS	
1.7	22/07/2024	AS	Office - remote work only
1.8	22/07/2025	AS	

Approvals

Approved by: Fraudfinder Limited

Policy Owner: Alexander Siedes, CEO