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

Email: alexander@fraudfinderai.com

Fraudfinder Data Loss Prevention Policy

1. Purpose and Commitment

This policy outlines the technical and procedural safeguards Fraudfinder uses to **prevent unauthorised disclosure, leakage, or destruction** of sensitive or client data, whether in transit, at rest, or in use. It applies to both structured and unstructured data across internal and production systems.

---

2. Scope

Covers all:

- Client-submitted documents (e.g., bank statements, payslips, utility bills)
- Personally Identifiable Information (PII) and sensitive financial data
- Model training datasets and AI model artefacts
- Credentials, logs, and audit trails
- Communications (email, Slack, file shares, etc.) containing sensitive data

---

3. Roles and Responsibilities

Role	Responsibilities
CTO / Engineering	Technical implementation of DLP tools and access controls
DPO / CEO	Policy enforcement and GDPR compliance oversight
Employees	Adhere to access controls, reporting duties, and acceptable use
DevOps / IT Admins	Enforce infrastructure-level DLP controls and monitor exfiltration attempts

---

4. DLP Strategy

1. **Data Classification**

   All data is tagged under three tiers:

   - **Confidential** – PII, client documents, model training data
   - **Internal** – Financials, internal metrics, test data
   - **Public** – Marketing, docs, job postings

   Rules are applied based on classification.

2. **Access Controls**

   - Principle of **least privilege** enforced on all internal and production systems
   - Role-based access (RBAC) via SSO (e.g., Google Workspace, AWS IAM, GitHub Teams)
   - Admin access is tightly restricted and requires MFA
   - Audit logs capture all access events to sensitive data

3. **Data in Transit**

   - All data transmitted over HTTPS with TLS 1.2+
   - Emails containing sensitive data are encrypted (S/MIME or TLS)
   - No document uploads via unsecured channels (e.g., WhatsApp, personal email)

4. **Data at Rest**

   - Client files and PII stored encrypted with AES-256
   - Secrets managed via AWS Secrets Manager or GCP Secret Manager
   - Backups encrypted, versioned, and monitored for tampering

5. **Endpoint Controls**

   - Company devices use full-disk encryption, password lock, and auto-timeout
   - USB/external storage is disabled unless approved by IT
   - Remote wipe enabled on all company laptops and phones

6. **Monitoring & Detection**

   - File transfer monitoring (e.g., large downloads, unsanctioned file sharing)

- Alerts on abnormal API behaviour or document access patterns
- Suspicious outbound traffic triggers alert to DevOps and Security lead

7. **Third-Party Services**
    - All third-party tools must pass a **vendor risk assessment**
    - Data transfer agreements (DTAs) and DPAs required for integrations
    - No sensitive data stored in unapproved tools (e.g., Notion, Trello)

---

5. Prohibited Activities

- Uploading client data to public cloud tools without written approval
- Sending sensitive files over personal email, WhatsApp, or Slack DM
- Using unapproved file-sharing tools (e.g., WeTransfer, Dropbox)
- Retaining client files locally after use (unless explicitly authorised)

---

6. Incident Response

Suspected data loss triggers the **Security Incident Response Plan**, which includes:

1. Immediate isolation of affected system/account
2. Forensics and log review within 24 hours
3. Notification to CEO/DPO and impacted parties (if required under GDPR)
4. Regulatory reporting (e.g., ICO) within statutory deadlines (72h for GDPR breaches)
5. Root cause analysis and post-mortem review

---

7. Enforcement

Violations of this policy — whether accidental or malicious — may result in:

- Revocation of system access
- Disciplinary action (up to dismissal)

- Legal action, if applicable

---

8. Review

This policy is reviewed **every 12 months** or after any data-related incident. Changes must be approved by the CEO and DPO.

Approved by:
Alexander Siedes, Chief Executive Officer

Effective Date: 06 July, 2025
Next Review Date: 05 January, 2026