Incident Response Plan
(Version 01)

1. Purpose

This Incident Response Plan (IRP) outlines the approach Simplified Loader follows to detect, manage, and respond to information security incidents. The objective is to minimize damage, reduce recovery time, and fulfil legal, regulatory, and client obligations.

2. Scope

This policy applies to all employees, contractors, and third parties who use or have access to Simplified Loader systems, services, or data.

3. Classification of Incidents

Security events are classified into the following categories to ensure appropriate and proportionate responses:

- Low Severity: Minor incidents with no data breach or service disruption.
- Medium Severity: Limited data exposure or temporary disruption.
- High Severity: Confirmed data breach, extended service disruption, or legal/regulatory impact.

Each classification determines the level of escalation, investigation, and reporting.

4. Roles and Responsibilities

- Incident Response Lead: The Founder (or delegated manager) is responsible for overall incident management and external communications.
- Technical Support: Investigates the root cause and mitigates technical risks.
- Compliance Coordinator: Reviews and reports on regulatory or legal considerations.
- Communications Officer: Coordinates internal and client communications.

5. Legal and Regulatory Considerations

All incidents are reviewed against applicable regulations, including:

- UK Data Protection Act 2018
- GDPR (if personal data is involved)
- Any contractual obligations with clients

Where required, relevant authorities (e.g. ICO) and affected clients will be notified within required timelines.

6. Incident Response Process

1. Detection: Identify and verify potential incident.
2. Classification: Assign severity level based on impact.
3. Containment: Limit exposure and secure systems.
4. Investigation: Root cause analysis.
5. Notification: Inform relevant stakeholders, clients, and authorities.
6. Remediation: Implement fixes and restore services.
7. Review: Conduct post-incident review and document lessons learned.

7. Communication During Disruption

If standard communication systems (e.g. email, support portal) are unavailable:

- Staff will use alternative methods such as mobile phones or pre-approved messaging platforms (e.g. WhatsApp for urgent coordination).
- External communication may be routed through third-party-hosted channels (e.g. our website or cloud collaboration tools).

8. Maintenance and Review

This Incident Response Plan is reviewed annually or following a major incident to ensure it remains effective and compliant with current risks and legal requirements.

Authorized signatory

Puneet Vishnoi (General Manager)

Simplified Loader

Signed on: 25-Jun-2025