Cybersecurity and Information Security Policy (Version 01)

1. Purpose

This policy outlines the cybersecurity and information protection measures taken by Simplified Loader to safeguard customer data, internal systems, and digital services. As a one-person company, Simplified Loader takes personal responsibility for upholding high standards of data security, privacy, and compliance.

2. Scope

This policy applies to all systems, software, data, and services managed by Simplified Loader, including any third-party services or infrastructure used to deliver products to clients.

3. Information Security Commitment

Simplified Loader is committed to:

- Confidentiality – Ensuring client and user data is accessed only by authorized systems or processes.
- Integrity – Protecting data from unauthorized modification or corruption.
- Availability – Ensuring systems and services remain functional and accessible to authorized users.

4. Roles and Responsibilities

As a sole operator, the founder of Simplified Loader assumes full responsibility for:

- Implementing and maintaining security controls.
- Managing user access and credentials.
- Monitoring systems and responding to any incidents.
- Keeping up to date with relevant data protection regulations and security best practices.

5. Access Control and Authentication

All accounts use strong, unique passwords and multi-factor authentication where available.

Access to development, production, and data systems is restricted to only the operator.

API keys, credentials, and sensitive configuration files are stored securely (e.g., in encrypted vaults or environment variables).

6. Data Security and Privacy

Customer and internal data are encrypted both in transit (via HTTPS/TLS 1.2+) and at rest (e.g., AES-256 encryption).

Regular offsite backups are taken and stored securely.

Simplified Loader complies with applicable data protection laws such as GDPR and the UK Data Protection Act 2018.

7. Device and Network Protection

All devices used to access Simplified Loader systems are secured with full disk encryption, anti-malware protection, and firewalls.

Software and operating systems are kept up to date with security patches.

Remote work is conducted over secure networks (e.g., trusted Wi-Fi or VPN).

8. Incident Response

In the event of a suspected data breach or security incident, the situation will be investigated immediately.

Affected clients will be notified promptly and within the timelines required by applicable laws.

Root causes will be identified and mitigated to prevent recurrence.

9. Third-Party Services

Third-party vendors (e.g., hosting, payment processors, or SaaS tools) are chosen based on their security reputation and compliance (e.g., ISO 27001, SOC 2).

Only trusted providers with appropriate data protection agreements are used.

10. Security Awareness and Practices

The founder remains personally responsible for staying informed about current security threats, technologies, and best practices.

Ongoing self-education and industry monitoring (e.g., OWASP, NCSC, relevant newsletters) are part of regular operations.

Authorized signatory

Puneet Vishnoi (General Manager)

Simplified Loader

Signed on: 25-Jun-2025