



INFORMATION SECURITY POLICY

Fin Con Outsourcing Pvt Ltd

Effective Date: 10-04-2026

1. Purpose

Fin Con Outsourcing Pvt Ltd is committed to ensuring the confidentiality, integrity, and availability of all information assets.

This policy establishes the framework for protecting client data, company information, and IT systems in line with industry best practices and applicable regulations including the UK GDPR and Data Protection Act 2018.

2. Scope

This policy applies to:

- All employees, contractors, and third parties
- All client data, including UK and international clients
- All IT systems, applications, and devices used by the Company

3. Information Security Principles

We follow these core principles:

- **Confidentiality** – Information is accessible only to authorised individuals
- **Integrity** – Data is accurate and protected from unauthorised modification
- **Availability** – Information is accessible when required for business purposes

4. Access Control

- Access to systems and data is granted on a **need-to-know basis**
- Unique user IDs and strong passwords are mandatory
- Access rights are reviewed regularly and revoked upon exit

5. Data Protection & Handling

- Client data is handled with strict confidentiality
- Sensitive data is shared only through secure channels
- Data processing is carried out in compliance with UK GDPR principles

6. Data Security Measures

We implement appropriate technical and organisational measures, including:

- Secure IT infrastructure and restricted access
- Anti-virus and system protection controls
- Data encryption where applicable
- Regular system monitoring

7. Remote Working Controls

- Work is performed only on authorised devices
- Secure internet connections are required
- Access to client systems is controlled and monitored
- Confidential data must not be stored on personal devices

8. Incident Management

Any suspected or actual data breach must be:

- Reported immediately to management
- Investigated promptly
- Resolved with corrective actions

Where required, clients will be notified without undue delay.

9. Third-Party Security

- Third-party service providers must adhere to data protection standards
- Confidentiality agreements are mandatory

- Access to data is limited and controlled

10. Data Retention & Disposal

- Data is retained only for as long as necessary
- Upon completion of services, data is securely returned or deleted
- Secure disposal methods are used to prevent data leakage

11. Employee Responsibilities

All employees are required to:

- Maintain confidentiality of client information
- Follow company security procedures
- Report any security risks or incidents
- Participate in security awareness training

12. Compliance & Review

This policy is reviewed periodically and updated as required to ensure ongoing compliance with applicable laws and industry standards.

Non-compliance with this policy may result in disciplinary action.

13. Management Commitment

Fin Con Outsourcing Pvt Ltd is committed to maintaining high standards of information security and continuously improving its security framework to protect client data and business operations.



Fin Con Outsourcing Private Limited

CIN: U70200BR2025PTC074969

G-7, Dukhanram Plaza, Exhibition Road, Kadamkuan, Hotel Republic, Phulwari,
Patna - 800001, Bihar

Email: info@fincono.com | Website: www.fincono.com | GST: 10AAGCF3396P1ZA