Barbourne Brook Ltd

CAT360 Information Security Policy

1. Overview

Barbourne Brook Ltd is committed to maintaining robust information security controls within CAT360, our proprietary FTA Reclaim Platform.

This policy outlines the governance framework, technical safeguards and operational controls in place to protect client data and ensure compliance with applicable UK regulatory requirements.

2. Governance & Accountability

- Information security oversight sits with senior management.
- Security responsibilities are clearly defined across technical and operational teams.
- Security controls are reviewed periodically and following material system or regulatory changes.

3. Regulatory Compliance

CAT360 operates in accordance with:

- UK GDPR.
- Data Protection Act 2018.
- Applicable contractual confidentiality obligations.
- Industry-standard information security practices.

Where required, data processing arrangements are governed by formal Data Processing Agreements.

4. Data Protection Controls

Client data processed within CAT360 is classified as confidential and subject to enhanced protection controls.

Controls include:

- Role-based access restrictions.
- Least privilege access principles.
- Controlled onboarding and offboarding procedures.
- Encryption of data in transit (TLS).
- Secure data storage environments.
- Controlled data retention and secure deletion processes.

5. Technical Security Safeguards

CAT360 is supported by a secure infrastructure incorporating:

- Network firewalls and perimeter protections.
- Endpoint protection and monitoring.
- Secure configuration standards.
- Regular patching and vulnerability management.
- Segregated development, test and production environments.
- Controlled change management procedures.
- Cyber Essential Plus certification.

6. Access Management

- Access is granted only to authorised individuals with a legitimate business requirement.
- MFA enforced.
- User permissions are role-based and reviewed periodically.
- Access is removed promptly upon termination or role change.
- Shared accounts are prohibited.

7. Incident Management

Barbourne Brook maintains a structured incident response approach:

- Immediate escalation of suspected security incidents.
- Investigation and containment procedures.
- Remediation and root cause analysis.
- Regulatory notification where legally required.

8. Business Continuity

To ensure service resilience:

- Regular data backups are maintained.
- Recovery procedures are documented and tested.
- Critical infrastructure is designed to support operational continuity.

9. Third-Party Risk Management

Where third-party service providers support CAT360 infrastructure:

- Due diligence is conducted prior to engagement.
- Security standards are contractually defined.
- Data protection obligations are formally documented.

10. Security Awareness

Authorised personnel receive appropriate training in:

- Data protection.
- Secure data handling.
- Cyber security awareness

11. Review

This policy is reviewed at least annually and updated where necessary to reflect changes in regulation, risk landscape or system architecture.

Last reviewed 10/02/2026