

CheckThis

Data Protection, Privacy & Shared Security Responsibility Charter

Issued by:	APOPS Assurance Ltd
Platform:	https://checkthis.top
Document classification:	Public
Version:	1.0
Effective date:	23 October 2026

1. Our Commitment

CheckThis is a business management Software-as-a-Service (SaaS) platform managed by APOPS Assurance Ltd, a company registered in Kenya.

We are committed to responsible information management, lawful data processing, confidentiality, integrity, availability and secure digital business operations.

We recognize that information security is not exclusively the responsibility of the technology provider. It is a shared responsibility involving CheckThis, subscribing organizations, authorized users and relevant infrastructure and service providers.

Our approach is guided by risk-based security principles, recognized cybersecurity frameworks and applicable data protection requirements.

2. Data Ownership and Control

Your business data belongs to you.

Customers retain ownership of the business information, documents, operational records and other content they lawfully upload, create or manage using CheckThis, subject to applicable rights of other individuals and organizations.

APOPS Assurance Ltd does not acquire ownership of customer business data merely because it is processed or stored through CheckThis.

Customer data is processed to provide, maintain, secure and support the subscribed services, or for other purposes permitted by applicable law and the relevant contractual terms.

We do not sell customer business data to advertisers or data brokers.

Where APOPS Assurance Ltd processes personal data on behalf of a subscribing business, the respective data-controller and data-processor responsibilities shall be determined by the actual processing activity and applicable law.

3. Legal and Regulatory Framework

Our data governance and privacy commitments are informed by:

- The Constitution of Kenya, 2010, particularly Article 31 on privacy.
- The Kenya Data Protection Act, 2019.
- The Data Protection (General) Regulations, 2021.

- The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.
- Other applicable Kenyan laws and contractual obligations.

We recognize the rights of data subjects, including applicable rights to information, access, correction, objection and deletion, subject to lawful retention obligations and statutory exceptions.

Customers using CheckThis are also responsible for complying with laws applicable to their own business activities and the personal data they collect.

4. Shared Responsibility Model

CheckThis adopts a Shared Security Responsibility Model in which each party has defined responsibilities.

APOPS Assurance Ltd - Platform Responsibilities

- Secure application development and maintenance.
- Platform-level authentication and authorization capabilities.
- Logical separation of subscribing organizations' data.
- Security patching and vulnerability management within our operational control.
- Protection of platform communications.
- Appropriate encryption and key-management controls.
- Backup, recovery and service-continuity planning.
- Logging, security monitoring and incident-response processes.
- Access restrictions for authorized platform administrators.
- Protection of customer information within our custody.

Subscribing Organizations - Customer Responsibilities

- Appoint and manage authorized users.
- Assign appropriate roles and permissions.
- Protect account credentials and authentication devices.
- Remove access promptly when employees leave.
- Ensure information uploaded is accurate, lawful and appropriately classified.
- Apply internal approval and segregation-of-duties controls.
- Secure computers, phones, local networks and exported documents.
- Report suspected unauthorized access or security incidents promptly.
- Train employees in responsible information handling.

Infrastructure and Third-Party Providers

Relevant hosting, communications and payment providers are responsible for security controls within their respective contractual and technical boundaries.

APOPS Assurance Ltd remains responsible for selecting and overseeing relevant service providers as required by applicable agreements and law.

5. Encryption and Information Protection

Our security architecture is guided by the principles of encryption in transit, encryption at rest, access restriction and secure cryptographic key management.

Our intended technical security baseline includes:

- TLS 1.2 or higher, with TLS 1.3 preferred, for protected network communications.
- Industry-recognized authenticated encryption such as AES-256-GCM for sensitive stored information where appropriate.
- Secure storage and controlled access to cryptographic keys.
- Strong password hashing using accepted password-specific algorithms.
- Restricted access to sensitive documents, financial records and personal information.
- Secure sessions, authorization checks and protection of application interfaces.
- Appropriate encryption or equivalent protective controls for sensitive backups.

Where customer-controlled or client-side encryption is offered, the relevant feature documentation must explain who holds the decryption keys and the associated recovery limitations.

Encryption does not replace proper access controls, auditability, secure configuration or responsible user behavior.

6. Cybersecurity Frameworks and Good Practices

The CheckThis security programme is guided by the following recognized frameworks and standards:

ISO/IEC 27001:2022

Information security management, governance and risk treatment.

ISO/IEC 27002:2022

Information security controls and implementation guidance.

NIST Cybersecurity Framework 2.0

Govern, Identify, Protect, Detect, Respond and Recover.

OWASP Application Security Verification Standard (ASVS)

Security requirements for web applications and APIs.

OWASP Top 10

Awareness and mitigation of critical web application security risks.

CIS Controls

Prioritized cybersecurity safeguards and operational security hygiene.

These frameworks inform the design, development and improvement of security controls. References to them do not constitute a claim of formal certification or independent compliance attestation.

7. Privacy by Design and Default

We seek to incorporate security and privacy considerations throughout the application lifecycle, including:

- Data minimization.
- Purpose limitation.
- Role-based and least-privilege access.
- Tenant isolation.
- Secure application development.
- Security testing.
- Appropriate retention policies.
- Controlled sharing and export of information.

- Secure deletion or anonymization where legally appropriate.

Each subscribing organization is responsible for setting appropriate internal user permissions and ensuring that its processing activities have a lawful basis.

8. Data Hosting, Retention and Recovery

Customer data is hosted and processed using infrastructure and service providers selected to support the CheckThis service.

The applicable service terms and privacy notices should identify relevant hosting locations, categories of subprocessors and international-transfer safeguards where required.

Records are retained according to applicable law, contractual obligations, operational requirements and configured retention policies.

Where a subscription expires or is terminated, customers should have access to the applicable data-export and retention arrangements described in their service agreement.

Backups, restoration procedures and recovery measures are maintained according to the capabilities and commitments of the subscribed service.

9. Security Incidents and Breach Management

APOPS Assurance Ltd maintains an incident-management approach intended to support:

- Detection and assessment of suspected security incidents.
- Containment and corrective action.
- Investigation and preservation of relevant evidence.
- Appropriate notification of affected parties.
- Reporting to relevant authorities where legally required.
- Recovery and continuous security improvement.

Customers must notify the platform administrator promptly when they suspect compromised credentials, unauthorized activity or data exposure.

10. Customer Rights and Transparency

Customers may request information concerning their account data, authorized access, available data-export options and applicable retention arrangements.

Personal data rights shall be handled in accordance with the Kenya Data Protection Act, 2019, and relevant legal requirements.

Where APOPS Assurance Ltd acts as a data processor, requests relating to personal information may need to be coordinated with the subscribing organization acting as data controller.

11. Confidentiality and Responsible Use

Customer information is treated as confidential and shall not be disclosed except where authorized, necessary to deliver contracted services, required by law or otherwise lawfully permitted.

Authorized users are responsible for handling downloaded reports, shared proposals, financial records and exported documents securely.

Each subscribing organization should establish appropriate internal policies covering confidentiality, acceptable

use, staff access and incident escalation.

12. Security Is a Continuous Responsibility

No technology platform can guarantee absolute immunity from cybersecurity incidents.

APOPS Assurance Ltd is committed to continuous risk assessment, security improvement and proportionate protective measures.

We encourage subscribing organizations to participate actively in maintaining a secure business environment through responsible account administration and timely reporting of security concerns.

13. Publication and Acceptance

This Charter shall be publicly accessible through CheckThis and the official APOPS Assurance document-download service.

A link to the Charter shall be provided during account registration and included in the new-customer welcome email.

Customers will be informed when material changes to this Charter occur.

14. Contact and Document Access

Platform:	https://checkthis.top
Managed by:	APOPS Assurance Ltd
Country of registration:	Kenya
General enquiries:	info@apopsassurance.com
Document repository:	https://downloads.apopsassurance.com

APOPS Assurance Ltd

Secure Business Operations. Shared Responsibility. Trusted Information Management.

© APOPS Assurance Ltd. All rights reserved.

Document fingerprint (SHA-256): 95b5cd83a1d2331b19150f99213d751c88edf2d33b99609fee015c1b96821450