cybooks

SECURITY PAPER

How Cybooks protects your company's books.

Your books deserve the infrastructure a bank would use. This paper shows what that means at Cybooks, in plain words, and what we don't offer yet.



October 2026
Last reviewed 15 Oct 2026
cybooks.com.cy

CONTENTS

In this paper

In short		3
1	How Cybooks is built	4
2	Keeping each company apart	6
3	Encryption	7
4	Backups and recovery	8
5	Sign-in and access	9
6	The audit trail	10
7	The Cybooks Brain	11
8	Monitoring and incidents	12
9	ISO/IEC 27001	13
10	What we don’t offer yet	14

For accountants, their IT reviewers and anyone who has to answer the question “is our financial data safe there?”. It describes how Cybooks works today. Amazon Web Services is the one provider we name.

IN SHORT

In short

Your books deserve the infrastructure a bank would use. That is the belief behind how Cybooks is built, and this paper shows what it means in practice.

Where	Amazon Web Services (AWS), Frankfurt (eu-central-1), in the EU
Your company's data	Its own database, not rows in a shared table; its own file folder; its own search index
Encryption	TLS 1.2 or 1.3 for every connection; database, backups and documents encrypted at rest; secrets such as bank connection credentials encrypted a second time
Recovery	The database can be restored within the available backup history, up to 35 days; earlier versions of documents kept for 90 days
Change history	Every change recorded with who, what and when, each entry stamped with a SHA-256 fingerprint, and the database refuses to edit or delete entries
Sign-in	Authenticator app or passkey, recovery codes; an admin can require two-factor for everyone; checked on every way in
The Cybooks Brain	Proposes, never moves money; Off, Watch, Suggest, Auto; Auto earned per company
Monitoring	Every administrative action in our AWS account recorded for a year; automated threat detection with alerts within minutes
Assurance	Preparing for ISO/IEC 27001: internal audit January 2027, certification audit February to March 2027. Not certified yet.

CHAPTER 1

How Cybooks is built

One professional platform, on AWS in Frankfurt

Cybooks runs on Amazon Web Services in the Frankfurt region (eu-central-1), inside the European Union. Your books, and the documents you upload, are stored there. As a Cyprus company, we work under the GDPR.

There is no server in an office, and no machine someone has to remember to upgrade. Every part of the platform is a managed AWS service:

- **The app** runs serverless on AWS Lambda. AWS starts as many copies of Cybooks as the moment needs and stops them when the work is done. The app runs in two separate AWS data centres (availability zones) in Frankfurt, behind a load balancer that spans both.
- **The database** is Amazon Aurora (MySQL-compatible), in its Serverless v2 form: its capacity grows and shrinks on its own.
- **Background work** such as bank imports, document reading, search indexing and the Brain's tasks runs on Amazon SQS queues, so your screen stays quick while heavy work happens behind it. Messages waiting in the queues are encrypted.
- **A memory cache** (Amazon ElastiCache) keeps frequently used data close to the app, kept apart for each company.
- **Documents** are stored in Amazon S3.
- **At the edge,** a web application firewall (AWS WAF) with AWS's managed rule sets stands in front of the app, and every connection is encrypted.

The journey of a request

When you open Cybooks:

1. Your browser connects over HTTPS with TLS 1.2 or 1.3. Plain http is turned away to https.
2. The web application firewall checks the request against AWS's managed rules for SQL injection, known bad inputs, addresses with a bad reputation, bots and account takeover attempts.
3. The app handles the request. Anything heavy is handed to a background queue.
4. The app reads and writes your company's own database, encrypted at rest.
5. Documents are fetched from your company's own folder through a short-lived signed link.
6. Behind the scenes, the database keeps a continuous backup.

Test and live are separate

Our test environment runs on its own database cluster, separate from the live one.

Built to grow, and measured

The database's capacity moves on its own between half a capacity unit and 128, a 256-fold range. Nobody has to press a button.

Measured on our live systems from 1 to 15 October 2026:

- The database rested at 0.5 units, averaged 2.1, and reached 27.5 at its busiest moment, with more than four times that still free.
- At the busiest moment, 362 copies of Cybooks were working side by side.
- More than 500,000 background tasks ran in those two weeks.

We don't publish a "maximum number of transactions": we haven't load-tested one, and we would rather show you what we measured.

CHAPTER 2

Keeping each company apart

Its own database. Every company in Cybooks gets a separate database, created for it when it signs up and deleted when the company is deleted. Your books are never rows in a table shared with other companies.

Its own files. Every company's documents live under its own folder in our document store. Files are served only through signed links that expire quickly, most within five to ten minutes.

Its own search index. In-app search keeps a separate index for each company, and a search can't run without a company selected.

Its own cache. Cached data is tagged and kept apart for each company.

What we don't do: per-company encryption keys or per-company database credentials. Isolation is by database, not by key.

Your data, from start to finish

Taking it with you. Export your reports, including the general ledger, whenever you want, and download any document.

When a company is deleted. Its database is deleted and its bank connections are revoked.

CHAPTER 3

Encryption

In transit. Every connection to the app uses TLS 1.2 or 1.3, under AWS's recommended TLS 1.3 policy for load balancers; plain http is redirected to https.

At rest. The database and its backups are encrypted with keys managed in AWS Key Management Service (KMS). Documents are encrypted with AES-256. The backup vault is encrypted.

A second layer for secrets. Inside the database, secrets are encrypted again by the application with AES-256: bank connection credentials, integration tokens, webhook secrets, mail passwords, identity-check data and two-factor secrets.

CHAPTER 4

Backups and recovery

Point-in-time recovery for up to 35 days. Aurora keeps a continuous backup of the database, so we can restore your books within the available backup history, up to 35 days. The production database is also protected against deletion.

Earlier versions of documents for 90 days. Our document store keeps every version. If a document is replaced or deleted by mistake, its earlier version stays for 90 days.

What we don't do: copy backups to a second AWS region.

CHAPTER 5

Sign-in and access

Two-factor sign-in. Cybooks supports an authenticator app with recovery codes, and passkeys.

A company-wide rule. An admin can require two-factor for everyone in the company, from today or within a week. Only people with the right to change company settings (Primary Admin and Admin by default) can set the rule, and they must use two-factor themselves to change it.

Checked on every way in. The second factor is checked whether you sign in with a password, a passkey, Google, a magic link or the customer portal, and when you switch to another company.

Session control. Each company chooses how long a sign-in lasts (8 hours, a day or a week) and when an idle session ends (30 minutes or an hour). Session cookies are secure and not readable by scripts.

Slowing down guessing. Wrong passwords and codes are limited to five tries a minute, and failed attempts are recorded in the company's audit trail.

Roles and permissions. Cybooks comes with roles for each job (Primary Admin, Admin, Accountant and View only), and you can create your own. Permissions are separate for every area of the books: view, create, edit, delete and, where it applies, approve.

Approvals. Bills, invoices, pay runs and expense claims can require approval before they go further, and so can a change to a supplier's bank details.

What we don't offer yet: single sign-on (SAML) for your company, and requiring two-factor for one specific person rather than the whole company.

Our own access

Our team. Every Cybooks staff account must use two-factor; the app enforces it.

Changes to Cybooks. Every change is reviewed before it ships, and nothing reaches production without passing our automated checks.

CHAPTER 6

The audit trail

Every change, recorded. Each company's audit trail records who did what, and when.

Fingerprinted. Each entry is stamped with a SHA-256 fingerprint of what happened, to what, when and by whom.

Refused for editing. The database itself refuses to edit or delete an audit entry, and the application refuses too.

What's in it. Changes to records; sign-ins and failed sign-in attempts; changes to roles and permissions; and every action of the Cybooks Brain, under its own name.

Where you see it. Each record's own history is available on every plan. The company-wide audit log and its export are part of Premium.

Filed means filed. Once a VAT return is filed, its period is locked. The database itself refuses to change or delete journal entries in a locked period, and a filed period can't be quietly reopened. A correction arrives as a new, visible adjustment, posted by someone with that specific permission, never as a quiet rewrite.

CHAPTER 7

The Cybooks Brain

The Cybooks Brain is the AI inside Cybooks: it reads bills, matches bank lines and prepares VAT. It is designed so that you stay in charge.

It never moves money. The Brain can't make a payment, and bank connections are read-only.

You set its autonomy. Each Brain helper is set to Off, Watch, Suggest or Auto.

Auto is earned. For bank matching, Auto opens only after at least 50 of your own decisions, and only when even a cautious statistical count says the Brain is right at least 9 times in 10 (the lower bound of a 95% Wilson interval must reach 90%), with no automatic booking undone. The first wrong automatic booking locks Auto again. Other helpers work within amount limits.

Checked like a person. Before anything is booked, our servers check the Brain's proposal with the same rules as a person's.

It learns from you. The Brain learns from corrections, and only a person's correction teaches it.

Tested. We test the Brain against examples checked by people, and every document it reads is treated as untrusted input, with tests for attempts to slip instructions into documents.

Recorded. Everything the Brain does appears in the audit trail under its own name.

The models. The Brain uses large language models from established AI providers, with our own instructions, tools, permission checks, limits and tests around them. We don't train or fine-tune our own model. When the Brain reads a document or answers a question, the parts it needs are sent to the provider for that task.

Read-only bank connections. Bank feeds come through a regulated open-banking provider. You give consent at your bank; Cybooks never sees your bank password, and the connection can read balances, account details and transactions only.

CHAPTER 8

Monitoring and incidents

Every administrative action recorded. AWS CloudTrail records every administrative action in our AWS account, in every region. Log file validation shows if a log file was altered, and the logs are kept for a year.

Automated threat detection. Amazon GuardDuty watches the account around the clock. Serious findings go straight to our security inbox; in our test, the alert arrived within a minute.

Errors and outages. CloudWatch alarms alert us to errors in the app.

How we build Cybooks securely

Reviewed changes. Every change is reviewed before it ships, and the production branch requires our automated checks to pass.

In-depth security reviews. We put our code through in-depth security reviews: our public API in September 2026, and the whole codebase in October 2026, with every finding checked by a second reviewer.

CHAPTER 9

ISO/IEC 27001

ISO/IEC 27001 is the international standard for running information security. We started preparing in September 2026:

- our scope, risks and controls are written down, with a Statement of Applicability covering the standard's controls;
- our policies are drafted, and the controls in this paper are part of that work;
- an internal audit is planned for January 2027;
- the certification audit (Stage 1 and Stage 2) is planned for February to March 2027, with an accredited certification body.

We are not certified yet. When we are, we'll publish the certificate here.

CHAPTER 10

What we don’t offer yet

We'd rather you hear it from us.

- **No ISO/IEC 27001 certificate yet,** and no SOC 2 report.
- **No independent penetration test yet**.
- **No single sign-on (SAML)** for your company.
- **No per-company encryption keys**: each company has its own database, under one well-managed key.
- **No live copy of the database in a second data centre:** recovery is from continuous backups.
- **No backup copy in a second AWS region**.
- **No one-click export of everything:** exports are by report and by document.
- **No uptime commitment (SLA)**.