Knowledgebase > Security / Privacy > How secure is Kahootz?

How secure is Kahootz?

Graham Smith - 2026-02-04 - Security / Privacy

Before you trust a cloud provider like Kahootz with your company or project data you want to be confident that it is going to be well looked after on many levels.

Security in transit

All communication between user devices and the Kahootz service is protected using HTTPS with Transport Layer Security (TLS).

TLS ensures that data is encrypted while in transit between the user’s browser and the Kahootz service, protecting it from interception or tampering. It also provides server authentication so users can be confident they are connecting to the genuine Kahootz service.

Kahootz uses modern, industry-standard TLS configurations and regularly reviews protocol and cipher support in line with current security best practice and guidance from the UK National Cyber Security Centre.

The same protections apply to all areas of the service, including login, file uploads and downloads, and API access.

Security on passwords

Each of the users in your site will have their own password. These are created by the users, not generated by Kahootz.
They're stored one-way encrypted, so they can't be read, only checked, and never emailed to people in plain text. (If you've forgotten your password, Kahootz can email you a reset link).

You can also opt for additional password security rules for your site based on length, required characters, number of changes, lockout on errors and so on.

Separation of customers

Although our systems run a large number of sites for a wide variety of clients, Kahootz offers client site separation as standard so your users are truly yours, and not accessing information from other Kahootz clients. Nobody else's workspaces will appear on your site just because some of your users are associated with other Kahootz clients too.

We also offer unique client addresses for every site as standard, meaning you can choose to allow access to your site, and your site alone, via your firewall.

Security at rest

Kahootz uses a variety of security lockdowns, perimeter tests and controls to stop attacks from affecting our servers. We also ensure that all parts of the software are fully security tested in design and deployment. As a government supplier working to high-security levels, we get regularly checked on this by CREST approved penetration tests that not only attempt many automated methods of cracking into the system, but also involve some dedicated cracking attempts by qualified individuals with up to date knowledge, skill, and competence of the latest vulnerabilities and techniques used by real attackers find any flaws we might have. We've been consistently marked as clean!

All customer data is encrypted at rest using strong, industry standard encryption, with access tightly controlled and logged.

All customer data is encrypted at rest using AWS Key Management Service (KMS)–managed AES-256 encryption across AWS services including Amazon S3, EFS and RDS. Encryption keys are securely managed and access is tightly controlled in line with the principle of least privilege.

People

In any evaluation of security, people should be considered as the weakest point; they make mistakes, and they can be compromised.
Every single staff member at Kahootz has been fully evaluated and vetted to BS7858 proving their identity and including full criminal records check.
We're a fully ISO27001-certified company, so all of our processes are checked and monitored by that standard. That's our own accreditation for our own development, release and internal processes, not just the accreditation of our data centre (although they are of course accredited too). Both of these standards apply to all our staff - those who can access your critical data, and those who can't - they even apply to our marketing team!

Only a limited number of authorised Kahootz staff have controlled access to production systems and customer data, and only where required to deliver the service or respond to support requests.
All their access is logged, and will only happen if need arises - usually based on a support ticket.

Resilience

Part of being a safe place for your data is not just the security but also the reliability of the service.
We use a scalable, cloud-based architecture deployed across multiple availability zones, designed to avoid single points of failure.

Kahootz is hosted on Amazon Web Services (AWS) within UK regions. AWS provides the underlying cloud infrastructure, including compute, storage, networking and physical data centre security.

AWS data centres are designed to meet high standards for physical and operational security and are independently certified to internationally recognised standards including ISO/IEC 27001, SOC 1/2/3 and PCI-DSS. Kahootz manages and secures the Kahootz application, data, access controls and configuration in line with our ISO 27001 certified information security management system.

Kahootz has long-term experience handling sensitive data for a variety of organisations, including the rigorous standards of the UK government's own tests and checks.
That's why we were one of the earliest organisations to pass the new Government wide accreditations (PGA), shortly after the likes of Microsoft, despite our distinctly smaller size.

CERTIFICATION INTERNATIONAL
ISO 27001
Cert No: CI/13258IS

UKAS
MANAGEMENT SYSTEMS
063

Crown Commercial Service Supplier

Related Content

- What is G-Cloud & Why Use it via Kahootz
- Who can view my Workspaces & How-To Change the Permissions
- Will you share my personal details with other people?
- Is my Kahootz data backed up?