CaptionHub

Security whitepaper

Version 2.9.9-rc1 9 September 2026

Overview

Your content is critically important. CaptionHub has been designed to be secure from its inception, and we do all we can to ensure that your data is only accessible by those you give access to.

This document outlines the steps we take to secure your data. Unless we specify otherwise, it relates to our cloud service on AWS. Please contact us with specific deployment requirements.

Risk and security management

LEADERSHIP COMMITMENT

CaptionHub's management team leads the organisation's commitment to a highly secure operating environment. A Security Working Group oversees information risk and security management, with clearly assigned roles: a Chief Information Security Officer responsible for security operations, a Chief Compliance Officer responsible for certifications and conformity, and board-level accountability for information risk held by our CEO as Senior Information Risk Owner. A systematic review of security performance runs through an internal and external audit programme and a system of continual improvement.

CERTIFICATIONS AND ATTESTATIONS

- **ISO/IEC 27001:2022** certified.
- **SOC 2 Type II** report (Security Trust Services Criteria), issued May 2026 — available under NDA.

RISK MANAGEMENT

Risk and security management occurs at every level of the organisation. Our approach includes a maintained risk register with defined ownership and acceptance, risk assessment of every significant technical or organisational change through a documented template, and an annual full review. Our Information Security Policy and supporting policies are reviewed at least annually and on significant change, with formal version control and approval evidence for every document.

Application security

CONTINUOUS ASSESSMENT

- Application vulnerability scanning — **Detectify** scans our systems every week using the latest attack vectors.
- Penetration testing and code review — at least annually, and after major architectural change.
- Container image scanning — every image is scanned before deployment (see Supply-chain security).
- Security control framework review — annually, through the ISO 27001 audit programme.

ENCRYPTION

- All traffic is encrypted in transit with **TLS 1.2 or higher**, using forward-secrecy cipher policies at our load balancers and CDN.
- All production data stores are encrypted at rest under **AWS KMS**: databases and caches with customer-managed keys set to rotate automatically each year, file systems with AWS-managed keys (also rotated annually by AWS); object storage under S3 server-side encryption (AES-256).
- Application secrets are held in **AWS Secrets Manager** customer secrets are stored encrypted (AES-256) in the CaptionHub database. User passwords are never stored by CaptionHub — they are held by **Auth0** as salted **bcrypt** hashes.
- Key lifecycle management is delegated to AWS KMS — keys are generated and held in hardware-backed key management, never handled manually.

AUTHENTICATION

We use **Auth0** to manage authentication, providing multi-factor authentication and password-strength management. For enterprise SSO we use **WorkOS** (SAML/OIDC against your identity provider). Custom integration with your own authentication scheme is available for on-premise customers.

Via Auth0, CaptionHub detects when a user's credentials appear in a third-party data breach, notifies the user, and prevents access until the password is reset. Internally, MFA is required on every system that supports it, credentials are generated and held in an end-to-end-encrypted password manager, and we follow NCSC guidance: strong unique credentials rather than arbitrary rotation, with immediate rotation on any suspicion of compromise.

PRODUCT SECURITY FEATURES

- By default a new user has no access — permission is explicit, per project.
- Full audit trail of user activity: logins (with IP), handover, download, assignment and more.
- Expiring URLs make it difficult to download linked media even when access has been granted.
- The logged-in user's email address can be superimposed over video, making screen captures traceable.
- Enterprise options: IP allow-listing, enforced two-factor authentication, SSO, watermarking of encoded media.
- All requests pass through a Web Application Firewall filtering known-malicious sources and attack patterns.

SECURE DEVELOPMENT

Rules for software and system development cover system design, development environments, secure testing and development principles. All code is peer reviewed before deployment through pull requests, with security analysis an explicit part of review. Code is automatically tested for security vulnerabilities with static analysis on every change, and dependency updates are managed continuously with prioritised security patches. Development, staging and production environments are separated in distinct AWS accounts.

SUPPLY-CHAIN SECURITY

All software reaches production through our peer-reviewed CI/CD pipeline. Container images are immutable, scanned with **Trivy** and **AWS Inspector** before deployment, and no additional software is installed at runtime. Our scanning toolchain itself is version-pinned to immutable releases. With every release we publish a **software bill of**

materials (SBOM) together with **OpenVEX statements** — where a reported CVE genuinely does not affect CaptionHub, the justification is published rather than silently suppressed.

Cloud-native security

CaptionHub deliberately does not deploy traditional EDR agents (CrowdStrike, Defender for Endpoint, SentinelOne and similar) on production infrastructure — our architecture removes the layer those agents exist to protect.

SERVERLESS CONTAINERS

Our workloads run as containers, the majority on **AWS Fargate** — a serverless container platform where the underlying hosts are provisioned, hardened, patched and isolated by AWS under the shared responsibility model. Containers run unprivileged. There is no server for us (or an attacker) to log into, and no host layer on which an EDR agent could be installed; AWS's controls at that layer are covered by their SOC 2 and ISO 27001 attestations.

HARDENED, DISPOSABLE IMAGES

For the minority of workloads that run on EC2, instances are built from images produced by an automated **EC2 Image Builder** pipeline that applies **DISA STIG and CIS Level 1 Server hardening** (Ubuntu Security Guide), generating before-and-after compliance audit reports on every build. Hosts are replaced rather than patched in place; obsolete images are automatically retired. There is no inbound SSH anywhere — administrative access is only possible through AWS Systems Manager under least-privilege IAM, and is logged.

RUNTIME THREAT DETECTION

Detection is cloud-native rather than agent-based: **Amazon GuardDuty** runs continuous threat detection across our AWS accounts, with **CloudTrail** and **CloudWatch** providing the audit and monitoring trail, and weekly external scanning by Detectify. The most sensitive logs are shipped to separate restricted accounts, so a compromised environment cannot erase its own trail.

ENDPOINTS, WHERE ENDPOINTS EXIST

All staff devices are company-managed and enrolled in MDM (**Iru**), with **Bitdefender GravityZone** endpoint protection, full-disk encryption, screen-lock and automatic OS updates enforced. Personal devices are not used for company work.

Personnel security

SCREENING

Every hire goes through employment-reference checks before joining and identity/right-to-work verification at onboarding. Enhanced checks (such as criminal-record checks) are applied for roles with elevated access. All staff complete a probation period.

TRAINING AND AGREEMENTS

All employees complete security-awareness training on joining and on an ongoing basis, including simulated phishing. Contracts contain dedicated information-security and non-disclosure obligations, and core security policies must be read and acknowledged before access to any information system is granted.

ACCESS CONTROL AND LEAVERS

We operate least privilege: employees receive only the access their role requires, access to production and customer data is restricted to a small set of engineering roles, and front-line support staff have no customer-data access unless a customer explicitly grants it. Access is reviewed quarterly. When someone leaves, access to every system is revoked on or before their last day through a documented checklist, with evidence captured for each system.

Data protection

WHERE YOUR DATA LIVES

Customer data is hosted in the EU: our primary region is AWS eu-west-1 (Ireland), with a disaster-recovery environment in eu-central-1 (Frankfurt). Object storage is redundantly stored across multiple availability zones with eleven-nines durability.

INTERNATIONAL TRANSFERS

Where data transfers outside the UK/EEA are required, we rely on EU Standard Contractual Clauses with the UK Addendum, or the UK International Data Transfer Agreement, as appropriate, alongside a UK GDPR-aligned data-protection programme (documented data-subject-rights procedure; regulator notification within 72 hours where required).

THIRD PARTIES AND AI SERVICES

Depending on how you configure CaptionHub, you may choose to share data with third parties — automatic transcription and machine translation are examples. Your data is shared only following an explicit action from you. We maintain a published sub-processor list, hold data-processing agreements with every processor, and record for each AI provider whether customer content is used for model training — with contractual opt-outs in place. Suppliers are risk-assessed on onboarding and verified annually.

CLASSIFICATION AND DISPOSAL

Information is classified against a four-level scheme covering both customer and internal information, and handled accordingly. Disposal is formal: managed remote wipe for devices, secure erasure for logical data, certified destruction for physical media.

Continuity

HIGH AVAILABILITY

CaptionHub runs in a high-availability pattern with no single point of failure: multi-availability-zone databases with automatic failover, and infrastructure-as-code to scale services seamlessly.

BACKUPS

Databases have continuous point-in-time recovery over a 35-day window, with daily backup copies replicated to a **segregated AWS account** with tightly restricted access — so backups survive even the compromise of the production account. Video media is stored on S3 (eleven-nines durability) and is not separately backed up; caption and work data is fully restorable from database backups.

DISASTER RECOVERY — TESTED

We maintain a disaster-recovery environment in a second EU region (Frankfurt) and rehearse using it: our most recent full exercise simulated the loss of every availability zone in our primary region and restored service — environment rebuild, database restore and DNS switchover — in around 70 minutes.

Recovery objectives are tiered by scenario:

Scenario	Recovery time (RTO)	Data loss (RPO)
Availability-zone failure	Minutes (automatic failover)	Near zero
Data loss or corruption	Hours (point-in-time restore)	≤ 5 minutes
Full regional failure	8 hours committed (4 hours typical)	24 hours worst case

INCIDENT RESPONSE

CaptionHub operates a documented incident-response process run through a dedicated incident-management platform, with defined severity levels, an on-call escalation path, a public status page, and customer notification commitments in line with our data-processing agreements. Automated alerting (GuardDuty, application monitoring, uptime checks) routes to the team continuously; incidents conclude with a documented post-incident review.

Infrastructure hosting

CaptionHub hosts applications and data with Amazon Web Services. Physical and environmental security of data centres — access control, surveillance, redundant power and cooling, fire suppression — is provided by AWS and covered by their SOC, ISO and PCI attestations; see the AWS compliance programme for details. Our own responsibilities under the shared responsibility model — everything from the operating system and network configuration upwards — are described throughout this document.

Timbra (live captioning)

- When adding subtitles to public live video, captions are served via a publicly visible URL containing a unique, hard-to-guess identifier, which can be rotated on request. For video-platform integrations the URL is constructed from the platform's public video ID.
- Timbra can be evaluated in private mode, with no data publicly available.
- Projects can be configured to allow only authorised access: all public endpoints are disabled and caption output is available only via the API with valid credentials.
- All transcription and caption data is kept within the CaptionHub system; customers can opt to use a private install of our transcription engine. Captions are no longer available for deleted projects.
- Low-latency input supports SRT (built-in AES encryption) or RTMP secured with an unguessable stream key.

FAQ

Can I install my own instance of CaptionHub behind my firewall? Yes. For our Enterprise customers, CaptionHub can be deployed in a variety of ways. Please contact us for details.

Does my data exist alongside other users'? It depends on your installation. For multi-tenant customers it does — CaptionHub is extensively tested to ensure users cannot see each other's data. If you require absolute separation, we recommend our single-tenant or on-premise options.

Who can see my information? Access to data is limited to a small set of CaptionHub engineering roles under least privilege, with quarterly access reviews. Where third-party developers are engaged, they are bound by the same contractual confidentiality and follow the same code-review pipeline.

Can you produce an audit trail of who accessed what? Yes. Users must be explicitly granted access per project; we track login times and IP addresses and log activity such as handover, download and assignment.

What about incident response and data breaches? We run a documented incident-response process on a dedicated incident-management platform with continuous automated monitoring and alerting, formal breach-notification procedures (including 72-hour regulator notification where required), and post-incident reviews.

How do you handle supplier and third-party security? Every supplier is recorded in our supplier register with a criticality and data-access rating, risk-assessed on onboarding, and verified annually — including review of their SOC 2/ISO attestations for critical vendors. Contracts include security and data-protection clauses.

Notices

This document is provided for informational purposes only. It represents CaptionHub's current product offerings and practices as of the date of issue, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of CaptionHub's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from CaptionHub, its affiliates, suppliers or licensors. The responsibilities and liabilities of CaptionHub to its customers are controlled by CaptionHub agreements, and this document is not part of, nor does it modify, any agreement between CaptionHub and its customers.

This document is generated from version-controlled source; its version and date are stamped from the release under which it was published.