Security Policy

This Security Policy describes AhaPlay's technical, organisational, and operational security measures, certifications, and security commitments. It forms part of the AhaPlay legal and operational framework and should be read together with the AhaPlay Terms of Service, the applicable Quote or Order Form, the applicable Data Processing Agreement (DPA) where applicable, the Privacy Policy, the Acceptable Use Policy, the IP Policy, and other applicable AhaPlay policies. Capitalised terms used in this Security Policy, unless otherwise defined herein, shall have the meanings assigned to them in the AhaPlay Terms of Service.

Specific technical practices, providers, configurations, and operational measures described in this Security Policy may evolve over time as AhaPlay updates its security programme. AhaPlay shall maintain protections substantially equivalent to or better than those described herein. The most current Security Policy is published at ahaplay.com/security.

Security Contact: security@ahaplay.com

Privacy Contact: privacy@ahaplay.com

1. Certification and Compliance

AhaPlay maintains ISO/IEC 27001:2022 certification (certificate number ISMS/262177/BG, issued by CSB Ltd., valid from 19 January 2026 to 18 January 2029) covering the Information Security Management System for the AhaPlay platform. AhaPlay's ISMS has been independently audited and certified by CSB Ltd. covering all aspects of platform development, operations, and data handling. A current certificate is available on request to security@ahaplay.com.

AhaPlay operates in compliance with the EU GDPR (Regulation 2016/679), the UK GDPR and Data Protection Act 2018, and the Privacy and Electronic Communications Regulations (PECR). AhaPlay maintains EU data residency for customer data at rest, with all primary processing in AWS eu-central-1 (Frankfurt). AhaPlay's sub-processors (Section 9) maintain their own SOC 2 Type II, ISO 27001, or equivalent certifications, with copies available on request to enterprise Customer Organisations under applicable confidentiality undertakings.

2. Data Processing Agreements

AhaPlay provides GDPR-compliant Data Processing Agreements (DPAs) to enterprise Customer Organisations. The AhaPlay DPA covers the scope and purpose of personal data processing; the sub-processor list and the 30-day advance notification procedure for material sub-processor changes (Section 9, and Section 10.6 of the Terms of Service); the technical and organisational security measures (TOMs) described in this Security Policy; data breach

notification obligations under Articles 33 and 34 GDPR (including the 72-hour regulatory notification commitment); data deletion and return procedures upon termination; and Customer Organisation audit rights, including the right to receive applicable certifications, audit summaries, and security questionnaire responses on reasonable request.

3. Infrastructure Security

AhaPlay is built on AWS infrastructure with all customer data at rest stored in AWS eu-central-1 (Frankfurt, Germany). The primary infrastructure components include AWS ECS Fargate for application compute, AWS RDS (PostgreSQL) for relational database storage, AWS S3 for file storage, AWS CloudFront for global content delivery (with edge caching limited to static assets only and no personal data cached at the edge), AWS Route 53 for DNS, AWS CloudWatch for monitoring and logging, AWS KMS for cryptographic key management, AWS Secrets Manager for production secrets and API credentials, and self-hosted KeyDB on AWS for in-memory caching. All AWS services used are within the eu-central-1 region for primary processing, with cross-region replication to a secondary EU region for disaster recovery purposes.

Production, staging, and development environments are fully isolated with separate AWS accounts or VPC boundaries, separate database credentials per environment, and environment-specific deployment pipelines. Production secrets are managed exclusively via AWS Secrets Manager and are never stored in source code repositories. Deployment pipelines enforce environment-specific configurations and prevent cross-environment secret leakage.

4. Encryption

In transit: all external connections enforce TLS 1.2 minimum with TLS 1.3 preferred (HTTPS only, HSTS enabled). Certificate management is automated via AWS Certificate Manager (ACM). API-to-database connections are encrypted via TLS. Internal service-to-service communication within the AWS VPC uses encrypted channels.

At rest: all database storage is encrypted using AES-256 via AWS RDS encryption with AWS KMS-managed keys. File storage in AWS S3 uses server-side encryption (SSE) with AWS KMS-managed keys. Backup volumes are encrypted with AES-256 using separate AWS KMS keys from production data. User passwords are hashed using BCrypt (cost factor 10 or higher) and are never stored in plain text.

Key management: all encryption keys are managed via AWS KMS with automated key rotation per AWS schedules. API secrets, third-party tokens, and operational credentials are stored in AWS Secrets Manager with access restricted by IAM policy. Encryption keys for backup data are kept separate from production-data keys.

5. Network Security

The Platform is protected by a Web Application Firewall via AWS WAF configured with OWASP rule sets. DDoS protection is provided by AWS Shield Standard (included with AWS services) augmented by AWS WAF rate-limiting rules. Rate limiting is enforced on all API endpoints both per-user and per-endpoint. IP allowlisting is available for enterprise Customer Organisations on request. The production database (AWS RDS) is not publicly accessible and is reachable only from within the AWS VPC private subnets. Internal administrative access to AWS infrastructure requires a self-hosted WireGuard VPN on EC2 with cryptographic key authentication and access restricted to authorised AhaPlay personnel. Real-time traffic anomaly detection and alerting is provided via AWS CloudWatch with automated alert routing to the on-call security team.

6. Backups and Disaster Recovery

AhaPlay performs daily automated backups via AWS RDS automated snapshots with point-in-time recovery enabled. Backup retention is 30 days rolling. All backups are encrypted with AES-256 using AWS KMS keys separate from production-data keys. Backup data is replicated cross-availability-zone within the eu-central-1 region for high availability, with cross-region replication to a secondary EU region for disaster recovery. Recovery Time Objective (RTO) is under 4 hours; Recovery Point Objective (RPO) is under 1 hour. AhaPlay conducts annual disaster recovery drills, with results documented and incorporated into the ISMS continuous improvement cycle.

7. Application Security

Authentication and access control: the Platform supports email and password authentication with BCrypt password hashing, magic-link (passwordless) authentication, and SAML 2.0 single sign-on for enterprise Customer Organisations. Multi-factor authentication (MFA) is required for administrative access and is available for all User Accounts. Role-based access control (RBAC) is enforced at both application and database layers, with roles including Platform Administrator, Workspace Administrator, Facilitator, Programme Member, and Participant. Session tokens use JSON Web Tokens (JWT) with configurable expiry and immediate revocability. Administrative impersonation of User Accounts is logged in immutable audit trails, with notification to the affected Workspace Administrator where reasonably practicable, in accordance with Section 5.3 of the Privacy Policy and Section 10.9 of the Terms of Service.

Secure development: all code changes require peer code review through the pull request model. Automated dependency vulnerability scanning runs continuously via Dependabot and `npm audit` equivalents. Static code analysis is integrated into the CI/CD pipeline. OWASP Top 10 mitigation is a baseline requirement for all production code. AhaPlay conducts annual third-party penetration testing, with summary reports available to enterprise Customer Organisations on request under confidentiality. AhaPlay operates a responsible disclosure programme for security researchers (see Section 12).

API security: Row-Level Security (RLS) is enforced at the database layer to ensure tenant isolation between Workspaces. Input validation and sanitisation is applied at all API endpoints. CORS policies restrict cross-origin requests. Per-user and per-endpoint rate limiting prevents abuse. Request logging and anomaly detection routes alerts to the security team via AWS CloudWatch.

8. AI Security

AhaPlay does not use Customer Content in identifiable form to train, fine-tune, optimise, or develop artificial intelligence models or machine learning systems, irrespective of whether such systems are intended for internal or external use, without the express prior consent of the applicable Customer Organisation. AhaPlay maintains contractual safeguards with its AI sub-processors under which Customer Content submitted via API is not used by those sub-processors to train their general-purpose AI models, except where expressly authorised by the applicable Customer Organisation or End User.

AI providers: OpenAI is used for AI Programme generation, AI-assisted chat, and AI-assisted support, under OpenAI's Enterprise API agreement with zero retention at OpenAI and contractual prohibition on training. Anthropic is used for AI Programme generation, AI-assisted chat, and AI-assisted support, under Anthropic's Enterprise API agreement with zero retention at Anthropic and contractual prohibition on training. LangSmith (LangChain) is used for AI execution tracing and quality monitoring, with prompts and responses retained for up to 90 days in anonymised form (no User Account identifiers or email addresses are sent to LangSmith), and with no use of submitted data for model training.

AI data handling: AhaPlay retains AI conversation data for 7 days after the conversation ends, after which it is auto-deleted (Privacy Policy Section 3.7). Uploaded documents (such as PDFs) are processed in memory by the AI provider and AhaPlay-side copies are deleted after 7 days. No User Account identifiers, email addresses, or account credentials are sent to AI providers — only the content the user types into AI-assisted features (goals, team context, uploaded documents, organisation name) is processed by AI providers. AI outputs are reviewed and filtered before display in the Platform. Prompt injection mitigation controls are in place and continuously updated.

9. Sub-Processors

AhaPlay engages the following sub-processors to deliver the Platform. All sub-processors are bound by Data Processing Agreements (DPAs) complying with Article 28 GDPR: Amazon Web Services (AWS) for cloud infrastructure including compute (ECS Fargate), database (RDS PostgreSQL), storage (S3), CDN (CloudFront), DNS (Route 53), monitoring (CloudWatch), key management (KMS), and secrets management (Secrets Manager), located in EU eu-central-1 (Frankfurt) with intra-EU processing and no transfer mechanism required; SendGrid (Twilio) for transactional email delivery, located in the US under Twilio DPA with Standard Contractual

Clauses (SCCs); Sentry for error monitoring and crash reporting, located in the US under SCCs; LangSmith (LangChain) for AI execution tracing and quality monitoring (anonymised), located in the US under SCCs; OpenAI for AI language model processing, located in the US under OpenAI DPA with SCCs and zero retention; Anthropic for AI language model processing, located in the US under Anthropic DPA with SCCs and zero retention; Jitsi / 8×8 (JaaS) for video conferencing infrastructure, located in US/Cloud under SCCs; Hotjar (Contentsquare) for heatmap and session replay analytics (platform-only, consent-gated), located in EU (Malta) with intra-EU processing; Synthesia for AI video generation, located in the UK under the UK Adequacy Decision; Tavily for web search for AI features, located in the US under SCCs; and Google Cloud / Google Workspace for Google Calendar integration and Pub/Sub, located in EU/US under Google DPA with SCCs.

Customer Organisations are notified at least 30 days before any material change to the sub-processor list, in accordance with Section 10.6 of the Terms of Service, with publication on the Platform, the Security Policy, the DPA, or a dedicated sub-processor page at ahaplay.com/sub-processors. Customer Organisations may object to a new or substituted sub-processor on reasonable grounds within the notice period, in which case the parties shall cooperate in good faith to identify a mutually acceptable solution.

10. Data Protection and Retention

AhaPlay supports all data subject rights under GDPR Articles 15–22 in accordance with the AhaPlay Privacy Policy. Data subject requests can be exercised via privacy@ahaplay.com or through in-platform account privacy settings.

The complete and authoritative retention schedule is set out in Section 7 of the Privacy Policy. Key retention periods include: User Account profile data — duration of active User Account plus 2 years after closure for dispute resolution; Session activity data — 3 years from Session date, then anonymised or deleted; AI conversation data — 7 days from conversation end (automatic deletion); AI Programme results — 1 year from creation; AI execution traces (LangSmith) — 90 days maximum; audit logs (Platform activity) — 1 year, then anonymised; application logs (CloudWatch) — 90 days; error reports (Sentry) — 90 days; access logs (ALB and CloudFront) — 90 days lifecycle policy; email delivery records (SendGrid) — 90 days; support communications — duration of active User Account plus 2 years after closure; and backups — 90 days after deletion from production, encrypted and geographically separated within the EU.

Right to deletion: Workspace Administrators can delete User Accounts and Session data at any time through Platform administrative functionality. For full Workspace deletion, Customer Organisations should contact security@ahaplay.com. Production data is removed within 30 days of a deletion request; backup data is removed within 90 days through encrypted overwrite and lifecycle policy. AhaPlay applies commercially reasonable technical and organisational measures to reduce the likelihood of re-identification of anonymised or aggregated data.

11. Operational Security

Incident response: AhaPlay maintains a documented Incident Response Plan aligned with ISO/IEC 27001 and incorporated into the ISMS. Incidents are classified by severity (Critical, High, Medium, Low) with corresponding response procedures and escalation paths; target initial response times for Customer-reported incidents are set out in Section 2.4 of the Service Level Agreement (SLA). For confirmed personal data breaches likely to result in a risk to the rights and freedoms of individuals, AhaPlay notifies the competent supervisory authority within 72 hours of becoming aware of the breach (GDPR Article 33), and notifies affected Customer Organisations and individuals where required (Article 34). Each incident triggers a post-incident review and root cause analysis (RCA), with lessons learned integrated into the ISMS continuous improvement cycle.

Monitoring and logging: AhaPlay operates 24/7 uptime monitoring with automated alerting via AWS CloudWatch; application performance monitoring (APM) covering response times, error rates, and resource utilisation; security event logging with SIEM-ready log export; immutable audit trails for administrative actions including User Account impersonation; and anomaly detection on authentication events and API usage patterns. Audit trails of AhaPlay personnel access to Customer Workspaces are maintained and may be made available to the applicable Customer Organisation on reasonable request, in accordance with Section 10.9 of the Terms of Service.

Business continuity: AhaPlay maintains a documented Business Continuity Plan (BCP) covering critical Platform functions, with multi-region failover capability across AWS regions in the European Union. The BCP is reviewed annually and tested through annual disaster recovery drills. AhaPlay commits to 99.9% monthly availability for paid subscriptions, with detailed uptime measurement methodology, incident response time targets, service credit mechanics, and exclusions set out in the applicable Service Level Agreement (SLA).

People security: AhaPlay conducts background checks for employees with access to production systems or customer data, subject to applicable Bulgarian and EU employment law. All staff complete security awareness training at onboarding and annually thereafter. The principle of least privilege is enforced across all systems, with access granted on a need-to-know basis. Access reviews are conducted quarterly. All team members and contractors are bound by confidentiality agreements covering customer data, security information, and AhaPlay's intellectual property.

12. Responsible Disclosure

AhaPlay welcomes security research conducted in good faith. If you discover a security vulnerability in the Platform, please report it to security@ahaplay.com. AhaPlay commits to acknowledging vulnerability reports within 24 hours and providing a resolution timeline within 5 business days. AhaPlay will not pursue legal action against security researchers who act in

good faith, comply with applicable law, do not exfiltrate or destroy data beyond what is reasonably necessary to demonstrate the vulnerability, and provide AhaPlay a reasonable opportunity to remediate before public disclosure.

13. Enterprise Documentation and Audit

Upon reasonable request and subject to applicable confidentiality undertakings, AhaPlay makes available to enterprise Customer Organisations a current ISO/IEC 27001 certificate, applicable surveillance audit summaries, a security overview document describing technical and organisational measures, and responses to standardised security questionnaires (such as SIG, CAIQ, or equivalent). AhaPlay is not obligated to permit on-site audits by Customer Organisations, but may accommodate reasonable security questionnaires and documentation requests consistent with industry standards.

14. Contact

For security questions, vulnerability reports, or compliance documentation requests, contact the AhaPlay security team at security@ahaplay.com (incident reports, vulnerability disclosures, compliance queries). For data subject requests, DPA inquiries, and GDPR questions, contact privacy@ahaplay.com. For postal correspondence, AhaPlay Bulgaria VCC, Attn: Security Team, 5 Rozova Dolina Street, Floor 4, Lozenets District, Sofia 1421, Bulgaria.