STUDYTUBE

SECURITY WHITE PAPER

Why information security matters at Studytube

October 2025

Table of contents

Introduction 3

Part 1 - Technical Security Controls 4

Authentication & Passwords 4
Web Security 5
Application Security 5
Malware Protection 6
Protection of Servers & Infrastructure 6

Part 2 - Operational Security & Data Management 7

Security during Development 7
Vulnerability Management 7
Logging & Monitoring 8
Data Management & Governance 8
Disaster Recovery & Backup 9

Part 3 - Oversight, Response & Compliance 10

Organization & Management 10
Security Audits, Penetration Tests, & Automated Tests 10
Incident Response 11
Compliance 11

Introduction

At Studytube we believe that humans should never stop improving – and the same applies to how we protect your data. Information security is a cornerstone of our platform and services, built on trust, transparency, and continuous improvement.

We are proud to be certified against ISO 27001 and independently audited for SOC 2 Type II compliance, demonstrating that our security practices meet internationally recognized standards. These frameworks, combined with GDPR compliance, guide how we manage risks, safeguard data, and fulfill our contractual and regulatory obligations.

This whitepaper provides an overview of the organizational and technical measures Studytube has implemented to protect your data and ensure the highest standards of confidentiality, integrity, and availability.

Part 1 - Technical Security Controls

Authentication & Passwords

Studytube uses modern standards and layered protections to ensure secure authentication, both for its customer-facing platform (controls that protect end-users) and for internal employee access (controls that protect Studytube's own systems and infrastructure).

Platform

- **API & SSO authentication** – OAuth 2.0 for API authentication and SAML 2.0 or OpenID Connect for Single Sign-On
- **Password standards** – Studytube adheres to the most recent password best practices outlined by the National Institute of Standards and Technology (NIST)
- **Password hashing** – Strong password security with salted BCrypt hashing
- **Reset & verification flows** – Secure, token-based flows for password resets and account verification
- **Brute-force protection** – Brute-force protection through automated lockout and application-level defenses (e.g. rate limiting)
- **Multi-factor authentication (MFA)** – MFA support available within the platform

Studytube Internal

- **Password security & MFA** – Access to critical systems requires strong passwords and MFA
- **Authorization management** – A formal access matrix defines roles and permissions. Administrative access is role-based, time-bound, and reviews are performed quarterly
- **Access restrictions** – Production consoles are limited to DevOps, integrations, and engineering managers; database access is restricted to machine users and database architects
- **Offboarding controls** – Access rights are revoked within one week of termination
- **Device policies** – All endpoints (laptops, workstations) must have screen lock (15 min), full-disk encryption, up-to-date OS versions, and malware protection

Web Security

Studytube protects all connections and online services with modern, industry-standard security controls:

- **Secure connections** – All traffic is encrypted in transit with TLS, and customer data is encrypted at rest with AES-256 and managed via AWS Key Management Service (KMS)
- **Firewalls and network controls** – AWS Security Groups and Network ACLs enforce strict access rules, ensuring only authorized traffic reaches our systems
- **Email security** – Outgoing email is encrypted and protected against spoofing through SPF, DKIM, and DMARC, handled by an ISO 27001-certified provider

Application Security

Studytube applies a fine-grained, role- and entitlement-aware authorization model. Access to platform data is always based on defined roles and permissions, ensuring users can only view or act on information relevant to their responsibilities. This covers key areas such as user data, learning content, and budget management, all protected by strict approval and governance rules.

Malware Protection

Studytube protects its platform and customers against malicious files with proactive malware scanning:

- **File scanning** – Automatic scanning of all user-uploaded files, with immediate blocking of unsafe content
- **Threat updates** – Continuously updated detection to stay protected against the latest threats
- **Environment coverage** – Active protection across environments, ensuring safeguards in both production and test systems

Protection of Servers & Infrastructure

Studytube ensures robust protection of its infrastructure through strict access controls and layered defenses:

- **Environment segregation & access** – Production and test environments are isolated, with access restricted to a limited group of engineers under multi-factor authentication and least privilege principles
- **Server security** – Firewalls, centralized configuration, version control, and timely patching ensure consistent and secure system management
- **DDoS protection** – Layered safeguards including AWS Shield, Web Application Firewall (WAF), rate limiting, and load balancing protect against malicious traffic and ensure service continuity
- **Physical security** – Studytube is hosted in AWS's Frankfurt datacenters, certified to ISO 27001 and SOC 2 Type II, with strict physical security and 24/7 monitoring

Part 2 - Operational Security & Data Management

Our security model is built on the principles of confidentiality, integrity, and availability (CIA), ensuring data protection, trust, and service continuity.

Security during Development

Studytube embeds security throughout its software development lifecycle (SDLC):

- **Environment segregation** – Production data is never used in test environments
- **Testing & QA** – Every code change is subject to automated and manual testing before release
- **Secure coding & reviews** – Developers are trained in application security, follow OWASP Top 10 guidance, and all code is peer-reviewed
- **Automated controls** – Continuous vulnerability scanning and dependency monitoring ensure protection against known threats

Vulnerability Management

Studytube follows a structured and auditable vulnerability management process, with clear ownership and accountability at management level. This ensures that risks are identified, prioritized, and resolved in line with industry standards:

- **Identification** – Vulnerabilities are detected through automated scanning, static/dynamic testing, and annual independent penetration tests
- **Prioritization** – Issues are classified by severity and business impact, with resolution timelines aligned to risk
- **Remediation** – Critical services are patched promptly, and exceptions are formally documented with mitigating controls
- **Review & compliance** – Vulnerability management is reviewed regularly to ensure effectiveness and compliance with ISO 27001 and SOC 2 Type II

Logging & Monitoring

Studytube ensures full visibility and traceability across its platform and infrastructure:

- **Application & audit logging** – All user and system activities are logged in centralized, write-protected audit trails, with sensitive data excluded and strict access controls applied
- **Backend & infrastructure logging** – Security-relevant events are continuously captured and protected against tampering, supporting compliance and operational integrity
- **Monitoring & alerting** – 24/7 monitoring with automated alerts enables rapid detection of suspicious activity or service disruptions. Alerts are routed in real time to on-call engineers for rapid triage and resolution
- **Compliance support** – Logging and monitoring practices meet ISO 27001 and SOC 2 Type II requirements, ensuring transparency and trust

Data Management & Governance

Studytube applies strict policies to safeguard customer data and ensure compliance with ISO 27001, SOC 2 Type II, and GDPR:

- **Classification & access control** – Data is classified (Public, Confidential, Sensitive/PII) with access restricted by role and continuously monitored. No customer data is publicly accessible
- **Storage & sovereignty** – All customer data is stored in AWS datacenters in Germany, ensuring compliance with EU and local residency requirements. Sub-processors operate exclusively within the EEA
- **Encryption & protection** – Sensitive data is always encrypted, monitored for anomalies, and logged for compliance
- **Retention & lifecycle** – Data is retained only as long as necessary, and upon contract termination all customer data is securely deleted or returned, with written confirmation available
- **Segregation & audits** – Customer data is logically segregated within the platform, and regular audits validate compliance with access and retention policies

Disaster Recovery & Backup

Studytube ensures resilience and business continuity through a robust backup and recovery strategy:

- **High availability** – Target uptime of 99.8%, excluding planned maintenance
- **Secure backups** – All critical data is backed up multiple times per day, encrypted in transit and at rest, and access is strictly controlled.
- **Recovery objectives** – Strict recovery time and data loss objectives ensure rapid restoration in the event of disruption (RTO=4h, RPO=24h)
- **Testing & validation** – Backups and recovery procedures are regularly tested to guarantee effectiveness
- **Business continuity** – A documented BC/DR policy guides preparedness, response, and communication in case of major incidents

Part 3 - Oversight, Response & Compliance

Organization & Management

Studytube maintains strong governance to ensure information security is embedded across the company:

- **Audits & risk management** – Regular risk assessments and annual internal and external audits under ISO 27001 and SOC 2 Type II confirm the effectiveness of our controls
- **People & awareness** – All employees are screened, trained in information security, and bound by confidentiality agreements before gaining access to customer data. Developers require proven security expertise before working in production environments
- **Operational safeguards** – Clean desk and clear screen policies, encrypted devices, automatic screen locks, and strong password policies with MFA protect sensitive data
- **Governance** – All security and compliance policies have identified owners and are reviewed regularly to align with evolving threats and regulatory requirements

Security Audits, Penetration Tests, & Automated Tests

Studytube's security is continuously validated through a mix of internal and external testing:

- **Penetration testing** – Independent penetration tests are conducted annually by specialized security firms
- **Automated security testing** – Continuous automated testing ensures SSL configurations, access controls, and application security remain at industry best-practice levels
- **Code verification** – Comprehensive test suites verify all code changes before release, safeguarding platform integrity

Incident Response

Studytube maintains a documented Incident Management & Response Policy to ensure security incidents are handled swiftly, transparently, and in compliance with ISO 27001, GDPR, and DORA.

- **Detection & monitoring** – Incidents are detected within minutes using advanced monitoring and alerting systems, supported by proactive testing and customer reporting channels
- **Response process** – A dedicated Incident Response Team coordinates containment, remediation, and recovery to minimize impact and restore services quickly
- **Data breach handling** – Personal data breaches are managed in line with GDPR requirements, with prompt customer notification if Studytube acts as Processor
- **Continuous improvement** – All incidents are logged, reviewed, and analyzed through post-incident reviews, feeding into ongoing risk management and strengthening defenses

Compliance

Studytube operates under a comprehensive Information Security Management System (ISMS) certified against ISO 27001. We are fully GDPR-compliant, with Data Processing Agreements in place for all sub-processors, and independently audited for SOC 2 Type II compliance.

External certifications and audits confirm that Studytube's controls are effective and consistently applied. Known issues are managed as part of standard hygiene, with continuous scanning, annual penetration tests, and employee awareness training steadily reducing residual risk over time.

We actively prepare for and comply with relevant EU regulations, including:

- NIS2
- DORA
- EU AI Act
- Digital Services
- Data Acts

In the Netherlands, Studytube aligns with governmental open standards to ensure interoperability, transparency, and data sovereignty for public sector customers. Studytube's AI features are developed following privacy-by-design and GDPR principles, with human oversight and readiness for the EU AI Act.

STUDYTUBE

Designed with your future in mind.

www.studytube.nl
Danzigerkade 17,
1013 AP Amsterdam

info@studytube.nl
Service: 020 - 779 69 94
Office: 020 - 233 02 17