STUDYTUBE

SECURITY WHITE PAPER

Warum Informationssicherheit bei Studytube wichtig ist

Oktober 2025

Inhaltsverzeichnis

Einleitung

Bei Studytube sind wir der Überzeugung, dass Menschen niemals aufhören sollten, sich weiterzuentwickeln – und das gilt ebenso für den Schutz Ihrer Daten. Informationssicherheit ist ein Grundpfeiler unserer Plattform und unserer Services, basierend auf Vertrauen, Transparenz und kontinuierlicher Verbesserung.

Wir sind stolz darauf, nach ISO 27001 zertifiziert zu sein und uns zudem jährlich einer unabhängigen SOC 2 Type II-Prüfung zu unterziehen. Diese Nachweise bestätigen, dass unsere Sicherheitspraktiken internationalen Standards entsprechen. Zusammen mit der DSGVO-Konformität bilden diese Rahmenwerke die Grundlage für unser Risikomanagement, den Schutz Ihrer Daten sowie die Erfüllung vertraglicher und regulatorischer Anforderungen.

Dieses Whitepaper gibt einen Überblick über die organisatorischen und technischen Maßnahmen, die Studytube implementiert hat, um Ihre Daten zu schützen und die höchsten Standards in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten.

Teil 1 - Technische Sicherheits-kontrollen

Authentifizierung & Passwörter

Studytube setzt moderne Standards und mehrschichtige Schutzmechanismen ein, um eine sichere Authentifizierung zu gewährleisten – sowohl für die kundenorientierte Plattform (Schutzmaßnahmen für Endnutzer) als auch für den internen Mitarbeiterzugang (Schutzmaßnahmen für Studytubes eigene Systeme und Infrastruktur).

Plattform

- **API- & SSO-Authentifizierung** – OAuth 2.0 für die API-Authentifizierung sowie SAML 2.0 oder OpenID Connect für Single Sign-On
- **Passwortrichtlinien** – Einhaltung der aktuellen Passwort-Empfehlungen des National Institute of Standards and Technology (NIST)
- **Passworthashing** – Starke Passwortsicherheit durch gesalzene BCrypt-Hashes
- **Reset- & Verifizierungsprozesse** – Sichere, tokenbasierte Abläufe für Passwortzurücksetzungen und Kontoverifizierung
- **Brute-Force-Schutz** – Schutz vor Brute-Force-Angriffen durch automatisches Sperren und anwendungsseitige Abwehrmechanismen (z. B. Rate Limiting)
- **Multi-Faktor-Authentifizierung (MFA)** – Unterstützung von MFA innerhalb der Plattform

Studytube Intern

- **Passwortsicherheit & MFA** – Zugriff auf kritische Systeme erfordert starke Passwörter und MFA
- **Autorisierungsmanagement** – Eine formale Zugriffsmatrix definiert Rollen und Berechtigungen. Administrativer Zugriff ist rollenbasiert, zeitlich begrenzt und wird vierteljährlich überprüft
- **Zugriffsbeschränkungen** – Die Produktion Konsole ist nur für DevOps, das Integrationsteam und Engineering-Manager zugänglich; der Datenbankzugriff ist auf Machine-User und Datenbankarchitekten beschränkt
- **Offboarding-Kontrollen** – Zugriffsrechte werden innerhalb einer Woche nach Ausscheiden entzogen
- **Geräte Sicherheitsrichtlinien** – Alle Endgeräte (Laptops, Arbeitsplätze) müssen mit einer Bildschirmsperre (15 Minuten), Festplattenverschlüsselung, aktuellen Betriebssystemversionen und Malware-Schutz ausgestattet sein

Web-Sicherheit

Studytube schützt alle Verbindungen und Online-Dienste mit modernen, branchenüblichen Sicherheitsmaßnahmen:

- **Sichere Verbindungen** – Sämtlicher Datenverkehr wird während der Übertragung per TLS verschlüsselt, Kundendaten sind im Ruhezustand mit AES-256 gesichert und werden über den AWS Key Management Service (KMS) verwaltet
- **Firewalls und Netzwerkkontrollen** – AWS Security Groups und Network ACLs erzwingen strikte Zugriffsregeln und stellen sicher, dass nur autorisierter Datenverkehr unsere Systeme erreicht
- **E-Mail-Sicherheit** – Ausgehende E-Mails werden verschlüsselt und durch SPF, DKIM und DMARC vor Spoofing geschützt. Der Versand erfolgt über einen ISO 27001-zertifizierten Anbieter

Applikationssicherheit

Studytube setzt ein fein abgestuftes, rollen- und berechtigungsbasiertes Autorisierungsmodell ein. Der Zugriff auf Plattformdaten erfolgt stets auf Grundlage definierter Rollen und Berechtigungen, sodass Nutzer nur die Informationen einsehen oder bearbeiten können, die für ihre Aufgaben relevant sind. Dies umfasst zentrale

Bereiche wie Nutzerdaten, Lerninhalte und Budgetverwaltung, die alle durch strikte Genehmigungs- und Governance-Regeln geschützt sind.

Malware-Schutz

Studytube schützt seine Plattform und Kunden proaktiv vor schädlichen Dateien durch umfassende Malware-Scans:

- **Dateiscans** – Automatische Überprüfung aller von Nutzern hochgeladenen Dateien mit sofortiger Sperrung unsicherer Inhalte
- **Bedrohungs-Updates** – Kontinuierlich aktualisierte Signaturen zur Abwehr neuester Bedrohungen
- **Umgebungsabdeckung** – Aktiver Schutz in allen Umgebungen, wodurch Sicherheitsmaßnahmen sowohl in Produktions- als auch Testsystemen gewährleistet sind

Schutz der Server & Infrastruktur

Studytube gewährleistet einen robusten Schutz seiner Infrastruktur durch strenge Zugriffskontrollen und mehrschichtige Sicherheitsmechanismen:

- **Umgebungssegmentierung & Zugriff** – Produktions- und Testumgebungen sind strikt voneinander getrennt. Der Zugriff ist auf eine begrenzte Gruppe von Ingenieuren beschränkt und erfordert Multi-Faktor-Authentifizierung sowie das Prinzip der minimalen Rechtevergabe
- **Serversicherheit** – Firewalls, zentralisierte Konfigurationsverwaltung, Versionskontrolle und zeitnahe Patches sorgen für eine konsistente und sichere Systemverwaltung
- **DDoS-Schutz** – Mehrstufige Abwehrmaßnahmen wie AWS Shield, Web Application Firewall (WAF), Rate Limiting und Load Balancing schützen vor bösartigem Datenverkehr und gewährleisten Servicekontinuität
- **Physische Sicherheit** – Studytube wird in den AWS-Rechenzentren in Frankfurt gehostet, die nach ISO 27001 und SOC 2 Type II zertifiziert sind und strenge physische Sicherheitsmaßnahmen sowie eine 24/7-Überwachung implementieren

Teil 2 - Operative Sicherheit & Datenmanagement

Unser Sicherheitsmodell basiert auf den Prinzipien Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability, CIA) – und stellt so den Schutz von Daten, Vertrauen und Servicekontinuität sicher.

Sicherheit während der Entwicklung

Studytube integriert Sicherheit in den gesamten Softwareentwicklungszyklus (SDLC):

- **Umgebungssegmentierung** – Produktionsdaten werden niemals in Testumgebungen verwendet
- **Tests & Qualitätssicherung** – Jeder Code-Change wird vor der Freigabe sowohl automatisierten als auch manuellen Tests unterzogen
- **Sicheres Programmieren & Reviews** – Entwickler sind in Anwendungssicherheit geschult, folgen den Richtlinien der OWASP Top 10, und jeder Code wird von Kollegen überprüft
- **Automatisierte Kontrollen** – Kontinuierliche Schwachstellenscans und Abhängigkeitsüberwachung sorgen für Schutz vor bekannten Bedrohungen

Schwachstellenmanagement

Studytube verfolgt einen strukturierten und nachvollziehbaren Prozess für das Schwachstellenmanagement, mit klarer Verantwortung auf Management-Ebene. So wird sichergestellt, dass Risiken identifiziert, priorisiert und nach Branchenstandards behoben werden:

- **Identifizierung** – Schwachstellen werden durch automatisierte Scans, statische/dynamische Tests und jährliche unabhängige Penetrationstests erkannt
- **Priorisierung** – Funde werden nach Schweregrad und Geschäftsauswirkung eingestuft; Behebungsfristen richten sich nach dem Risiko
- **Behebung** – Kritische Dienste werden umgehend gepatcht; Ausnahmen müssen formal dokumentiert und mit kompensierenden Kontrollen abgesichert werden
- **Review & Compliance** – Das Schwachstellenmanagement wird regelmäßig überprüft, um Wirksamkeit sowie die Einhaltung von ISO 27001 und SOC 2 Type II sicherzustellen

Logging & Monitoring

Studytube gewährleistet vollständige Transparenz und Nachvollziehbarkeit über seine Plattform und Infrastruktur:

- **Anwendungs- & Audit-Logging** – Alle Benutzer- und Systemaktivitäten werden in zentralisierten, schreibgeschützten Audit-Trails protokolliert. Sensible Daten sind ausgeschlossen, der Zugriff streng kontrolliert
- **Backend- & Infrastruktur-Logging** – Sicherheitsrelevante Ereignisse werden kontinuierlich erfasst, gegen Manipulation geschützt und unterstützen Compliance sowie die Betriebssicherheit
- **Monitoring & Alarmierung** – 24/7-Überwachung mit automatisierten Warnmeldungen ermöglicht die schnelle Erkennung verdächtiger Aktivitäten oder Serviceunterbrechungen. Alarme werden in Echtzeit an Bereitschaftsingenieure weitergeleitet, um eine sofortige Analyse und Reaktion sicherzustellen
- **Compliance-Unterstützung** – Logging- und Monitoring-Praktiken erfüllen die Anforderungen von ISO 27001 und SOC 2 Type II und gewährleisten damit Transparenz und Vertrauen

Datenmanagement & Governance

Studytube wendet strenge Richtlinien an, um Kundendaten zu schützen und die Einhaltung von ISO 27001, SOC 2 Type II und der DSGVO sicherzustellen:

- **Klassifizierung & Zugriffskontrolle** – Daten werden nach Sensitivität eingestuft (Öffentlich, Vertraulich, Sensitiv/PII). Der Zugriff ist rollenbasiert und wird kontinuierlich überwacht. Kundendaten sind niemals öffentlich zugänglich
- **Speicherung & Datenhoheit** – Alle Kundendaten werden in AWS-Rechenzentren in Deutschland gespeichert, im Einklang mit EU- und lokalen Anforderungen zur Datenresidenz. Sub-Prozessoren arbeiten ausschließlich innerhalb des EWR
- **Verschlüsselung & Schutz** – Sensible Daten sind stets verschlüsselt, werden auf Anomalien überwacht und für Compliance-Zwecke protokolliert
- **Aufbewahrung & Lebenszyklus** – Daten werden nur so lange wie erforderlich aufbewahrt. Nach Vertragsende werden alle Kundendaten sicher gelöscht oder zurückgegeben; auf Wunsch mit schriftlicher Bestätigung
- **Trennung & Audits** – Kundendaten sind logisch voneinander getrennt. Regelmäßige Audits überprüfen die Einhaltung von Zugriffs- und Aufbewahrungsrichtlinien

Disaster Recovery & Backup

Studytube stellt durch eine robuste Backup- und Recovery-Strategie Ausfallsicherheit und Geschäftskontinuität sicher:

- **Hohe Verfügbarkeit** – Zielverfügbarkeit von 99,8 %, ausgenommen geplante Wartungsfenster
- **Sichere Backups** – Alle kritischen Daten werden mehrfach täglich gesichert, sowohl während der Übertragung als auch im Ruhezustand verschlüsselt, und nur autorisierte Personen haben Zugriff
- **Wiederherstellungsziele** – Strenge Vorgaben für Wiederherstellungszeit und Datenverlust stellen sicher, dass Dienste schnell wiederhergestellt werden können (RTO = 4h, RPO = 24h)
- **Tests & Validierung** – Backups und Wiederherstellungsverfahren werden regelmäßig getestet, um ihre Wirksamkeit sicherzustellen
- **Business Continuity** – Eine dokumentierte BC/DR-Policy regelt Vorsorge, Reaktion und Kommunikation im Falle schwerwiegender Vorfälle

Teil 3 - Aufsicht, Reaktion & Compliance

Organisation & Management

Studytube stellt durch starke Governance sicher, dass Informationssicherheit im gesamten Unternehmen verankert ist:

- **Audits & Risikomanagement** – Regelmäßige Risikoanalysen sowie jährliche interne und externe Audits nach ISO 27001 und SOC 2 Type II bestätigen die Wirksamkeit unserer Kontrollen
- **Mitarbeiter & Sensibilisierung** – Alle Mitarbeitenden werden vor Beschäftigungsbeginn überprüft, in Informationssicherheit geschult und durch Vertraulichkeitsvereinbarungen gebunden. Entwickler müssen nachweisbare Sicherheitsexpertise vorweisen, bevor sie Zugang zu Produktionsumgebungen erhalten
- **Betriebliche Schutzmaßnahmen** – Clean-Desk- und Clear-Screen-Policies, verschlüsselte Geräte, automatische Bildschirmsperren sowie starke Passwort-Richtlinien mit MFA schützen sensible Daten
- **Governance** – Alle Sicherheits- und Compliance-Richtlinien haben benannte Verantwortliche und werden regelmäßig überprüft, um mit neuen Bedrohungen und regulatorischen Anforderungen Schritt zu halten

Sicherheitsaudits, Penetrationstests & Automatisierte Tests

Die Sicherheit von Studytube wird kontinuierlich durch interne und externe Prüfungen validiert:

- **Penetrationstests** – Unabhängige Penetrationstests werden jährlich von spezialisierten Sicherheitsfirmen durchgeführt
- **Automatisierte Sicherheitstests** – Kontinuierliche automatisierte Tests stellen sicher, dass SSL-Konfigurationen, Zugriffskontrollen und Anwendungssicherheit stets den aktuellen Best Practices entsprechen
- **Code-Verifizierung** – Umfassende Test-Suites überprüfen alle Codeänderungen vor der Veröffentlichung und gewährleisten so die Integrität der Plattform

Incident Response

Studytube verfügt über eine dokumentierte Incident-Management- & Response-Policy, um Sicherheitsvorfälle schnell, transparent und konform zu ISO 27001, DSGVO und DORA zu behandeln:

- **Erkennung & Monitoring** – Vorfälle werden innerhalb von Minuten über moderne Monitoring- und Alarmsysteme erkannt, unterstützt durch proaktive Tests und Meldekanäle für Kunden
- **Reaktionsprozess** – Ein dediziertes Incident Response Team (IRT) koordiniert Eindämmung, Behebung und Wiederherstellung, um Auswirkungen zu minimieren und Dienste schnell wiederherzustellen
- **Umgang mit Datenschutzverletzungen** – Personenbezogene Datenvorfälle werden gemäß DSGVO behandelt, mit zeitnaher Benachrichtigung der Kunden, wenn Studytube als Auftragsverarbeiter agiert.
- **Kontinuierliche Verbesserung** – Alle Vorfälle werden protokolliert, überprüft und durch strukturierte Nachanalysen bewertet. Ergebnisse fließen in das Risikomanagement und die Stärkung der Sicherheitsmaßnahmen ein

Compliance

Studytube arbeitet nach einem umfassenden Informationssicherheits-Managementsystem (ISMS), zertifiziert nach ISO 27001. Wir sind vollständig DSGVO-konform, haben Auftragsverarbeitungsverträge (AVV) mit allen Sub-Prozessoren und werden unabhängig nach SOC 2 Type II auditiert.

Externe Zertifizierungen und Audits bestätigen, dass die Kontrollen von Studytube wirksam und konsistent angewendet werden. Bekannte Themen werden im Rahmen der täglichen Sicherheitsroutine adressiert. Durch kontinuierliches Scannen, jährliche Penetrationstests und Awareness-Schulungen wird das Restrisiko stetig verringert.

Wir bereiten uns aktiv auf relevante EU-Verordnungen vor und erfüllen diese, darunter:

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

In den Niederlanden richtet sich Studytube nach den staatlichen offenen Standards, um Interoperabilität, Transparenz und Datensouveränität für öffentliche Kunden sicherzustellen. Die KI-Funktionen von Studytube werden nach den Prinzipien Privacy by Design und DSGVO entwickelt – stets mit menschlicher Aufsicht und in Vorbereitung auf den 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