SECURITY WHITE PAPER

Why information security matters at Studytube

Version 2.0

STUDYTUBE

Inhoudsopgave

Introduction

At Studytube we believe that humans should never stop improving. Through learning and development, our users and colleagues aim to perform their jobs as best they can. But this motto also applies to our back-end processes. Especially when it comes to securing and protecting your data. That's why we are proud to have obtained our ISO 27001 certificate.

Besides employee development, the trust of our users and clients and the security of information are the foundation of our services. Studytube is continuously working on the improvement of our information security. This has always been an essential aspect of all processes at Studytube. As our company and the number of customers have grown, the need for a more formalized Information Security Management System (ISMS) has become more pressing.

Over the past few years, we've documented procedures and policies, setting up regular checks and audits. We've also reviewed our systems and assets and have assigned owners with specific, documented responsibilities. Finally, we've introduced a risk management process, which helps us to direct our efforts when it comes to improving and implementing information security controls. All are aimed at securing your data to the highest degree.

Having an ISO 27001 compliant management system helps us to comply with regulations such as GDPR, but it also ensures that we fulfill our contractual obligations with clients and suppliers.
On the following pages, you will find a summary of all the organizational and technical measures that Studytube has taken in relation to information security.

3. **Application** Security

Studytube ensures that users of the platform have access to precisely the data they are authorized to access. The security model works as follows: The platform has an elaborate permission-based structure that is built on three pillars of information: People, Learning Items and Budgets. Only specified roles can access either one, two, or all of the pillars. Access to People is limited to the data of specified Users, depending on the team they work in. Access to Learning Items can be differentiated based on permissions to view, edit, share, or access user data information connected to the Learning Item. Access to Budgets is dependent on approval rules.

4. **Web** Security

- All connections to and from our service use HTTPS with the TLS 1.2 (or newer if possible) protocol, using 2048-bit RSA keys and AES encryption, provided that clients support this as well (most modern clients do). We use a Content Security Policy (CSP) and HSTS HTTP headers to prevent XSS and Man-in-the-middle HTTPS attacks.
- The older and weaker TLS 1.1 and SSL protocols are disabled.
- We use AWS Security Groups that restrict access to the Web Server to specific protocols.
- All user input is validated before processing. Special care is taken to prevent Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and SQL Injection.
- We read the OWASP Top 10 regularly and take the provisions provided by OWASP as an essential element to building secure software.

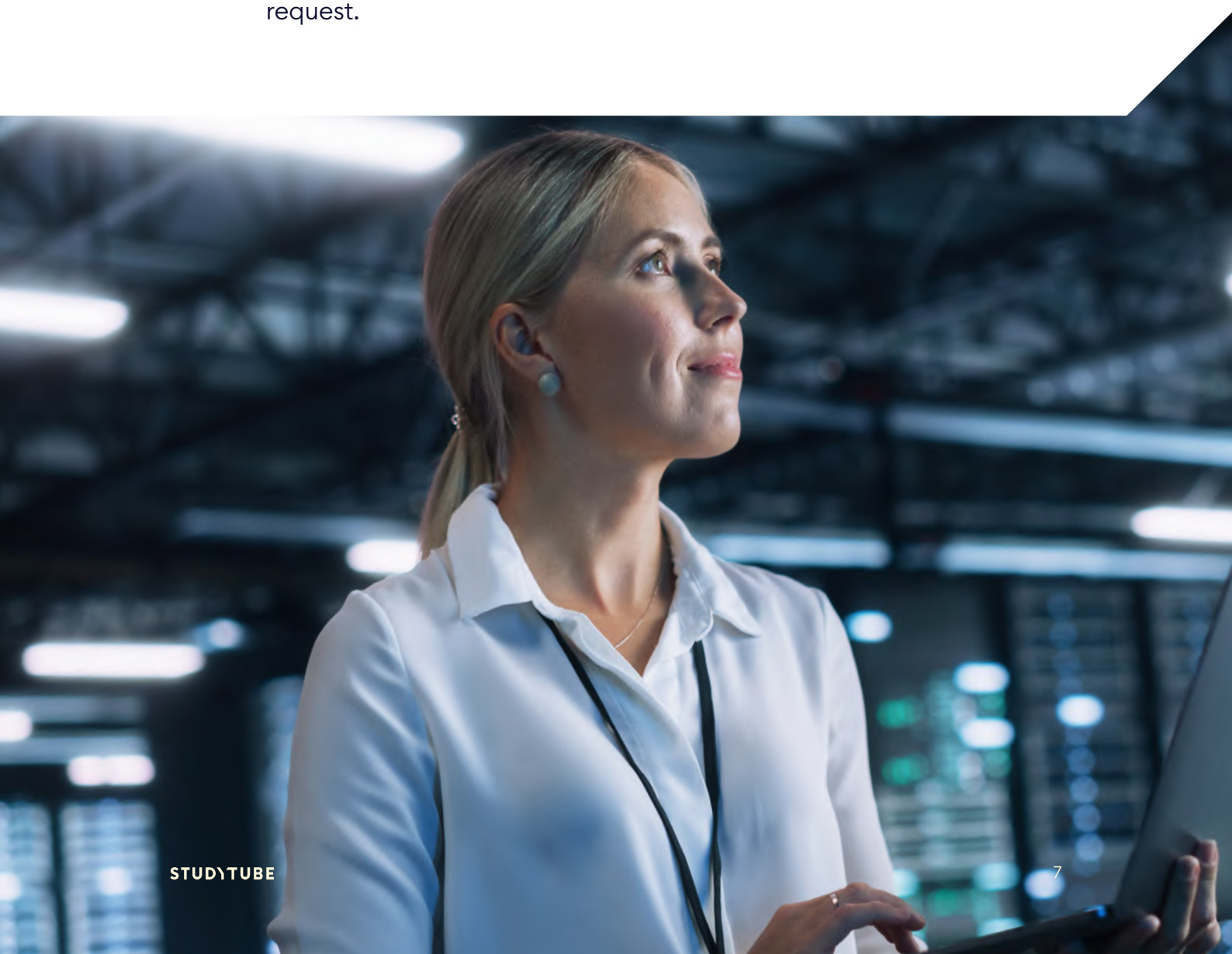
5. **Malware** Protection

- User-uploaded files are automatically scanned for malware upon upload and rejected if malware is found.
- Malware definitions are updated regularly and automatically.

6. **Authentication and Passwords**

- Studytube API Authentication is based on OAuth 2.0. Access tokens have a length of 100 bytes, are generated using OpenSSL's pseudo-random byte-string generator, and have a lifetime of 1 hour, after which they need to be refreshed.
- All active access tokens are revoked when a user changes his or her password.
- SAML 2.0 can be used for Single Sign-On.
- Devices can be logged out remotely.
- Passwords have a minimum length of 10 characters and must contain at least one lowercase character, one uppercase character, and one non-alphabetic character.
- Passwords are stored as salted hashes using the BCrypt algorithm, so Studytube has no knowledge of the actual passwords.
- When a password is forgotten, a user can request a password reset. A secret link to reset the password is sent to the user's primary email address.
- Email addresses need to be verified using a secret token before they can be used as primary email addresses.
- Passwords are never stored by Studytube on the user's device or in the browser. Instead, an OAuth token is stored securely.

- The token is cleared on mobile devices when the user logs out.
- Authentication tokens expire automatically when not used for a longer amount of time.
- All internal Studytube Admins use MFA to access the Studytube platform.
- AWS Infrastructure user keys/passwords have a regular rotation cycle.
- Studytube Login is protected on an application level against brute-force attacks.
- Whitelisting for specific logins and IP addresses can be enabled on request.



7. **Encryption**

- Data is encrypted in transit and at rest.
- All communication over public networks uses HTTPS with TLS 1.2 or later (where supported by the client). RSA keys have a length of 2048 bits.
- The older, weaker SSL protocol is disabled.
- Customer data is encrypted at rest using the AES-256 algorithm.
- Passwords are stored as hashes using the highly secure BCrypt algorithm.

8. **Email Protection**

- Outgoing transactional email is handled by our ISO 27001:2017 certified email delivery partner: Mailgun.
- DKIM signing is applied to all outgoing emails.
- Sender forgery is prevented using SPF.

9. Protection of Servers and Infrastructure

- The production environments are divided into multiple secure zones with firewall rules protecting traffic between them.
- Access to the production environments requires AWS SSM connection with mandatory 2-factor authentication.
- Least-privilege principle for access management is applied. Therefore, only a limited group of senior system engineers are provided with access to the servers in the production environments.
- All services are protected by firewalls allowing only absolutely required (web) traffic.
- Studytube servers are provisioned using a centralized configuration management system which ensures unified, secure configuration across all servers. Version control is applied to all configuration data.
- Security-critical patches are installed within 24 hours of availability.
- Studytube servers are automatically protected against L3, L4 and L7 DDoS attacks by the utilized load balancers.

10. **Logging and Monitoring**

- Operations performed by users in the application are logged into a centralized audit log.
- Server logs that are relevant to security are stored in a centralized way and are subject to automated analysis and alerting.
- 24/7 monitoring and alerting ensure that Studytube system engineers can act quickly in case of service disruptions.

11. **Data centers**

- The data centers in which Studytube is hosted are ISO 27001:2017 certified.
- Studytube's primary EU data center is operated by Amazon Web Services and is located in Frankfurt, Germany.
- Physical access to data centers and servers is restricted to authorized data center personnel.

12. **Disaster Recovery, Backup, and Redundancy**

- Studytube guarantees a 99.8% uptime, excluding scheduled maintenance windows.
- All critical services are set up redundantly to ensure high availability, in most cases with fully automatic failover.
- All customer data is backed up multiple times a day and kept for one month so that data can be restored in case of an emergency.
- Studytube's disaster recovery plan helps to recover services in the event of a disaster quickly.

13. **Security during Development**

- Studytube development environments are separated from testing and production environments.
- Production data is never used for testing purposes.
- Production data is never transferred from the production environment to test environments.
- Automated test suites are run for every change to Studytube code, and changes are not deployed until all tests pass. In addition, manual testing and quality assurance are done in an isolated testing environment that is not accessible to regular user
- All developers are trained to have extensive knowledge of application security.
- All changes to the Studytube code are peer-reviewed by senior developers. The application is developed according to industry best practices, and measures are taken to prevent vulnerabilities such as those listed in the OWASP Top 10.

14. **Security Audits, Penetration Tests, and Automated Tests**

- At least once a year, penetration tests are carried out by an independent security firm.
- Daily automated SSL server tests ensure our SSL configuration stays up to industry standards.
- The access controls of the application are subject to automated tests, which are run on every change and every release.
- All changes to the application are subject to an extensive suite of API and integration tests as well as unit tests and static analysis.
- Customers are permitted to conduct their own penetration tests on request.

15. **Organization and Management**

- Risk assessment and business impact analysis are carried out periodically.
- The ISMS is audited both internally and externally on a yearly basis as required by the ISO 27001:2017 standard.
- Information Security Awareness training ensures awareness of security risks and controls among all personnel.
- Personnel with access to customer data is screened prior to employment.
- Developers are required to demonstrate in-depth knowledge of security topics prior to employment.
- To protect sensitive data, Studytube employees sign a non-disclosure agreement upon employment.
- A clean desk and clear screen policy ensure confidentiality at the Studytube offices.
- Employee workstations are required to have strong passwords, full-disk encryption, and automatic screen-lock.
- Studytube's Password Policy requires that employees use strong, unique passwords for all systems used and that additional measures such as 2-factor authentication are applied when possible.

- Information classification policies, together with documented information and asset handling procedures, ensure confidentiality, integrity, and availability of sensitive information.
- All policies have identified owners and are reviewed regularly.
- Access Management procedures ensure that employee access to systems is granted and revoked when changes occur, such as onboarding, changes in roles within the organization, or termination of employment.

15

16. **Incident Response**

- Studytube has a documented Information Security Incident Response Procedure to ensure that responsibilities are clearly defined, and the correct actions are taken in case of security incidents.

- Studytube has a documented Personal Data Breach Notification Procedure, which ensures that the correct people are notified in accordance with GDPR articles 33 and 34.

17. **Compliance**

- Studytube maintains an Information Security Management System which is ISO 27001:2017 certified.

- Studytube is GDPR compliant.

- Data Processing Agreements are in place with all sub-processors.

- Studytube will direct law enforcement requests to the customer unless legally prohibited so that the customer can decide whether to produce the requested information or oppose the request.

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