Data Security at Wrike

Keeping your information safe is our top priority.

We know you need unparalleled data security as you work in the cloud. That's why Wrike is proud to offer one of the most advanced security models on the market. We are committed to keeping your organization secure while allowing it to be flexible enough to take advantage of rapid innovation and collaboration with internal and external stakeholders.

Our security protocols are in line with global best practices. Here is what you need to know about these features.

Stay in control of your data.

Wrike Lock* allows customers to own and manage the encryption keys to their Wrike data, giving them full access control.

Protect data at every touchpoint.

Safeguard sensitive data in transit and at rest with industry best practice use of AES256 bit encryption. Available on desktop and on mobile using Wrike's native Android and iOS apps.

Easily spot risks.

CASB integration support* enables customers to use SIEM systems and the CASB offering of their choice to easily spot unusual user activity and enforce enterprise security policies.

Authenticate with ease.

Wrike offers centralized password management and policies while supporting multiple methods of secure authentication, including multiple SSO* and SAML2* options. Users only need to sign in once to access Wrike projects.

Limit access to sensitive data.

Customized Access Roles* and Selective Sharing* ensure privacy and content integrity by enabling customers to create roles with unique permission sets to satisfy varied access and sharing requirements.

Know who has access.

Access Reports* enable customers to quickly and easily track and audit which users have access to folders or projects, as well as any tasks with attachments that external guest users have been invited to review.

Continuous reliability.

Wrike provides multi-site data redundancy and meets and exceeds an uptime of 99.9%. This means customers can access their tasks and projects without interruption.

Enterprise-grade security.

Wrike is trusted by 20,000+ leading brands and 2M+ users worldwide to manage their team's most important projects and to collaborate in the cloud securely, reliably, and to scale.

*Available on Wrike's Enterprise plan only

To physically secure your data, Wrike leases dedicated physical space for all of its servers in top tier data centers in the US and the EU. These data centers have implemented industry-standard systems and procedures to protect against anticipated security threats and unauthorized access of customer data.

Because we take data privacy and security seriously, we consistently undergo independent, third-party certifications.

SOC2 Type II: This independent, third-party examination assesses the nature and effectiveness of the internal controls Wrike uses to protect customer data. SOC 2 Type II audits demonstrate Wrike's commitment to taking a mature, robust, and secure approach to products, processes, and security as it relates to customer data.

ISO/IEC 27001:2013: This independent, third-party certification ensures Wrike has an end-to-end security framework and a risk-based approach to managing information security. The certification illustrates Wrike's dedication to a best practice security strategy aligned with international security standards.

ISO/IEC 27018:2019: This certification ensures Wrike has measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

CSA STAR: Wrike has passed the third party stage of this certification (Level 2 of CSA STAR). This demonstrates that Wrike, as a cloud service provider, has addressed issues critical to cloud security as outlined in the CSA Cloud Controls Matrix. It also demonstrates that Wrike has been assessed against the STAR Capability Maturity Model for the management of activities in cloud security control areas. CSA STAR is an independent, third-party assessment of cloud service provider security. The technology-neutral certification leverages the requirements of ISO/IEC 27001:2013 management system standards and focuses on specific cloud-service requirements.

Privacy Shield: To comply with EU data protection laws around international data transfer mechanisms, Wrike self-certifies under the EU-US Privacy Shield and the Swiss-US Privacy Shield. These frameworks were developed to establish a way for companies to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States.

GDPR & CCPA: For customers who request it, we have a Data Processing Addendum and CCPA Addendum that outlines the obligations Wrike has in its role as a provider of the Wrike Service to Customer. This may include obligations related to the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), Standard Contractual Clauses (SCCs), and California Consumer Privacy Act (CCPA) as well as other applicable laws.

HIPAA: The Health Insurance Portability and Accountability Act provides security provisions and data protection for safeguarding medical information. If Wrike processes Protected Health Information (PHI) on behalf of either a Covered Entity or a Business Associate (both known as "roles" under HIPAA), then Wrike has a Business Associate Agreement that meets industry standards and requirements as well as the HIPAA Security Rule. This is available upon request.

Privacy Policy: The Wrike Privacy Policy has been carefully cultivated to address your privacy concerns and your rights with regards to your personal data. If requested, Wrike will also provide a Data Protection Addendum, which describes our data practice.

Wrike

For more information on Wrike Security, please visit www.wrike.com/security/

Last Updated: May 2020