1. Collaborate on your projects in a secure environment

Thousands of businesses, including Fortune 500 corporations, trust Wrike for managing their projects through collaboration in the cloud. Security of your personal data, project-related information, files, and interactions within our system is our top priority. Which is why we are constantly focusing our efforts on maintaining the reliability of our product, infrastructure, technologies, and procedures. As we provide you with an easy-to-use, flexible, and scalable project management application, it is vital for us to ensure a trustworthy and reliable service, with comprehensive security at all levels. Below, you can read an overview of Wrike's security model across five elements — physical, network, system, application, and people. For our European customers, with EU Data Privacy mandates, Wrike is compliant with EU - U.S. Privacy Shield, Swiss - U.S. Privacy Shield as well as providing a EU data center location that retains customer sensitive data within the EU.

2. Physical security

World-Class datacenters in US and EU:

Wrike hosts their servers in locked cages within data centers located in the U.S and EU:

- Trusted Data Center in the U.S is compliant with SSAE 16 Type II and ISO 27001 standard, and is located in San Jose, California.
- Wrike's European Data Center is hosted in Amsterdam, Netherlands and is also compliant with ISO 27001 and ISAE 3402 standards (equivalent to SSAE 16). This data center is isolated and retains customer and sensitive data within EU only.

These facilities feature 24/7 manned security, fully redundant power backup systems, physical access controls, biometric authentication systems, extensive seismic bracing, the latest in early-detection smoke and fire alarms, and digital surveillance systems. All server and network components are constantly monitored by internal Wrike staff and by the colocation providers. Wrike's Disaster Recovery infrastructure resides in Google Cloud Platform for both US and EU regions, having great scalability and security with SSAE16 / ISAE 3402 Type II, ISO 27001, FedRAMP, PCI DSS, HIPAA and other certifications. Access to each

system, network device, and application is limited to authorized personnel, and login details with the event logs reviewed on a regular basis.

Uptime over 99.9%

Over years of continuous service, Wrike has consistently met or exceeded 99.9% uptime, ensuring customers can access their tasks and projects when needed without interruption. We also provide an alternative approach to the availability of your workspace: if Wrike is temporarily unavailable due to technical reasons or scheduled maintenance, you can log in to the stand-alone, read-only replica of Wrike in order to access all your data at: https://read.wrike.com, or https://read-app-eu.wrike.com for European customers.

Continuous data backup

Wrike is running real-time database replication, to ensure that customer data is both backed up and available on redundant and geographically dispersed servers, physically separated from the primary Wrike application servers, aiming to ensure fault tolerance.

3. Network and System Security

Tenable Network Security Infrastructure

Wrike uses industry-standard network protection procedures, including network segregation using VLAN's, firewall and router technologies, intrusion detection systems, log aggregation and alert mechanisms in conjunction with secure connectivity including VPN and SSH keys for authorized Systems Operations personnel. This allows us to prevent, detect, and promptly remediate impacts of malicious traffic and network attacks.

Regular Updates and Patch Management

Regular internal network security audits and scanning gives us an overview for quick identification of outdated systems and services. According to the in-house patch management policy: operating systems, software, frameworks, and libraries used in Wrike infrastructure are updated to the latest versions on a regular basis. Whenever a vulnerability in a product used by Wrike or a High or Critical vulnerability is publicly reported, prompt actions are taken in order to mitigate any potential risks for our customers — we apply hot fixes and patches promptly upon availability.

System Integrity Protection

Wrike uses operating systems based and custom integrity check services in order to ensure

the integrity of all critical files and system objects. A quick response to any potential unauthorized changes to the system helps assure that our customers are using authentic Wrike application services.

4. Application security

Application Security Process

An in-depth Application Security Life Cycle process is fully integrated into Wrike's Software Development Life Cycle (SDLC), including:

- Defined in-house security requirements and policies, and well-known security best practices applied in every stage of the lifecycle.
- Security review of architectures, design of features, and solutions.
- Iterative manual and automated (using static code analyzers) source code review for security weaknesses, vulnerabilities, and code quality, and providing of sufficient advice and guidance to the development team.
- Regular manual assessment and dynamic scanning of pre-production environment.
- Security trainings conducted for IT teams according to their respective job roles.

Authentication and Access Control

Each user in Wrike has a unique account with a verified email address, and protected with a password, which are validated against password policies and stored securely using a strong hashing algorithm with unique salt for every password. 2-Factor Authentication is available as an additional security measure to protect Wrike accounts. Wrike also supports multiple methods of federated authentication, including Google Open ID, Azure, Office 365, ADFS and SAML V2, to conveniently and securely gain access to Wrike account leveraging corporate credentials. A Wrike account administrator manages and controls individual user rights by granting specific types of user licenses. Details about various user licenses, roles, and authorization controls in Wrike are documented in our Help Section. Customer data, including tasks and folders, can only be accessed by other users within your Wrike account if those items were specifically shared with them, or if the items were placed in shared folders. Otherwise, your projects and tasks are not accessible by other Wrike users. Wrike Support Team is always happy to assist you with any Wrike-related issue. If troubleshooting or verifying the issue requires Support to access to your account; that access can only be granted by you. This is enabled by a system generated security token that you provide out of band to our Support team, allowing Support to delve deeper into solving your problem

for a limited amount of time. This systemic approach ensures additional confidentiality for your data stored in Wrike.

Monitoring user activities

Wrike offers the possibility to get a report with up-to-date account activity information, including authentication events, changes in the authorization and access controls, sharing folders and tasks, and other security activities.

Data Encryption

Wrike uses Transport Layer Security (TLS) TLS 1.2 with a preferred AES 256 bit algorithm in CBC mode and 2048-bit server key length with most modern browsers. When you access Wrike via a web browser, mobile applications, email add-in, or browser extension, TLS technology protects your information using both server authentication and data encryption. This is equivalent to network security methods used in banking and leading e-commerce sites. All users of Wrike get the same encryption reliability, regardless of their subscription type, so that your passwords, cookies, and sensitive information is reliably protected from all eavesdropping. User files uploaded to Wrike servers are automatically encrypted with AES 256 using per file keys. If someone were to gain physical access to the file storage, this data would be encrypted and impossible to read directly. These encryption keys are stored in a secure key vault, which is a separate database decoupled from the file storage layer.

Mobile Applications

Wrike provides access to workspace via Android and iOS applications, which inherit security functional from web-based application, but also have additional security features like encryption at rest, certificate pinning, checking against rooted/jailbroken device and application-level protections using PIN code or fingerprint, allowing mobile access to be more secure.

Account and Content Recovery

You can safely recover accidentally deleted items from Wrike's recycle bin. If a user is deleted by mistake, there is possibility to recover the deletion (including some of their tasks) if you contact us no later than 3 days. Some user account information can be recovered for the user account up to a month after the deletion took place.

5. Organizational Security

Processes

Designing and running data center infrastructure requires not just technology, but a disciplined approach to processes. This includes policies about escalation, management, knowledge sharing, risk management, as well as the day-to-day operations. Wrike's security and operations teams have years of experience in designing and operating datacenters, and we continually improve our processes over time. Wrike has also developed best-in-class practices for managing security and data protection risk. All of these elements are essential parts of Wrike's security culture.

Need-to-Know and Least Privilege

Only a limited set of employees have access to our data center and the data stored in our databases: there are strict security policies for employee access, all security events are logged and monitored, and our authentication methods and data are strictly regulated. We limit access to customer data to employees with a job-related need, and require all those staff members to sign and agree to be bound by a confidentiality agreement. Accessing customer data, is only done on an as-needed basis, and only when approved by the customer (i.e. as part of a support incident) via a support token, or under authorization from senior management and security for the purposes of providing support, maintenance, and improving service quality.

6. Data Privacy and Sharing

Wrike has self-certified with U.S. - EU Privacy Shield Frameworks and is registered with the U.S. Department of Commerce's Privacy Shield program as documented at www.privacyshield.gov. Additional details available at www.wrike.com/privacy.

7. Audit and Certification

Wrike is independently certified with AT 101 SOC 2 (Type II) for Security and Confidentiality principles, confirming that Wrike takes appropriate steps to protect its systems and customers' data. In addition, Wrike is a member of the Cloud Security Alliance (CSA) and the result of our Security, Trust & Assurance Registry (STAR) Level One assessment is published on the CSA website, and can be found at https://cloudsecurityalliance.org/star-registrant/wrike-inc/.

8. Enterprise Grade Security

If you have any security concerns, please contact our Sales team at **877-779-7453**, and they will provide you with additional security artefacts and external reports confirming our security maturity.

Would you like to learn more? Have a security concern?

If you have any questions about the security of Wrike, you can contact our IT Security Team anytime at security@team.wrike.com.