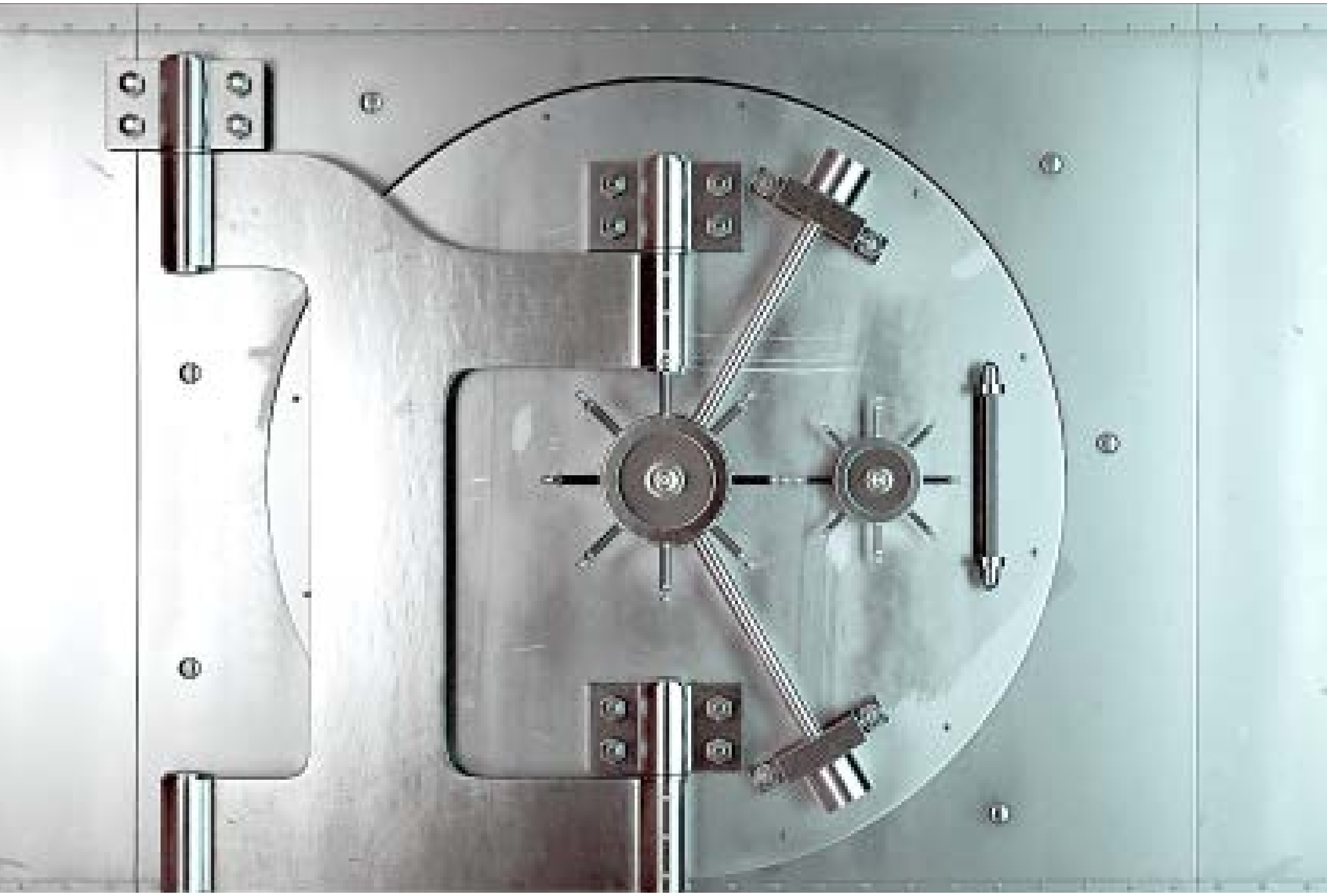
WORKSTORM™

Secure. Collaborate. Work.



Our Mission is Your Productivity

Workstorm provides enterprise-grade workplace collaboration technology. Built by professionals for professionals, the company's fully integrated, customizable collaboration platform combines workflow efficiency with data security. The platform combines all forms of communication including: messaging, email, video conferencing, calendar, screen sharing, and file sharing, to name a few. With Workstorm, details are never missed, wires are never crossed, and everyone stays on the same page.

But, collaboration isn't just about sharing ideas and documents. It's also about keeping those ideas and documents secure and confidential. **At Workstorm, the security of your data is the core focus of our technology and our business.**

The foundation of Workstorm is rooted in privacy, security, and data controls. The company's founders and key employees originate from the financial industry where information transfer is highly regulated. These leaders are highly involved in the day-to-day operations of Workstorm. Further, ethics and integrity are built into the organization's values and behavioral standards. Our team has a deep appreciation for the importance of the data we are hosting and its impact on your business.

We also believe that your data is your data, not ours. Other technology companies may sell or rent your data to advertisers or third parties. At Workstorm, that will never happen.

This background and understanding guide our decisions when it comes to infrastructure, software design, access rights, and policy development. With that in mind, we developed Workstorm to give you control over your own data. This document describes the methodologies and techniques used to mitigate security risks and implement privacy controls within Workstorm.

Serious Security for Serious Collaboration

Workstorm is dedicated to ongoing identification, analysis, and management of security risks relevant to our platform and your data. Every decision we make involves answering questions about how a new feature or process impacts your security and privacy.

The key principles contained herein form our security controls environment. Each of these topics is covered in-depth in a Type II SOC 2 report generated by an independent auditor. This report is available upon request.

INFRASTRUCTURE

Information that flows, not leaks.

Workstorm's environment is constructed to ensure that you have the highest confidence in our safekeeping of your data.

DEPLOYMENT MODEL: With multi-tenant cloud, private cloud and on-premise deployment options, Workstorm provides the flexibility and security necessary to match a range of client and corporate privacy and compliance policies.

- Most of our clients operate effectively in a multi-tenant hosting model that allows clients to share computing resources, driving down infrastructure costs while increasing IT efficiencies. Each client's data is isolated and remains invisible to other clients. For this model, we select the world's most secure cloud providers, such as Amazon Web Services and Microsoft Azure, which meet enterprise security standards.
- If you are required to conform to specific regulatory or security demands, we can set up a private cloud model, in which a hosting environment is built and maintained specifically for you.
- Workstorm can be installed behind your firewall and configured on your hardware for complete control. On-premise licensing is highly customizable and includes configuration support and training to ensure a smooth deployment, as well as compliance with the most stringent IT and information security requirements.

LOGICAL ACCESS CONTROLS: Logical access security measures have been implemented to protect against security threats from outside the system.

BACKUP AND DISASTER RECOVERY: Workstorm's business continuity and disaster recovery framework ensures resiliency, recoverability, and contingency from significant business disruption. Daily backups are performed and successful and failed backup alerts are monitored. Periodically, restores are tested to verify the backup and recovery procedures.

MONITORING CONTROLS: Workstorm applies intrusion prevention and detection systems to monitor system problems, including, but not limited to, system performance degradation, system errors, unusual activity, and suspected or actual unauthorized access. There are defined protocols that we follow in the event of an incident of this manner.

PENETRATION TESTS: External penetration tests are performed routinely, conducted by an outside firm specializing in this type of work. The objective of this assessment is to identify weaknesses within the Workstorm systems that may lead to the exposure of sensitive information or unauthorized system access.

SUBSERVICE PROVIDERS: Workstorm obtains and reviews the annual system and organization control (SOC) audit reports for subservice organizations.

SOFTWARE

Technology that is secure by design.

Workstorm runs on a technology platform that is conceived, designed, and built to operate securely.

SOFTWARE DEVELOPMENT LIFECYCLE AND SOURCE CODE: Workstorm upholds a software development and maintenance process that is critical to the availability and integrity of the Workstorm platform. Further, application source code is stored within a code repository, which controls access to authorized personnel that require access to perform their job.

PASSWORDS AND ACCOUNT SET-UP: Workstorm enforces strong password creation requirements. When a company profile is created, you designate a contact person to administer new accounts and set up all other accounts.

ENCRYPTION: Workstorm offers enterprise-grade encryption that follows industry security standards. Your communications and data are encrypted both in transit between devices and parties, and when at rest on our servers.

ANALYTICS: Workstorm provides you with insight into the use of the technology to proactively ensure users are complying with security policies and standards specific to your industry or regulatory requirements.

PEOPLE

Security engrained in our culture.

Our employees understand the importance of protecting the information entrusted to us.

BACKGROUND CHECKS: All offers of employment at Workstorm are contingent upon clear results of a thorough background check.

CONFIDENTIALITY: All employees contractually agree to maintain confidentiality of client information.

PHYSICAL ACCESS CONTROLS: Physical access restrictions are implemented and administered so that only authorized individuals have the ability to access Workstorm facilities.

TRAINING: Employees are required to attend an annual security training that covers information security, data protection, and confidentiality of client data.

PROCEDURES

Policies driven by priorities.

Workstorm implements policies and procedures so that you can rely on our products to operate with the highest levels of security.

TECHNICAL SUPPORT AND INCIDENT REPORTING: Support is available to answer your security questions or help you report failures, incidents, or concerns related to the system in the event problems arise.

RETENTION AND DISPOSITION: For data disposal, we will support your retention and disposition requirements and follow industry standards and advanced techniques for data deletion and media destruction.

COMPLIANCE: Data can be exported from Workstorm for compliance purposes in regulated industries.

LEGAL REQUESTS: If we receive a legal request for information about or contained within your Workstorm account, we will ask the requesting party to contact you directly, unless prohibited by law.

Ready to get to work?

workstorm.com