WeWorked

Security Overview

Introduction

Ensuring the safety and security of customer data is not just a priority, but a monumental responsibility for WeWorked. Diligently, we devote ourselves to shielding our customers from emerging threats, employing rigorous measures to safeguard their sensitive information. It's worth noting that we store our own critical data on the very servers utilized by our customers, underlining our shared interest in fortifying defenses against potential breaches. In essence, our commitment to preserving data integrity aligns seamlessly with our customers' objectives, fostering mutual understanding and a shared dedication to maintaining the highest level of security possible.

Access control and organizational security

All personnel, including both employees and contractors, are required to sign confidentiality agreements prior to obtaining access to our code and data. While background checks are not conducted on our workers, comprehensive training sessions are provided to all members of the WeWorked team, ensuring they are well-versed in security protocols and best practices for their respective systems.

Access to servers remotely is exclusively granted through our VPN, utilizing two-factor authentication, and is restricted solely to individuals whose roles necessitate such access for their daily tasks. Additionally, we meticulously log all account access, tracking it by IP address for accountability and security purposes.

We implement centralized management and robust security measures for Mac computers utilized by our staff, minimizing our vulnerability to security breaches. This entails applying a uniform configuration to each device, which includes enabling disk encryption, firewall protection, and enforcing password regulations. Furthermore, essential applications are installed, and we ensure they are regularly updated with the latest security patches to mitigate potential risks.

Dedicated Teams

Our Operations team, in collaboration with our Security, Infrastructure, and Performance (SIP) team, holds responsibility for access and identity management, network connectivity, firewall configurations, and log file management. Their diverse range of duties encompasses:

- Sustaining and enhancing our automated test suite for development machines
- Vigilantly scrutinizing all code and infrastructure modifications to ensure adherence to best practices and stringent security protocols
- Architecting and maintaining the WeWorked infrastructure, which encompasses logging, monitoring, and authentication systems
- Formulating, testing, and refining incident response procedures to swiftly address security breaches
- Promptly addressing alerts triggered by any detected security incidents
- Orchestrating external audits and pursuing security and privacy certifications to uphold industry standards
- Proactively monitoring and flagging any aberrant activities within the system
- Collaborating with external security researchers to conduct vulnerability assessments
- Implementing and deploying application-level encryption and cutting-edge tools to fortify internal safeguards for customer data

Audits, Security Policies and Standards

We utilize a system designed to monitor and proactively block any suspicious activities, such as vulnerability scanning and repeated failed login attempts, among other potential threats. Additionally, our system is configured to generate alerts for instances of excessive resource utilization, which are promptly escalated to our Operations team for thorough manual investigation.

Furthermore, our products operate within a dedicated network environment fortified by robust firewalls and undergo meticulous monitoring to ensure the integrity and security of our infrastructure.

Privacy

Our overall privacy policy is available at **https://weworked.com/privacy**

Data Location

We used Amazon AWS and our main data centers are situated in the United States. As an AWS customer we inherit all the best practices of AWS policies, architecture, and operational processes built to satisfy the requirements of our most security-sensitive customers. AWS environments are continuously audited, with certifications from accreditation bodies across geographies and verticals. You can read more about the various AWS compliance programs at **https://aws.amazon.com/compliance/programs/**.

Some of the highlights are: ISO 9001:2015, ISO/IEC 20000-1:2018, SOC 1, SOC 2, and SOC 3.

To fortify data integrity and resilience, all information undergoes instantaneous replication across multiple disks, with daily backups stored in diverse locations. Files uploaded by our customers are housed on servers engineered with advanced techniques to mitigate bottlenecks and minimize potential points of failure.

Moreover, our software infrastructure receives regular updates incorporating the most current security patches, ensuring ongoing protection against emerging threats.

Encryption

Over public networks we send data using strong encryption. We use SSL certificates issued by Go Daddy Secure Certificate Authority - G2. The connection uses TLS 1.2, AES_128_GCM, and ECDHE_RSA with P256 for encryption.

Physical Security

Our state-of-the-art servers are protected by biometric locks and round-the-clock interior and exterior surveillance monitoring. Only authorized personnel have access to the data center. 24/7/365 onsite staff provides extra protection against unauthorized entry and security breaches. Read more about our the security of our data centers at **https://aws.amazon.com/compliance/data-center/data-centers/**

Law enforcement

We uphold a strict policy regarding the release of your data to law enforcement agencies. Unless compelled by a court order, we categorically refuse requests from both local and federal authorities seeking access to data. Furthermore, we are committed to informing you whenever we receive such requests, unless legally prohibited from doing so.

Data deletion

Upon cancellation, all of your content will become immediately inaccessible on the last day of your current subscription period. All of your data across our apps will be permanently deleted from our servers after 30 days.

We maintain backups for an additional period of 30 days. Consequently, following cancellation, our data recovery team may have the ability to retrieve your information from a backup for a fee.

Incident management and disaster recovery

We conduct routine recovery drills to simulate various disaster and failure scenarios, ensuring our preparedness for any eventuality. Hourly backups of all databases are performed, while files are automatically backed up upon upload to WeWorked. These backups undergo regular testing and are securely stored off-site for up to 30 days.

In the event of an incident, our dedicated Operations and Security, Infrastructure, and Performance teams are poised to respond swiftly. Within 24 hours of an incident, we will reach out to your account owner and collaborate closely with you to address the situation effectively.

Company Name, Mailing Address, and Representative

Techstoned, LLC
12011 Wardell Way, Brandywine, MD 20613
contactus@weworked.com

Point of Contact: John Holmes II

Conclusion

While we're unable to fill out security questionnaires, we trust the documentation here provides the information required.

Over the past decade, we've dedicated ourselves to cultivating trust among hundreds of thousands of companies globally. This commitment remains steadfast as we strive each day to uphold that trust.

At WeWorked, longevity and stability form the bedrock of our mission.

Want to know more?

Contact us if you have other security questions. We'll get back to you as quickly as we can.