# Security Whitepaper

*September 2022*

*We are very proud and excited to announce that after the successful completion of a series of audits, Remo is now* **ISO 27001 & SOC 2 Type 1** *certified as a SaaS organization. To request details or copies of the certification and the full report, you can email legal@remo.co for these milestones.*

Security is oxygen to any modern business. As Remo humanizes the online social interactions and helps create meaningful connections, security is built into the very core of our company. Even as a startup, we breathe security starting with utmost privacy of critical human information amidst the modern technology - without spoiling the human experience and collaboration. We take pride as we go all out in protecting sensitive business data and critical personal information of all our clients and partners who entrust to us their online conferences, web gatherings, and virtual human events experience.

This document intends to answer the usual questions on how Remo ensures data privacy, information security awareness, how we collect and process data, IT security compliance, information security policies, ISMS, and the high-level information and related resources overarching security within Remo.

### Privacy and security

As organizations and clients streamline their businesses, protecting everyone's privacy is always at the core of Remo's security. Our web application uses secure video, audio, chat, and lots of collaboration features to enable users to interact naturally in real-time, from anywhere in the world. We have different types of users with distinct access to secured sets and levels of features and perks. Remo events can be set as Public or Private as an additional secured flexibility and users can log in via secure SSO options using their Microsoft, Google, LinkedIn or Facebook accounts. We can also implement SAML SSO as an add-on for your organization, just kindly email your request to sales@remo.co for assistance and evaluation. As we expand and provide more meaningful connections to our ever-growing list of clients and partners, Remo is ever diligent and always vigilant to all aspects of privacy and security. We have a very comprehensive Cookie Notice and Privacy Policy hand-in-hand with our Data Protection and our Information Security Policies. At the very start of your journey with us, you will clearly experience Remo's permission-based approach in data privacy and security. You'll basically provide data inside our web application only when it is with your consent and permission. As for any content during the event, Remo does not intercept or record it unless you as the host actually record it. Our data privacy and security commitment is further strengthened with GDPR in all our Data Processing Agreements (DPAs) for US, European, and other international clients for mutual consideration of obligations. Whenever you have clarifications prior to entering an agreement or sharing any information with Remo, our support teams are always available.

### Secure real-time human interactions

Making the online interactions transformed into a humanized experience is our noble goal in Remo. With the accessible technology, we protect your connected experience end-to-end with your data and your privacy secured real-time. Everything in our events is focused with your vital interest and with your consent. Remo adheres to data minimization principle. Remo strives to limit the scope of information used, requested, and processed to the minimum. A speaker or guest only needs to indicate the name & email address to get access to the platform. Guests can also register using only their names or nicknames without surnames. The Host (Account Owner) is responsible for all the content used, produced and reproduced during the event and Remo does not monitor events actively and can't be held responsible for what happens in the events as explained in our Customers Terms of Service and Users Terms of Service. Furthermore, using an alias and made up emails is possible. We only need information about the account owner (individual or corporation). Remo's secured platform has the ability to make your event as private as you want and with the right participants that you want by allowing you or the event owner to expel and ban users from your event real-time. You as the Host or your assigned Event Manager can also securely upload your guest list ahead when you create an event. All these perks of privacy and security, the responsibilities, and the things that govern your access to and use of Remo are found in our Customers Terms of Service and Users Terms of Service along with our Privacy Policy and Cookie Notice. We further protect you and secure your online experience with how Remo processes sensitive information and our Data Protection. You can rest assured that your interactions and human connections are safe with Remo and our platform. All you have to focus on is growing your network, enjoying your events while making meaningful human connections.

### Security awareness

We at Remo give additional focus and extra care to the security of the sensitive data and all information entrusted to us. We constantly take all reasonable steps to safeguard and only process personal information relevant to the purpose for which it needs to be collected with user consent in accordance with our Privacy Policy, Data Protection, Information Security Policies and ISMS. We employ strong password policy, multi-factor authentication (MFA), role-based access restriction, a need-to-know basis of data availability, and other security controls via our stringent Access Control Policy among others. Our secure system only allows user data access just to fulfill customer requests. Other policies and their detailed information are found in our

Information Security Policies. Our support articles include what security standards does Remo adhere to and technical requirements with troubleshooting.

## Security compliance and standards – the reliability of our Cloud technology

As a SaaS company, we are now SOC 2 Type 1 certified. Our live website (the actual platform users log in to) is equipped with Content Security Policy (CSP), HTTP Strict-Transport-Security (HSTS), TLS 1.3 protocol, Clickjacking prevention and other website security implementation. Our dedicated 24/7 teams in Remo Engineering make sure of our OWASP Top 10 and CWE Top 25 above-standard awareness and protection real-time. Regular Penetration tests, vulnerabilities and other proactive security testing are periodically performed in accordance with our Information Security Policies.

Remo is built on highly secured Cloud technology and leverages inherent extra layers of security and privacy, encryption, data protection, compliance, and other redundancies provided by our trusted Cloud technology partners. They also provide extra protection in our secure transactions and subscription management, global and flexible firewalls, identity and access management, continuous data transmission and backup, data loss prevention, and necessary Cloud security scanning, alarms and proactive alerts.

Security and Compliance is a pair of inherent leverages Remo always has together with a shared responsibility between its Cloud technology providers. This shared model and partnership provides Remo the powerful business technological edge as our providers operate, manage and control the Cloud infrastructure for Remo – the components, the systems involved and even the virtualization layer down to the physical security of the facilities in which the services they offer operate. They also provide us with the security of the Cloud and the necessary protection and monitoring of the global infrastructure that runs all the services we partnered with them. As they provide us the Infrastructure as a Service (IaaS), we also inherit their secured physical and environmental controls including database security, best practices, and a variety of IT security standards, including:

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018
- ITAR
- FIPS 140-2
- MTCS Level 3
- HITRUST

The Cloud technology platform additionally provides inherent flexibility and control allowing Remo to deploy solutions that meet several industry-specific standards, including:

- Cloud Security Alliance (CSA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)

- Motion Picture Association of America (MPAA)
- Criminal Justice Information Services (CJIS)

You can find more detailed security information about our main partners and their services below:

- Google Cloud
- AWS (Amazon Web Services)
- MongoDB
- Cloudflare
- Stripe
- Chargebee
- Freshworks

### Data processing

We carefully and securely handle all data Remo collects about users starting with how Remo processes sensitive information. Our business model is to provide a paid service to users who need additional features on top of the trial version and does not rely on widespread collection of general user data. We at Remo are committed to safeguarding the privacy of our users. We will only collect information that we need to deliver the service to you and continue to maintain and develop the service. Every Remo employee adheres to company security policies and standards of conduct on stringent data processing and protection. Criminal background checks are also included on top of our hiring procedures, skills, references, and credentials validation. Our platform security, video and audio streaming, cloud database, network security, role-based permissions and access control, Cloud and encryption technologies, Customers Terms of Service, Users Terms of Service, Privacy Policy, Data Protection, Cookie Notice, all Information Security Policies and ISMS encapsulate our protection to user account information and secure data processing as we partner with highly secured and well known Cloud technology giants mentioned above.

### Data encryption

All communications between our platform in Remo along with underlying access to Cloud databases, storage layers and other services are all encrypted via AES-256 and AES-128 algorithms in different situations, all data integrity verified and using HTTPS connections via our HSTS, CSP, TLS 1.3 protocol and other security implementation mentioned above. Our highly secured Cloud technology platform provides us numerous at rest storage encryption and other protection with all database systems fully redundant across multiple availability zones and backup in the Cloud.

Remo also leverages Cloud technology in using dedicated server infrastructure to allow more users in the conversation enjoying quality interactions with better stability. Streams will always be encrypted with the AES-256 algorithm in transit and will be decrypted and re-encrypted when passing through highly secured infrastructure of video routers strategically distributed across the world. The video router servers and all our infrastructure adhere to strict security standards and inherent security compliance preventing any eavesdropping or interruption of the video/audio streams.

**Highly secured firewall solution**

Remo further protects all users and their data via a highly secured firewall solution in place that filters both ingress and egress traffic, secures all communication instances, and adheres to high standards of Cloud technology on top of the usual WAF and DDoS attack protection. We also have a very comprehensive Gear Test (system compatibility) available handy to check a user's browser and network compatibility including secure firewalls, internet speed, operating system, VPN and any Ad-blocker. Inherent layers of protection and higher levels of security are afforded by our secure web application with the firewall solution deployed on the network and all its virtual interface as Remo is built and maintained by a highly skilled and experienced team of SaaS engineers, developers and QAs.

**GDPR journey and other compliance**

Remo processes and protects data based on legitimate interests, vital data protection and user consent along with their rights and obligations per our Customers Terms of Service, Users Terms of Service, Privacy Policy and Data Protection. As a startup, we are taking our GDPR journey seriously and have numerous wins and positive outlook on our roadmap ahead together with other compliance journey below:

- **GDPR at Remo**
- **GDPR Roadmap**
- **FERPA**
- **HIPAA**
- **CCPA**
- **COPPA**

**Security & accessibility in our knowledge base**

Secured, timely and easy-to-follow steps to assist all users on common Security and

Accessibility related solutions are found and updated in our knowledge base online with link below:

https://help.remo.co/en/support/solutions/63000134089

### Something we didn't cover?

Connect with us via our Contact a Specialist button (upper left across all remo.co web pages), 24/7 Online Product Support Chat (bottom right),

In-event Product Support Chat (bottom left of your Remo Events), Remo Help Desk, or email us at legal@remo.co