Security Measures MinuteTrack

Date: 28-03-2024

Introduction

At MinuteTrack, we consider the security of your data to be extremely important. We are fully committed to protecting your privacy and information with the latest security technologies. We implement advanced techniques such as data encryption, network security, and strict access controls. Our goal is to provide a reliable and secure platform where users can confidently manage and share their data.

Table of Contents

Security Measures

In this chapter, we discuss the security measures that we and our partners implement to protect your data. To optimize security, we do not specify all the security measures we take. This helps to further protect our systems and your data against potential threats.

1. **Advanced Cryptography:** We apply password encryption using 'bcrypt'. This protects your data from breaches by ensuring that even if data is intercepted, it is unreadable without the correct key. In addition, we limit access to the server with strong public/private key cryptography, where only authorized users with, among other things, the correct 'private key' can gain access, while any information sent to the server is encrypted with a 'public key'.
2. **SSL-encryption:** To ensure the safety of your data, our website uses advanced SSL encryption. This means that during transmission, your data is fully encrypted with PKCS #1 SHA-256 and RSA encryption, protecting the data from interception between your device and our servers.
3. **Data encryption:** All files you store via our platform are encrypted on the physical disk using 256-bit AES-XTS full-disk encryption, one of the most advanced encryption technologies available. Even with physical access to the disks, the data is unreadable without the correct decryption key, providing an extra layer of security against attempts at data intrusion or theft.
4. **Two Factor Authentication:** We standardly implement two-factor authentication (2FA) for all services and tools we use, such as DigitalOcean, Stripe, and email, where this extra security layer is always activated if the service offers it. The application of 2FA significantly increases security by adding a second verification step; in addition to the password, a physical or digital token is required, such as a code sent to a mobile device. This method enhances security and effectively protects against unauthorized access to your data.
5. **Daily backups:** Backups of all data are automatically made daily. Regular checks are conducted to ensure complete backups. The backups are stored with DigitalOcean and are protected at the same level as other data, ensuring that your data is always available, even in unforeseen events.
6. **Virus and malware protection:** With our advanced virus and malware protection, we also keep threats away from our own workstations. Incoming emails are scanned before delivery, and our employees are instructed on recognizing phishing and other unreliable emails.
7. **Limited access:** Through strict physical and digital security measures and access restrictions, we ensure that only authorized personnel can access your data. Examples of physical security include limited authorization and access to login information, employee instructions, and confidentiality agreements, intrusion prevention, and camera surveillance. Examples of digital security include location-based access and rights restrictions, the use of strong passwords and password managers.
8. **Logging en monitoring:** We use continuous monitoring and real-time alerts, allowing us to respond immediately to any irregularities. This not only enables us to respond quickly to errors but also provides us with insights into performance, server, and network usage. This proactive approach to logging and monitoring increases our response speed to incidents and contributes to the ongoing improvement of our security and service.

Our partners

At MinuteTrack, we also use various online partners to offer our services. We want to be transparent about this so you know you can trust our software. We only work with leading partners who take their security seriously.

1. **DigitalOcean (server/data):** DigitalOcean is known for its advanced security measures and reliable cloud services. Their robust encryption, firewalls, and continuous monitoring provide a secure environment for our server infrastructure. We choose DigitalOcean for their commitment to security and stability, ensuring that you, our end users, can always rely on us for safe and reliable service.
   See also: https://www.digitalocean.com/security/
2. **Stripe (payments):** Stripe is globally recognized for its excellent security standards and reliability as a payment provider. With strict adherence to the highest industry standards, advanced encryption techniques, and continuous fraud prevention, Stripe offers a secure payment platform. By using Stripe, we ensure that your transactions are safe and your financial information remains protected, allowing you to use our services with confidence.
   See also: https://stripe.com/docs/security/stripe
3. **Google Firebase (app services):** Thanks to Google Firebase, our app can function effectively, with platform security meeting Google's high standards. This means your data is protected with the most advanced encryption technologies and security protocols, allowing you to use our services with confidence.
   See also: https://firebase.google.com/docs/security
4. **Sendgrid (e-mail):** We use SendGrid from Twilio for reliable email sending, where SendGrid's security measures meet industry standards, including advanced encryption and continuous monitoring to ensure the integrity and confidentiality of your communication. Your data is safe, allowing you to use our services with confidence.
   See also: https://sendgrid.com/en-us/policies/security

What can you do yourself?

It's important to note that security is a shared responsibility. While we and our partners do our best to keep your data safe and provide robust security measures, you as a customer also need to do your part to maintain your own security. This includes, for example, using secure passwords and, if applicable, proper use of password managers, two-factor authentication, managing access rights, virus and malware protection, etc.

Practical tips

We are committed to the security of your data and encourage you to actively contribute to this security. Here you'll find practical tips and recommendations to optimally protect your data:

1. **Use strong passwords:** Create complex passwords with a password manager for extra security and convenience.
2. **Install antivirus and anti-malware:** Protect your device against malicious software and viruses.
3. **Be vigilant about phishing:** Avoid clicking on suspicious links and do not carelessly disclose your information.
4. **Update your devices:** Keep your devices and browsers up-to-date to prevent security vulnerabilities.
5. **Secure your network:** Use secure network connections, especially in public spaces.
6. **Data backup:** Regularly back up important data.
7. **Limit access:** Grant only the necessary access rights within your team.

Incidents and Feedback

At MinuteTrack, we highly value the security of your data and your experience with our platform. We understand that security is a dynamic field and that our users play an essential role in keeping our ecosystem safe. Therefore, we encourage you to actively participate in our security culture by providing feedback or reporting security incidents.

How to report feedback or indicents?

If you have comments about our security measures, want to make suggestions for improvements, or wish to report a potential security issue or incident, you can contact us directly via:

Phone: +31 (0)88 505 4330

E-mail: support@minutetrack.app

We take all feedback and reports seriously and are committed to a swift and effective response. Our team carefully reviews each report and will take immediate action if necessary to address the reported issues.

What happens after your report?

1. **Assessment:** Your report is evaluated by our specialized security team.
2. **Communication:** We keep you informed about the status of your report and inform you of any actions taken.
3. **Action:** If necessary, we take action to address the problem and ensure the safety of our platform.
4. **Feedback:** We appreciate your involvement and may, if applicable, provide feedback or recommendations to prevent similar incidents in the future.

Your proactive involvement not only helps us identify and address potential security risks but also strengthens our collective commitment to a safe and reliable digital environment. Together, we work towards maintaining a secure and trusted platform for everyone.