TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

As an industry leading customer success solution provider, we understand that our clients are entrusting us with sensitive and confidential business data. To that end, we are committed to support industry leading security practices, to ensure our customers' information is kept safe.

Totango has based our security management practices on the ISO 270001 standard for information security management systems (ISMS). By following this framework, our team performs the following high-level activities on a regular basis:

- Performing regular security reviews internally and with external auditors to ensure ongoing governance and risk mitigation
- Performing ongoing monitoring and analysis of our network infrastructure to detect threats and suspicious activities
- Performing ongoing and onboarding security training for our staff
- Practicing secure development and ongoing security thread analysis on our software and infrastructure

Following are key practices and principles of our security programs

Data Center & Physical Security

Totango is hosted on Amazon Web Services infrastructure (AWS), an industry leading provider of data center. AWS provides a rich set of security and compliances for their data-centers as explained on their website.

This includes physical security and environmental controls to ensure the data is kept safe from human attack and environmental hazards.

Data access and Encryption

All customer data stored in Totango is encrypted using strong encryption. This related to both "in-flight" (network traffic) and "at rest" (stored on disk) data.

Only our technical staff has access to customer data, and our team is training to review custom data only for the purpose of troubleshooting in relation to a customer support case. Access to custom data is audited and we review these logs regularly to ensure compliance. Technician level access to data is only possible using secure connection and multiple factor authentication (MFA).

Secure Software Development

Any new feature and product enhancement we implement goes through a security review during design. Additionally, any code committed to our code base goes through a code-review process ensuring code quality and adherence to standards. We also perform regular penetration testing and automatic scanning to validate no security vulnerabilities exist in our platform.

Network Security

Our data center is protected with firewalls, shielding customers from attacks or scans. Technician level access is only available through our VPN, requiring two layers of authentication (MFA) just to gain basic network access.

System Monitoring, Logging and Alerting

We perform extensive monitoring and logging of our servers and the application running on them. This includes monitoring of basic server metrics (CPU, memory), access logs and application-level logs. All telemetry data is centralized and we an extensive alerting framework to be alerted of any critical item

Backup

All customer data is backed up daily. Backup data is stored securely, in an encrypted fashion in our Amazon data center. We perform regular restore tests to ensure our backup procedure is sound.

Employee Training and Security

Totango technical staff goes through security training when upon joining our organization and at least annually during regular training. All employee computers and laptops are centrally managed to ensure critical OS and application patches are installed, antivirus software is properly running and configured, strong login passwords and disk encryption are enabled, and other critical policies to ensure employee devices are kept secure.

All employees go through background and reference checks upon hiring, as allowed by local employment rules.

Compliance

Totango is ISO-27001 certified and uses that as our security framework. Additionally, our hosting provider AWS has obtained the relevant compliance levels as listed here.

Need more info?

We care deeply about security and are happy to engage clients with additional information.
Feel free to reach out at security@totango.com to get in touch!