CTOUCH® The power to engage SOFTWARE SECURITY

Security is at the basis of CTOUCH software development

We go to great lengths to keep your data safe. Industry-accepted best practices and frameworks form the foundation of our security baseline. This baseline is developed by Grant Thornton and is updated periodically. Our employees are trained to make sure our hardware and software products stays in-line with the security baseline.

CTOUCH general software security principles

The CTOUCH security baseline is based on the concept of defense in-depth: securing your data at every layer, using multiple specific principles and controls. Such principles in the baseline include:

- Secure by design
- Secure by default – most secure default settings for all CTOUCH software
- Zero trust & least privilege principles
- Regular (third-party) auditing
- App vetting process using MobSF for third-party compliance to our security standards

CTOUCH compliance certifications & regulations

CTOUCH is front-runner in our industry in terms of security of our screens and software. We use broadly recognized security standards and periodically verify our adherence to these standards.

CTOUCH certifications and attestations

Adherence to GDPR standards

Verified by Grant Thornton

ISO IEC 27001 certified

From Summer 2023 onwards

Adherence to German data protection act

Conforms to Auth0 protocols

CTOUCH Sphere – device management

CTOUCH Sphere is the device management web application that lets you manage all your CTOUCH touchscreens remotely. That way, CTOUCH touchscreens can be kept up to date, safe and secure. We employ a robust set of specific security and data protection principles in Sphere, ensuring that you can use and manage our products with ease of mind.

CTOUCH® The power to engage

SOFTWARE SECURITY

Identity & access management

Device management within Sphere starts with identity controls. We use the security principle of least privilege to assign a user type. By default, all users receive a customer user profile. A reseller can then request a user profile update, which is verified and approved by CTOUCH. In order for the reseller or CTOUCH to access customer's touchscreens hardware settings remotely, the customer must give explicit approval for access within Sphere. So, the user is in control of the settings they share.

IDENTITY & ACCESS CONTROLS

- Session duration
- JIT Privileged Access Management
- Password controls using Auth0
- Single sign-on and two-factor authorization option

Data protection

By default, CTOUCH encrypts confidential data at rest and in transit as part of our foundational security controls. We use hashing and salting encryption to ensure your passwords are only known to you. All Sphere data is stored in Germany – employing the highest storage security standards in Europe.

DATA PROTECTION MEASURES

- HTTPS and WSS protocols
- Decryption in security key vault on Azure server
- Active vulnerability identification & management
- Automated security testing with Azure services

Data logging & storage

CTOUCH does not collect any personally identifiable information in Sphere or on our touchscreens. Recorded data from your screens that is visible in Sphere is not visible to CTOUCH personnel, unless CTOUCH manages your account – this must be explicitly confirmed by the customer in the Sphere settings. Recorded data will never be shared with third parties.

RECORDED DATA

- Latest display settings are logged
- Daily energy usage per screen is logged
- Only email address and company name are used for the Sphere account
- Aggregated product and service statistics