



APPLICATION NOTE i3TOUCH SECURITY

CONTENTS

1.	Introduction.....	1
2.	i3TOUCH device security.....	1
2.1.	Firmware & software installation and updates.....	1
2.2.	User profiles.....	1
2.3.	Personal user data.....	1
3.	Secure Communications & Cloud App Hosting.....	2
3.1.	Data encryption & Data Protection	2
3.2.	Infrastructure	2
4.	Notice	2

1. INTRODUCTION

This document describes the security aspects of the **i3TOUCH** and **i3SIXTY** display series and related solutions like **i3STUDIO**.

2. i3TOUCH DEVICE SECURITY

2.1. FIRMWARE & SOFTWARE INSTALLATION AND UPDATES

The **i3TOUCH** displays devices leave the factory pre-installed with approved firmware and software. Further updates and upgrades all happen automatically without the need for user manipulation, substantially reducing the risk of (un)intentional wrongdoing and security breaches. During the first boot we offer a setup wizard to allow non-technical personnel to configure the basic parameters of the display (language, date & time, network, enrollment into remote management, ...). Furthermore, users can define their UI preferences (quick launch buttons on the home screen, theme, ...). More complex settings are hidden for ordinary users and require in-depth knowledge and access rights.

No hidden “backdoor” communication or test routines have been implemented into the devices.

2.2. USER PROFILES

i3-Technologies has developed a system of user profiles that allow the segmentation of users into administrators, ordinary users and guest users, all but the latter protected by user names and passwords. This allows organizations to reduce the rights of ordinary users to change settings on the display.

2.3. PERSONAL USER DATA

No personal user data is stored on the display.

Screen captures of whiteboarding and annotation can be shared locally and or stored on user-protected network storage, if they wish so. Locally shared screenshots are removed from the system with a 4h expiration period.



3. SECURE COMMUNICATIONS & CLOUD APP HOSTING

3.1. DATA ENCRYPTION & DATA PROTECTION

Network security is important to i3-Technologies. Therefore, all external network communication is being encrypted (e.g. using HTTPS protocols and TLS) using 256-bit AES.

User passwords are never stored in machine readable version and user data is not accessible for 3rd parties.

Backups of data are also being stored in encrypted format.

Our internal IT security policy forbids unauthorized access to this servers and databases, and restricts unauthorized personnel from copying and/or distributing this information. Strict access management shields all environments, databases and infrastructure from unauthorized access.

3.2. INFRASTRUCTURE

i3-Technologies relies on major IP service providers for hosting its cloud infrastructure to ensure that best practices and high standards are being applied to service and data management.

In particular, i3-Technologies' cloud hosting infrastructure is based on Amazon Web Services (AWS) and hosted in an Amazon data center in Ireland. This high-end infrastructure meets the latest security and data privacy standards. This means that all data traffic between the i3-Technologies' display application and the server is being encrypted and only a limited amount of people has access to the infrastructure. These individuals have no means to download, decrypt nor read sensitive information that resides on the server.

For remote connectivity and mailing services i3-Technologies uses the infrastructure of other trusted providers like Twilio and its Sendgrid subsidiary. They only provide connectivity or processing services, not user data is stored.

For access and identity management ('user profiles' in **i3RDM** and storing the cloud management credentials in **i3WHITEBOARD**) we make use of accredited and secure 3rd party service supplied by auth0.com.

Hence, you as a customer can benefit from the i3-Technologies' solutions and remain confident that your data is compliant with core security and compliance requirements such as data locality, confidentiality, and protection.

4. NOTICE

i3-Technologies' products are constantly evolving to improve customer functionality and user experience. This means that the effectively used cloud services and servers might evolve over time. Efforts have been made to check that information provided here to be correct and complete at the time of publication, subject to change without prior notice.