Privacy Policy

INTEGRA CONTROL is a mobile application and supplementary product offered for the family of alarm control panels called **INTEGRA**. It was created by **SATEL Sp. z o.o,** to provide to our **Customers,** useful and modern application client offering: secure access, remote control and visualization of the state of the alarm control panel installed in Customer's premises.

The **Application** is provided by SATEL Sp. z o.o at no cost and is intended for use as is.

This page is used to inform our **Customers** regarding our **Privacy Policy** if anyone decided to use our Application. The Privacy Policy is also accessible at INTEGRA CONTROL mobile application.

If you decide to use our Application, then you agree to the collection and use of information in relation with this policy. The **Information** that we collect are used for providing and improving our Application. We are not using or sharing customer's information with anyone except as described in this Privacy Policy.

Information Collection and Use

There are two ways of realizing End-to-End communication between INTEGRA CONTROL application and alarm control panel:

Case 1: Direct P2P network connection,

Case 2: Indirect network connection realized through communication servers.

In both cases, End-to-End communication between your alarm control panel and mobile Application client(s) is realized over the network with the use of secured transport protocols.

In case of Indirect network connection, End-to-End communication is also realized with the use of secured transport services hosted on dedicated communication servers. Those dedicated servers belongs to and are maintained by SATEL Sp. z o.o.

If you decide to use our Application to achieve remote connection and visualization of the state of your alarm system, then you agree to initialize the application client with the following information:

Case 1: Direct P2P network connection

IP address or URL representing your alarm control panel, communication **PORT,** the **User Password** representing the user account in your alarm control panel and the **GuardX key** needed to open communication channel with your alarm control panel. This set of data is entered in Application and stored in Application's resources, locally on your device. This set of data is enough to establish connection with your alarm control panel.

Case 2: Indirect network connection realized through communication servers.

MAC Address, **ID** of alarm control panel, the **User Password** representing the user account in your alarm control panel and the **GuardX key** needed to open communication channel with alarm control panel. This set of data is entered in Application and stored in Application's resources, locally on your device. This set of data is enough to establish connection with your alarm control panel.

Details:

- **IP address** or **URL** and **PORT** are representing communication with your alarm control panel and identifying your alarm control panel in network.
- **MAC Address** is an identifier assigned to alarm control panel at manufacturing process. MAC is used to identify your device in the network and in our system. MAC is presented on the product labels in clear.
- **ID** of alarm control panel is generated by our servers and assigned to the device while requesting and initializing the connection between alarm control panel and server. ID is stored in protected manner. ID can be retrieved using user functions available in the alarm control panel upon valid authentication of the user.
- **User password** is only known to you and your alarm control panel. This password is needed to access your user account in your control panel. This is not mandatory data. Without entering this data, the customer won't have access to functions related with his account. Customer will only have and access to virtual keypad which is representing the same functionality as real keypad installed in the alarm system.
- **GuardX key** is a private key, defined by the administrator of alarm control panel while configuring communication channel. This key is stored in memory of alarm control panel. Can be retrieved using dedicated service function available only in service mode of alarm control panel or by dedicated software called DLOADX used to configure the alarm system. On application side it has to be entered manually by the user.

Note: SATEL Sp. z o.o. does not have complete set of data which would allow to establish connection to your alarm control panel. On Customer's side, above set of data is stored in application's resources on your device. Additionally, in Application, you can set password which will be used to verify access rights to Application and to data stored in resources of Application.

Established End-to-end communication means continuous transportation of secured data from alarm control panels to customer's Application to exchange configuration of the alarm system and to get the state of alarm system through the following functionalities: checking system status, checking zone status, checking output status, viewing current troubles, viewing all system events.

SATEL Sp. z o.o. does not collect any transported data realized via End-to-end communication. The data is only kept in customer's alarm control panel and mobile Application. Our communication servers are only representing transport layer.

If you decide to activate PUSH messaging in Application client, then you agree that identifier of your device, on which the Application is installed, will be collected and used by us to provide PUSH messaging service. Tokens representing instances of Applications using PUSH service are stored in databases of our servers. The configuration of PUSH messaging service is stored in Application's cache. With this data SATEL Sp. z o.o. is not able to identify the customer.

Our Application is using QR codes to ease the import of data, needed for initializing the connection with your alarm control panel. The same functionality is used to export the data of alarm control panel to other instance of your Application, on another device.

If you decide to use our Application to scan QR code and to import alarm control panel's data via QR code, then you agreed to use your device's camera. Note that our Application uses camera only for QR code scanning.

The user data stored in QR code is not presented in clear. The QR code is generated once per exchange session and protected with session key. Session key is defined by the user and is not exchanged within our Application. While reading the QR code with Application on destination device, you will be prompted to enter exact session key.

Our Application does not use third party services that may collect an information used to identify you. Our Application does not use and does not collect any data which could be assessed as sensitive.

Log Data & Analytics

If you decide to use our Application, then you agree that the following analytics technologies are in use: **Google Analytics** and **Crashlytics** (part of Fabric, which has been acquired by Google). To learn more about Google Analytics's privacy policy, visit: http://www.google.com/analytics/learn/privacy.html. To learn more about Crashlytics's privacy policy, visit: http://try.crashlytics.com/terms/

We use these technologies to collect anonymous data to help us understand how you use our Application. These tools help us learn how to make our Application better in use. These technologies can tell us what functions of our Application you are using. They also provide us with general information about where in the world our Application is used and what language version our customers are using.

We want to inform you that whenever you use our Application, in case of an error in the Application, Crashlytics can process the error reports stored as Log Data on your device. This Log Data may include information such as: Device name, Operating system version, Application version, the time and date of use of Application. The Log Data is only collected to allow us to lead development and improvement processes for our Application.

Cookies

Cookies are files with small amount of data which may include an anonymous unique identifier. These are sent to customer browser from the website that you visit and are stored on Customer device's internal memory.

Our web site are using cookies to collect information and to improve our Services. You have the option to either accept or refuse these cookies, and know when a cookie is being sent to

Customer computer. If you choose to refuse our cookies, you may not be able to use some portions of our Service.

INTEGRA CONTROL application does not have any reference to any of our web sites so it doesn’t use cookies.

Links to Other Sites

INTEGRA CONTROL application does not have any reference to any urls.

Security

We value Customer trust in providing us the data described above in this Privacy Policy, thus we are striving to use commercially acceptable means of protecting it. But remember that no method of transmission over the internet, or method of electronic storage is 100% secure and reliable, and we cannot guarantee its absolute security.

Changes to This Privacy Policy

We may update our Privacy Policy from time to time. Thus, you are advised to review this page periodically for any changes. We will notify you of any changes by posting the new Privacy Policy on this page. These changes are effective immediately, after they are posted on this page.

Contact Us

If you have any questions or suggestions about our Privacy Policy, do not hesitate to contact:

SATEL Sp. z o.o.
ul. Budowlanych 66
80-298 Gdańsk, Poland
satel@satel.pl

Made to Protect
http://www.satel.eu/