Data Security and Privacy

atfrontdesk.com

Inside - the App at your front desk

We get it. We understand your data is private and sensitve.

Privacy

Your privacy is very important to us. It is not our business to know your business. It is our business to help you succeed in your business.

We need to know:

- Unique email address and a password for the account
- That you have paid for the license of our software
- We will use your email only to notify you of issues regarding Inside, such as resetting passwords, feature upgrades, etc.

Accordingly, we have developed this policy in order for you to understand how we collect, use, communicate and disclose and make use of personal information.

We promise the following:

- We will not share or sell any your corporate data, ever. It's your data, they belong to you.
- We will not make contact with your visitors or employees without explicit permission.
- We will protect all account information by reasonable security safeguards against loss or theft, unauthorized access, disclosure, copying, use or modification.

We are committed to conducting our business in accordance with above principles in order to ensure that the confidentiality of corporate information is protected and maintained.

GDPR

There are two key roles in the context of GDPR.

Data Controller: You are considered the data controller because you decide how and what data to collect.

Data Processor: We are considered the data processor because we process your data collection on your behalf.

As a Data Processor, we have added the following features to our service so our customer can purge the data if necessary.

- Deleting individual visits
- Deleting visit records based on the date range
- Deleting visitor records and cascading visit records

If you ever discontinue the service with us, you can export and purge all visitor data before you leave.

We would like to let you know once the data is purged, we cannot retrieve the data. So please use caution when deleting the data.

Billing/Credit Card Information

We use Recurly as our subscription/billing service provider. We do not store any credit card information in our servers. Cardholder data is sent directly to Reculry to minimize risk. Recurly is PC-DSS Level 1 compliant, and recognized on the Visa Global Registry of Service Providers. For more information on Recurly's security, visit Recurly's website.

Servers and Network Protection

Inside servers and services are hosted in the AWS. Private networks are strictly segmented according to function. Restrictive firewalls protect communication entering the network and between private networks. All access to Inside servers are logged. Audit logs are kept a minimum of 365 days. Network penetration tests are performed on a regular basis. Our servers and databases are backed up daily.

Data in Motion

Any data moving between your iPad, AWS, and Reculy is encrypted using TLS protocol. We do not use SSL which is know for its vulnerability.

Data Retention

We store your data in our database indefinitely. You may purge your data yourself from the enterprise interface. If we ever change our retention policy, we will notify you well in advance.