# Privacy and Security

At Kenai, we have a strict policy regarding the privacy of sensitive customer data: we will never sell your visitor or employee data, and we will not contact your visitors or employees without their explicit permission. Our support team will only access your account in the event of a technical support issue that requires real-time access.

## Secure and trusted infrastructure

Kenai does not independently maintain, host or transmit customer data. Such data resides with Amazon Web Services ("AWS") secure cloud services platform. AWS continually maintains a high bar for security and compliance across all of their global operations. Their industry-leading security is evidenced by their long list of internationally recognized certifications and accreditation which demonstrate compliance with rigorous international standards. Such certifications include ISO 27017 for cloud security, ISO 27018 for cloud privacy, SOC 1, SOC 2 and SOC 3 and PCI DSS Level 1 amongst others. AWS also complies with the CISPE Data Protection Code of Conduct for Data Protection in the Cloud.

### Storage and transmission

All customer data is transferred securely using HTTPS (TLS protocol with perfect forward secrecy) from the app and Kenai dashboard to the cloud and servers (which are secured per AWS security protocols described above). At rest, data is encrypted using 256-bit AES Server-side Encryption using secured encryption keys managed by AWS Key management service.

### Access to the Dashboard

Access to the dashboard is restricted to authenticated users. Users are authenticated via OIDC compliant OpenID connect flows and backed by Auth0 as identity provider. Once successfully authenticated, users are authorized via OAuth tokens which restrict user access to company specific data and enforce role-based administration.

# Data privacy by design

Kenai is a company founded in an era where data privacy is a primary concern to both individuals and the companies that serve them. As a result, securing data is built into the fabric of Kenai itself.

Kenai secures visitor data by only surfacing their details if they originally opted to be remembered at a client on the Kenai Network and then:

1. Are recognized with facial recognition (or another verification method) at that same location; or
2. Verify their mobile number with a one-time pin at that same client but at a different location.

This is more secure than alternative systems which surface personal information on the device after entering the email or searching through the names of previous visitors to facilitate returning sign-in. It also means visitors can securely enjoy the convenience of not having to re-enter their personal information anywhere on the Kenai Network.

Kenai is the only visitor management system in the world that provides returning visitors with the convenience of being remembered, whilst ensuring that their personal information is only ever surfaced to them and the company they are visiting.

Employee data is only surfaced through:

1. Authorized access to the company dashboard,
2. Internal notifications to company administrators
3. For onsite identification (as specified by the company) through the Kenai Covid-19 Screening app.

## Data environment

All data is stored on a company segmented AWS shared environment to facilitate visitors accessing their data across the network with their mobile number and one-time pin. Access to information regarding visitor or employee sign-in/out (transactional data) is strictly limited to the company where they signed-in/out. Visitors' transactional data is never shared across companies.

## Personal information on iPad

While the iPad or Android device is connected to the internet, the visitor's or employee's personal information is only stored on the device for the duration of the sign in process, before being synced to Kenai.

If the iPad or Android device is disconnected from the internet, visitors can continue to sign in, and their data will be securely stored locally in an encrypted format protected by iOS keychain managed encryption keys. As such, if the devices are ever stolen, there is no loss or breach of data.

Upon re-establishing internet connectivity, all encrypted locally stored visitor data will sync to Kenai (and be removed from the device itself).

## Data subject rights

If you are a visitor or employee at a location where Kenai is installed, you are subject to the Terms of Use and Privacy Policy of the particular company where you are visiting or employed. Kenai facilitates full transparency of our client's Terms and Privacy Policy by provisioning a visitor or employee agreement screen where this information can be disclosed and consented to by the visitor or employee. We also provide our clients with the ability to delete and employee data, should they be required to do so.

Kenai has enacted policies to protect visitors' rights. We allow Kenai visitors to opt-out of being remembered on the Kenai network with a simple toggle switch when finalizing the sign in process. If at any stage a visitor opts out of being remembered, Kenai will automatically remove their profile from the Kenai Network. It is important to note that removing a visitor's profile from the Kenai Network does not result in the log of that visitor being removed from our client's dashboard. As such, the client still has access to the log of visitors that have entered the building (for safety and security reasons), while giving their visitors the option to opt out of the broader Kenai Network.

Kenai has enacted policies to protect visitors' rights. We allow Kenai visitors to opt-out of being remembered on the Kenai network with a simple toggle switch when finalising the sign in process. If at any stage a visitor opts out of being remembered, Kenai will automatically remove their profile from the Kenai Network. It is important to note that removing a visitors profile from the Kenai Network does not result in the log of that visitor being removed from our clients dashboard. As such, the client still has access to the log of visitors that have entered the building (for safety and security reasons), while giving their visitors the option to opt out of the broader Kenai Network.

# Client access to data

## Permissions

Role-based administration allows clients to provide the right dashboard access to the right employees. Kenai currently provides three admin roles:

1. Global Admin
2. Local Admin
3. Front Desk User

Global Admin have read and write access to the full visitor history, the user log (complete record of client login activity) and the device configuration across all company locations. The Local Admin has the same rights as the Global Admin but limited to a single location. The Front Desk User have read only access to a limited history of the visitor log (past 12 hours) to facilitate the daily safety and security processes of the building.