CommuniBee Security & Privacy

This document outlines the security and privacy considerations in the CommuniBee app.

Privacy

Our philosophy when it comes to privacy is to collect as little information as is necessary (typically only email addresses as usernames), and to never share that information with any 3rd party except for the purposes of enhancing our service. For details, see the privacy policy posted on our web site:

> https://communibee.ca/privacy-policy/

Server Security

- API and database server are running Ubuntu 18.04, a Long Term Support version supported out until 2023.
- Server runs UFW firewall locked down with IP whitelisting as needed for developers to access.
- All communications are done over HTTPS with RSA 2048-bit encrypted SSL.
- Database can only be accessed by API, blocked by firewall rules from anything but API
- Database is running the latest version of Microsoft SQL Server, and API is running the latest .NET Core runtime for Linux.
- All database access uses Entity Framework to mitigate SQL injection attacks.
- All passwords used for accessing the server are strong, randomly generated strings.
- Database is backed up daily.
- User passwords are properly hashed so they cannot be extracted and reverse engineered.

Application Security

Communities within CommuniBee can be flagged as discoverable or not. If discoverable, like Edmonton Community Leagues are, users are presented a drop down of available communities to join. If not discoverable, guests need to either be given an invite code that they enter to join a community, or they can be invited directly by an admin through the dashboard.

Additionally, the ability to join can be configured in the app with three levels:

1. No Approval Required – anyone with invite code can join and has immediate access.
2. Approval Always Required – people join with an invite code and enter a pending state until approved by an admin.
3. Email Domains Auto-Approved – admins can add approved email domains. When users register with such a domain they are automatically approved, otherwise they enter a pending state as in #2.

User access can be controlled by admins from the dashboard at any time, revoking or granting access to members of the community.

Access privileges are calculated on the app side for speed, but also on the API to prevent circumvention. We use signed JWT tokens for authentication with anti-forgery checks.

Payment Security

For payment we use Stripe (https://stripe.com/), which is a bit of an industry standard for online credit card processing. It is used by many recognized names like SalesForce, Expedia, OpenTable, Spotify, etc.

When a payment is made in CommuniBee, a dialog is presented to collect payment information (credit card #, expiry date, CVV), and that information is passed directly to Stripe along with the email address of the account. It is important to note that the credit card information is never passed to or stored on our servers.

When Stripe approves the payment, a token and client ID is returned and then passed to our server. Our server then contacts Stripe with that token to validate the payment, and this finalizes the transaction. If auto-renew is toggled on, the CommuniBee system can use the client ID to process a renewal payment without requiring the card information again.

Infrastructure Security

We use Digital Ocean for hosting the server and database. Digital Ocean is one of the leading providers of hosting services. The servers we use are hosted on Canadian soil in Toronto.

For details on Digital Ocean’s data security practices, visit:

https://www.digitalocean.com/legal/data-security/

An excerpt from that page:

Security controls provided by our datacenter facilities includes but is not limited to:

- *24/7 Physical security guard services*
- *Physical entry restrictions to the property and the facility*
- *Physical entry restrictions to our co-located datacenter within the facility*
- *Full CCTV coverage externally and internally for the facility*
- *Biometric readers with two-factor authentication*
- *Facilities are unmarked as to not draw attention from the outside*
- *Battery and generator backup*
- *Generator fuel carrier redundancy*
- *Secure loading zones for delivery of equipment*