GROUNDFLOOR

Information Security at Groundfloor™

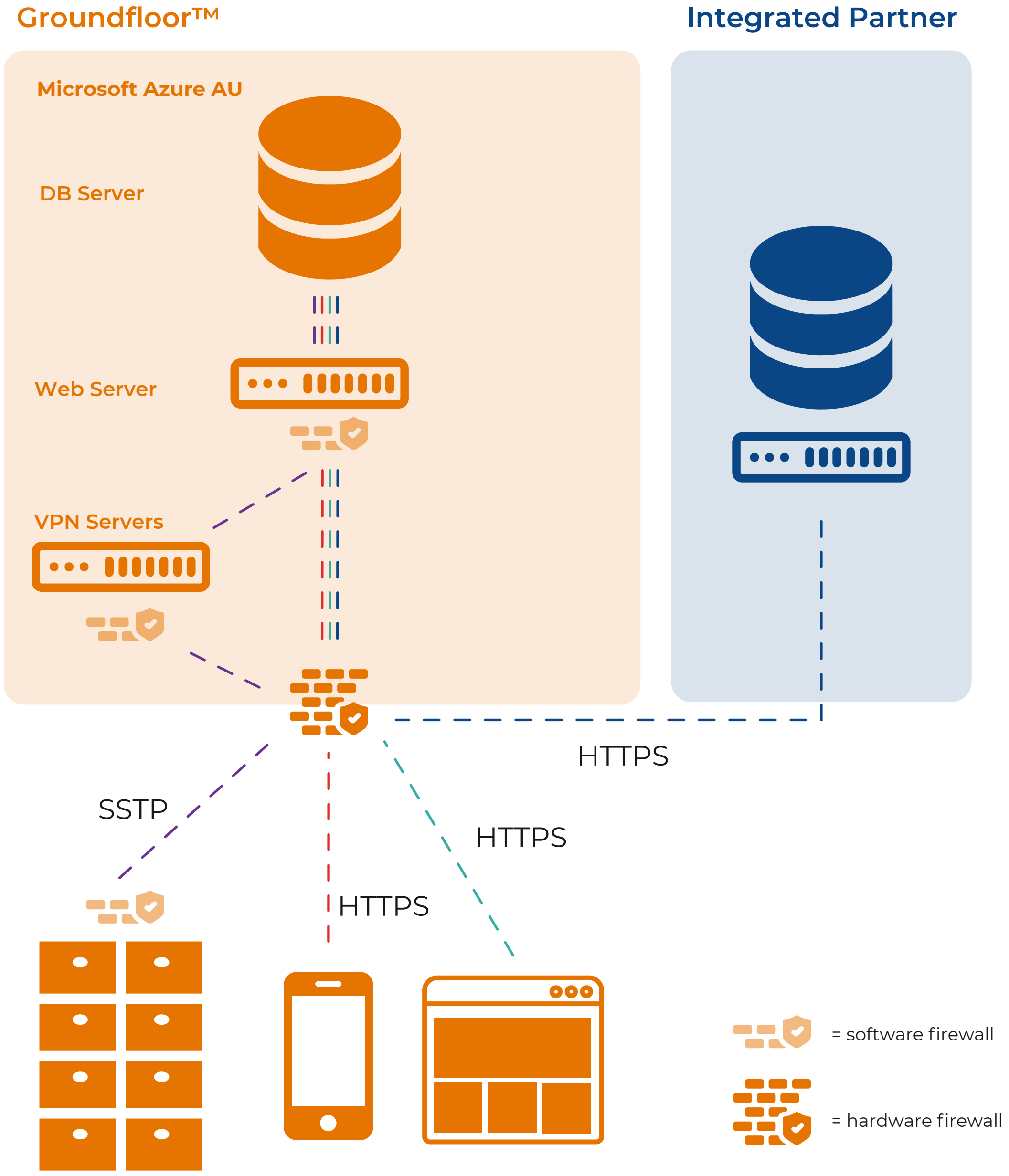
Groundfloor™ takes all precautions to ensure protection of our customers' data.

We host our data and applications in Microsoft Azure in the Australian East and South East Regions. The Azure SQL Server is not directly accessible, with only our Web Server and VPN Servers able to connect to it.

Any personally identifying data is encrypted at rest as well as ALL data being encrypted in transit. Groundfloor™ requires the use of HTTPS for all services including our admin portal, mobile apps and APIs.

Our system does not require access to any of a customer's internal network, but may at your request integrate with another software vendor over secure protocols via our API Gateway.

Our lockers connect to our VPN server through a SSTP VPN on port 1723. For monitoring and management of the lockers we also utilise these ports: HTTPS(443) TCP(8883) UDP(3544).



Updated: May 2021

Security Policy Continued...

Access Controls

Groundfloor™ utilise user-based access controls to restrict visibility and functionality to only those who require it.

Users with access are:

Groundfloor™ staff & sub-contractor (a Singaporean software vendor with enterprise and government clients)

- Who provide customer support – YES
- Who develop and test our software – YES
- Any other staff (such as installers or sales only) – NO
- API keys are stored encrypted and not visible in our portal

Customer Facility Management staff

- Staff requested as Admin users at system setup – YES
- Staff requested as Admin users by either primary contact – YES
- Any other customer staff – NO
- Any customer residents – NO

Courier staff/company

Only to the extent required to make a delivery. This includes showing registered couriers matching names:

1. When they are making a delivery and begin to type a name
2. When they are making a delivery and type in the recipient's full phone number

Security Patches and Antivirus

Groundfloor servers are updated monthly with the latest security patches from Microsoft. Antivirus software is run on our system, with virus definitions being updated automatically as available.

Incident Response Plan

A Cyber Security Incident Response Plan is in place. Groundfloor™ commit to conducting assessments in line with the requirements of the NDB scheme and notifying any impacted customer and the Office of the Australian Information Commissioner of any 'eligible data breach'.

Insurance

Groundfloor™ maintains $5M Cyber Enterprise Risk Management policy. A copy of our certificate of currency is available upon request.

User Behaviour

Our kiosk, mobile apps and website utilise Google Analytics in order to understand user behaviours. This captures data about how users interact with our software, such as what was pressed, how long a user stayed on a page and the device used to access it. Understanding our user's behaviour helps us to continually improve our products.

Privacy Policy

The latest version of our privacy policy is available at: https://groundfloordelivery.com/privacy-policy/