Security Policy

Section 1 - Overview

1. We take all reasonable steps to keep secure any information that we hold about you. Here is a summary of what we do to guarantee your data is safe with Wesurance.

Section 2 - Backups/ Disaster Recovery

1. Backups are replicated everyday in the same data centers in order to meet Disaster Recovery objectives.
2. Wesurance will keep a full backups of each deactivated account for up to 12 months.

Section 3 - Database Security

1. All data related to your customer is stored in a dedicated database and converted into unrecognisable code using industry standard data encryption.
2. Data access control rules implement complete isolation between customer databases running on the same cluster, no access is possible from one database to another.

Section 4 - Password Security

1. Customer passwords are protected within Amazon Cognito is encrypted at rest in accordance with industry-standard.
2. Wesurance staff does not have access to your password, and cannot retrieve it for you, the only option if you lose it is to reset it.
3. Login credentials are always transmitted securely over HTTPS.

Section 5 - Staff Access

1. Wesurance helpdesk staff and engineers may sign into your account to access settings related to your support issue with limited and reasonable manner. For this they will use their own special staff credentials and not your password (which they have no way to know).
2. Our Helpdesk staff strives to respect your privacy as much as possible, and only access files and settings needed to diagnose and resolve your issue.

Section 6 - System Security

1. All servers are running in Amazon AWS cloud in Linux base with up-to-date security patches.
2. Installations are ad-hoc and minimal to limit the number of services that could contain vulnerabilities (no PHP/MySQL stack for example).
3. Only a few trusted Wesurance engineers have clearance to remotely manage the servers, and access is only possible using an encrypted personal SSH keypair, from a computer with fulldisk encryption.

Section 7 - Physical Data Location

1. The servers are hosted in trusted data centers in various regions of the world (e.g. MongoDB, AWS). It should be closest to where you are based, and you can request a change of region (subject to availability).

Section 8 - Credit Card Safety

1. We never store your credit card information in our systems.
2. Your credit card information is always transmitted securely and directly between you and our PCI-Compliant payment acquirers. (Please refer to our Privacy Policy page)

Section 9 - Communications

1. All data communication to client instances are protected with state-of-the-art TLS1.2 SSL encryption (HTTPS).
2. All internal data communications between our servers are also protected with state-of-the-art encryption (SSH).
3. Our servers are kept under a strict security watch, and always patched against the latest SSL vulnerabilities, enjoying Grade A SSL ratings at all times
4. All our SSL certificates use robust 2048-bit modulus with full SHA-2 certificates chains.

Section 10 - Network defense

1. All data center providers used by Wesurance have very large network capacities, and have designed their infrastructure to withstand the largest Distributed Denial of Service (DDoS) attacks. Their automatic and manual mitigation systems can detect and divert attack traffic at the edge of their multi-continental networks, before it gets the chance to disrupt service availability.
2. Firewalls and intrusion prevention systems on Wesurance platform help detect and block threats such as brute-force password attacks.