How Secure Is the Donesafe Platform?

As we hold a lot of private and sensitive information, security is our number one priority. We employ defence in depth to ensure our system is as secure as possible while also aiming to ensure a very fast system with a high level of availability.

Hosting Partner

All data is held in Australia with our hosting partner Amazon Web Services (AWS) based in Sydney. AWS data centres are housed in nondescript facilities. Australian data is not sent offshore. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilising video surveillance, intrusion detection systems, and other electronic means.

Encryption & Firewall

We use SSL on our system to ensure all traffic is encrypted and also encrypt all data in the system at rest. We use server hardening, port blocking, a physical firewall and have installed an intrusion detection system to protect our system and your data. We engage an independent third party to conduct regular penetration testing on our system to ensure ongoing security.

Physical Security

AWS data centres are housed in nondescript facilities. Data will be primarily held in AWS Sydney data centre. Australian data is not sent offshore. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilising video surveillance, intrusion detection systems, and other electronic means. Authorised staff must pass two-factor authentication a minimum of two times to access data centre floors. All visitors and contractors are required to present identification are signed in and continually escorted by authorised staff.

How Secure Is the Donesafe Platform?

Secure Client Systems

Donesafe separates clients on a per request level to filter our clients. Furthermore Donesafe segregates client data into separate database schemas meaning all clients are logically walled from each other. In practice this means:

1. Clients can not authenticate to other domains.
2. Client information is scoped to that client alone, there is no shared application data between clients.
3. Client customisations are constrained to a particular subdomain.
4. Client requests are separated at the network level
5. Account level data is separated from client operational data and therefore information about other clients cannot leak between clients.

Data Loss Protection

Our hosting environment is protected with a Data Loss Prevention system. Actively managed monitoring tools are designed to detect unusual or unauthorised activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorised intrusion attempts.

Donesafe backup and availability

Archiving and Backup

Donesafe leverages Amazon Glacier under a document Information Security Management Framework for data archiving and backup.

Objects (or archives, as they are known in Amazon Glacier) are optimised for infrequent access, for which retrieval times of several hours are adequate.

Amazon Glacier is designed for the same durability as Amazon Simple Storage Service (Amazon S3).

Amazon S3

Amazon S3 provides a highly durable storage infrastructure designed for mission critical and primary data storage. AWS provides further protection for data retention and archiving through versioning in Amazon S3, AWS multi-factor authentication (AWS MFA), bucket policies, and AWS Identity and Access Management (IAM). We also use Amazon's RDS functionality in a Multi-AZ configuration meaning client data is automatically replicated to another location in Australia to increase our availability.

Disaster Recovery

For disaster recovery (DR) Donesafe has chosen a single site warm standby solution in AWS which allows for a scaled-down fully functional version of the Donesafe environment running in the cloud. This decreases the recovery time because some services are always running. In a disaster, the system is scaled up quickly to handle the production load.

As a modern SaaS provider we also store our environment configuration in the configuration management tool chef (see https://www.chef.io/) and use Amazon's cloud formation (see https://aws.amazon.com/cloudformation/) to provide the ability to spin up a complete environment in minutes.