HELM CONNECT
DATA SECURITY

Your data. Secure.

The security of your data is of the utmost importance to us. That's why Helm CONNECT is hosted on Amazon Web Services (AWS) – to provide the best level of security available, while ensuring you have constant access to your data from anywhere in the world, onboard or onshore. With Helm CONNECT, your data is protected by the best standards in IT security. Our progressive data policies use redundant backups, fail-over processes, and recovery approaches to ensure that your data is accessible and available even in the event of a disaster.

Powered by AWS

We host our client data on a Relational Database Service (RDS) instance on AWS. To protect your data, we take full advantage of AWS's data security features, we comply AWS established best practices, and we operate in accordance with ISO 27001 principles.

The IT infrastructure provided by AWS complies with many certifications and standards including:

- SOC 1/ISAE 3402, SOC 2, SOC 3
- FISMA, DIACAP, and FedRAMP
- PCI DSS Level 1
- ISO 9001, ISO 27001, ISO 27018

At Helm Operations, we follow Amazon's recommended best practices for security, network, storage, and backup and recovery wherever possible.

Security

- Proactively managing access to AWS resources and APIs using identity federation, Identity Access Management (IAM) users, and IAM roles.
- Implementing the most strict/least permissive rules for our security group.
- Use of Elastic Compute Cloud (EC2) instances which only allow local traffic and receive all outside requests via Elastic Load Balancer (which is the only object publicly accessible on the AWS System).
- Regularly patch, update, and secure the operating system and applications on your instance of Helm CONNECT.

Back up and recovery

- Use of Elastic Block Store (EBS) volumes and RDS servers with nightly snapshot backups for disaster recovery.
- Utilizing an RDS server with multi-availability zone mirroring so that it has no single point of failure.
- Use of an ephemeral/replicable web server that can easily be regenerated via running a single script. If the web server fails, then Helm's monitoring system notifies us so that we can generate another one nearly instantaneously. Once the new server is created the load balancer will immediately start directing traffic to your Helm CONNECT instance.