

DATA SECURITY + AVAILABILITY

Available, accessible, secure

Helm CONNECT makes one thing clear: your data is important. Using the best standards in IT security, we constantly work to ensure that your data is protected and always available to you, no matter the situation.

Always Secure

The security of your data is of the utmost importance to us. That's why we use multiple layers of the best measures in IT security—from in-app to our hosting provider to internal policies—to protect your data.

SECURITY MEASURES IN HELM CONNECT

There are several basic security measures built directly into Helm CONNECT that allow you to control which users can access specific data:

- > Role-based security
- > Limit access to client lists
- > Assign read versus edit rights
- > Assign user permissions based on usergroups

SECURITY MEASURES IN AWS

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.

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, and we use AWS-established best practices 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

SECURITY MEASURES THROUGH OUR GRC

At Helm Operations, we used Amazon's recommended best practices to develop our internal governance, risk management, and compliance (GRC) policies, tailored to fit our customers in the maritime industry:

- > We proactively manage access to AWS resources and APIs using identity federation, Identity Access Management (IAM) users, and IAM roles.
- > We use Elastic Compute Cloud (EC2) instances that only allow local traffic and receive all outside requests via Elastic Load Balancer (the only object publicly accessible on the AWS System).
- > For our hosted environments on RDS, security patches are handled automatically by AWS. We maintain asset and software registers for our internal systems and support and implement documented procedures to ensure patch management on all staff equipment according to ISO27001/2 standards.

ENCRYPTION

Web traffic to Helm CONNECT is secured using a TLS certificate issued by AWS's Certificate Authority. The following encryption types apply to HTTPS communications between customers and our servers.

- > RSA Encryption 2048 bits
- > SHA256 with RSA Encryption

AUDITS & STANDARDS

Volaris Security requires our participation in the Governance Risk Compliance (GRC) program. Our company is audited bi-annually against a set of 81 data security controls covering requirements from NIST, ISO 27001/2, SOC, PCI, and other regulations. All Volaris Business Units must participate in this program and undergo annual internal and external audits against this standard.

Always Available

We chose Amazon Web Services (AWS) as our hosting provider because AWS has been recognized as the leading major cloud infrastructure provider, sustaining an uptime percentage of 99.99% year after year. Building on the AWS infrastructure, we implement policies and procedures to limit system downtime as much as possible. Helm CONNECT has maintained a system uptime of greater than 99.99%, excluding updates and scheduled maintenance downtimes. With Helm CONNECT, your data will be there when you need it.

Always Recoverable

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.

AWS BACKUP PROCESSES

We fully utilize Amazon's industry-leading Multi-Availability Zone (Multi-AZ) functionality to ensure data redundancy and reliability, meaning that at least two copies of customer data are always maintained in parallel in separate availability zones. In the event of a failure in a single availability zone, fail-over to the remaining server occurs seamlessly and automatically, with a second replica of the data created in another availability zone to ensure ongoing redundancy. In the event of a complete failure or outage of one of Amazon's regions, we can further replicate data to another AWS region (for example, US West). We tested this process as part of our disaster preparedness procedures and know that it takes less than one hour to restore data to operational in such instances.

OUR BACKUP PROCESSES

In addition to the backup procedures provided by AWS, we routinely run our own backup procedure to ensure your data is always available:

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

LOCATION OF STORED DATA

Helm CONNECT uses a combination of file system and database storage at the AWS N. Virginia (us-east-1) location; however, we can offer various hosting locations globally.

DISASTER RECOVERY

To protect your data from natural disasters, we house Helm CONNECT's main data servers in AWS's Northern Virginia availability region – the same server system used by the US Government to protect sensitive government data. Our AWS hosting also protects Helm CONNECT and your data from any natural disasters that may impact our head office in Victoria, BC.

AWS HARDWARE FAILURE

In the rare event that AWS has a hardware failure, we automatically replicate the system data to a database mirror and launch a new web server immediately, ensuring that you have access to your data with minimal, if any, downtime.

Always Accessible

With Helm CONNECT, you own your data, and we promise you'll always have access to it.

EXPORTING DATA FROM HELM CONNECT

In addition to our API, data can also be extracted in-app through many different views. Many of the screens have "Print" or "Export to CSV" buttons, allowing users to export what they are currently viewing on the screen. Users also have access to a configurable in-app reporting tool to build reports based on data sources. Users can dynamically link these reports to third-party reporting or dashboarding tools, such as PowerBI or Tableau, with CSV connection strings.

QUITTING HELM CONNECT?

We hope you never leave, and we dedicate ourselves to keeping our customers happy and successful on Helm CONNECT. But one thing we'll never do is limit your access to your data.

As a subscriber, you can export all user-created data from Helm CONNECT in CSV or an Excel format at any time through our reporting tool. If you decide to leave, a full backup in JSON—a language-independent, open-source data format—can be made available at no charge. We can also export and convert your data to the data format of your choice for a small fee.