Gallagher Data Centre - Security Statement

Gallagher Group understands that partnerships need to be based on trust, transparency and security. These values are also reflected in our approach to information security with respect to the Gallagher Fuel System cloud products.

Cloud Hosting

Gallagher Group uses Amazon Web Services as the strategic hosting platform for cloud services including the Data Centre solution. Amazon Web Services is the industry leading supplier of cloud based hosting services including Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). Amazon Web Services implements a range of certifications and voluntary measures to ensure data privacy and compliance with industry data privacy standards. Please refer to this page for further information on the relevant certifications and standards implemented by Amazon Web Services.

Security Review

Gallagher cloud products directly benefit from the significant security engineering and in-house capabilities within Gallagher Security. We have a dedicated penetration test team that assesses and assures the security of the Gallagher products including Data Centre. The product is under constant review as part of our internal development program.

Managing Threats

The OWASP Top 10 and WASC Threat Classification are lists of common security issues faced by internet applications. We mitigate these risks by maintaining relationships with key Internet security standards bodies such as OWASP and the Centre for Internet Security and implement recommended mitigation strategies and controls as part of Gallagher software products and for our own internal processes.

Monitoring our solution

We monitor the Data Centre solution for both active and passive threats to the service.
Preventative measures include:

- Operational monitoring of application logs and user activity
- Monitoring and scanning for Common Vulnerabilities and Exposures (CVE) in platforms and dependencies used by the Data Centre solution
- Monitoring and implementing relevant security related errata and advisories from Gallagher technology partners

What does Gallagher know about Security?

At Gallagher Group, Security is not just an afterthought, but an essential part of our DNA - and the DNA in the Data Centre solution is no exception.

What data communications do we use?

All communication with Dispenser Units, the Data Centre application and the associated API is encrypted via HTTPS with TLS v1.2. We use secure WebSockets for backchannel messaging between Data Centre and the pumps.

How do we proactively manage security?

Our API and its associated infrastructure is built to ensure we are always up to date with security patches. We provide these for Data Centre as part of our automated patch and release process.

Is the Data Centre data ever exposed?

Whether in transit from the Dispensers or accessed from a smartphone the information is always encrypted.

What password rules does Data Centre follow?

The default password policy requires at least 8 characters with at least one digit, a capital, a lower case and a special character.

Where is my tablet connecting to, and my data stored?

All data and interaction is with Amazon Web Services based on dual server zones within the Sydney area.

Secure Communications

All network communications channels of the Data Centre application, including within the Amazon Virtual Private Cloud used to host the Data Centre solution, are encrypted using TLS 1.2 and forward secrecy, which is a property of secure communications protocols in which compromise of long-term keys does not affect past session keys. All network and messaging communications channels of the Data Centre application are protected by public key cryptography.

Accessing Data

Only Gallagher engineering and technical support staff working on the Data Centre solution have access to customer data. Gallagher applies standard screening procedures to all engineering staff as part of the recruitment process.

Customers can grant access to data for third parties such as accredited services providers assisting customers with site management and maintenance. This can be changed by request with customer authorisation.

Protecting the Data

Gallagher use the Amazon Web Service (AWS) platform for hosting all aspects of the Data Centre solution. We take advantage of AWS security and data protection features available in various AWS products including EBS, RDS, S3, etc. to protect customer data during processing and at rest. All data stored via EBS, RDS, S3 is automatically encrypted to help prevent unauthorised access.

All user passwords are hashed using standard hashing algorithms before they are stored or validated. The Data Centre solution uses the PBKDF2 algorithm with 20,000 iterations and a separate salt for each password.

Backup and Recovery

We regularly back up all data associated with the Data Centre solution (excluding data stored in S3). All Data Centre services and any associated customer data are currently hosted and managed in the Amazon AWS Sydney region.

MAR-016489 02-2021

GALLAGHER

For more information regarding Gallagher Data Centre

Scott Ellery | Business Development Manager - NZ
DDI +64 6 327 0334 | MOB +64 21 792 934
EMAIL scott.ellery@gallagher.com

Derek Hjelm | Business Development Manager - AUS
MOB +61 424 164814
EMAIL derek.hjelm@gallagher.com