DATA CENTRE
Security Statement

PEC 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 PEC Fuel System Cloud products.

Hosted in the Cloud

PEC Limited 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.

Threats Managed

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 PEC software products and for our own internal processes.

A Monitored 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 PEC technology partners

Communications are Secure

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.

Access is Controlled

Only PEC engineering and technical support staff working on the Data Centre solution have access to customer data. PEC 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

PEC 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.

For more information contact:

Derek Hjelm: Business Development Manager, Australia
Mobile: +61 424 164 814
Email: derek.hjelm@pec.co.nz

Scott Ellery: Sales Executive, New Zealand
Mobile: +64 21 792 934
Email: scott.ellery@pec.co.nz

PEC FUEL SYSTEMS
2 Station Road, Marton 4710, New Zealand
PO Box 308, Marton 4741, New Zealand
Phone: +64 6 327 0060
Email: info@pec.co.nz

MAR-016489 03-2022