Data Management and Security Fact Sheet

This document outlines the data management and security practices undertaken by Fluid Management Technology to ensure the reliability and security of the fmtdata.com website.

Data Management	
Where is our data stored?	All data and database backups are stored on dedicated servers deployed on the virtual private cloud on AWS Infrastructure. Unit Configuration and log backups are stored on Google Cloud Platform.
Where is our data physically Stored?	AWS servers are located in Northern Virginia, USA. Google Cloud Platform servers are located in Sydney, Australia. Australian clients will get their data served from Australian edge locations of AWS.
When do we backup data?	Database backups are performed incrementally every 5-10 minutes, in addition to a full daily backup. Unit configuration and log file backups are performed weekly.
What data do we backup?	We keep backups for the website database, log files, and unit configurations.
How long are backups kept for?	A minimum of two years after account inactivity
What is our process to recover data from a potential problem or data loss?	In the event of data loss, a point in time recovery can be performed on our database.
What activity is logged?	All user activities are logged.
How long are logs kept for?	A minimum of two years after account inactivity
Security	
IP address range blocking	IP range blocking can be configured for your website by contacting support.
Is data encrypted during transit when accessing the fmtdata.com website?	Yes
Do all backend technologies use the latest versions available? (e.g. HTML5, PHP 7)	Yes
Will FMT completely delete all user data if asked?	Yes
Certifications	
PCI (Payment Card Industry)	Certified by SecurityMetrics and Comodo.