Hach Mobile Sensor Management Data Security, Privacy and Safety

At Hach®, our number one concern is our customers' data security and data privacy. Hach's products, development processes and operations satisfy the internationally accepted directives on information security management set forth by ISO/IEC 27001, ISO/IEC 62443-4-1 and -4-2.

Your data is secure.

All communications between the Mobile Sensor Management hardware and the Hach Remote Server utilise industry standard 2048-bit Secure Sockets Layer (SSL/TSL) encryption algorithms, making sure that only known and trusted end-points can communicate. The implemented firewalls ensure all other traffic is being ignored so that no unauthorised 3rd party is able to access the system or eavesdrop on the communication.

All data stored on the server (data at rest) is encrypted and safeguarded using the latest IT technology and operational processes.

Access to the application is controlled by user name and password. Least Privileged Principle is enforced and we maintain strict password policies to ensure no passwords can be guessed or compromised by a brute force attack.

All sensitive data in the Hach devices like SC1500 and DR3900 are stored in a "data safe" (encrypted flash memory). This prevents vulnerability even if the devices are stolen and physically accessed by an unauthorised 3rd party.

Your data is private.

Data privacy means only you and those you authorise can see your data. Hach's implementation is certified to one of the most restrictive data privacy policies worldwide. This includes:

- Customer's exclusive ownership of all key material
- Strict separation of Customer's data
- Local data privacy rules are complied with through local servers
- Hach tech support access via certificate based VPN on customer's explicit invitation and approval only
- Hach administrators logon to the MSM system through 2-factor authentication

Hach reserves the right to query the data in anonymised form for product development purposes.

Your data is safe.

The Hach Remote Server maintains a 99.9% uptime. The datacenter handles all backups and hot switchovers during hardware upgrades/failures, ensuring you will always have access to your data.

Data is stored on multiple servers in different data centers, ensuring quick data recovery if needed

- Data centers are in different geographically locations for disaster recovery purposes

To ensure the highest level of protection for your data, Hach partners with Microsoft as a professional, renowned and very experienced expert keeping your data secure, private and safe. For more information about Microsoft's compliance with international regulations see:
https://azure.microsoft.com/en-us/support/trust-center/compliance

Below is a list of the most important regulations and directives that have been applied by Hach:

- IEC 62433 (international)
- ISO/IEC 27001-27005 (international)
- NIST 800-34, 800-53, 800-82 (international)
- BSI IT Protection (Germany)
- BDSG (BundesDatenSchutzGesetz, Germany)
- AWWA G340 (USA)

DOC063.52.30367.Nov16