Seguridad, privacidad y protección de datos de Mobile Sensor Management de Hach

En Hach® la preocupación más importante es la protección y privacidad de los datos de nuestros clientes. Los productos, los procesos de desarrollo y las operaciones de Hach cumplen las directivas aceptadas internacionalmente sobre gestión de la seguridad de la información expuestas en ISO/IEC 27001, ISO/IEC 62443-4-1 y -4-2.

Sus datos están protegidos.

Todas las comunicaciones entre el hardware de Mobile Sensor Management y el servidor remoto de Hach usan los algoritmos de encriptación Secure Sockets Layer (SSL/TSL) de 2048 bits estándar del sector que garantiza que solo los extremos conocidos y de confianza pueden comunicarse. Los firewalls utilizados garantizan que el resto del tráfico será ignorado para que terceros no autorizados no puedan acceder al sistema o interceptar la comunicación.

Todos los datos almacenados en el servidor (datos en reposo) están encriptados y protegidos por la última tecnología informática y procesos operativos.

El acceso a las aplicaciones está controlado por el nombre de usuario y la contraseña. Se aplica el principio del privilegio mínimo y mantenemos políticas estrictas para las contraseñas para garantizar que no puedan adivinarse ni estar en peligro en caso de un ataque malintencionado.

Todos los datos sensibles de los dispositivos de Hach como el SC1500 y el DR3900 se almacenan en un "entorno seguro para datos" (memoria flash encriptada). Esto evita que sean vulnerables incluso aunque un tercero no autorizado robe los dispositivos y acceda a ellos físicamente.

Sus datos son privados.

La privacidad de datos significa que solo usted y aquellos a los que autorice pueden ver sus datos. La implementación de Hach está certificada por una de las políticas de privacidad de datos más restrictivas del mundo. Esto incluye:

- Propiedad exclusiva del cliente de todo el material importante
- Separación estricta de los datos del cliente
- Cumplimiento de las reglas de privacidad de los datos locales a través de los servidores locales
- Acceso del soporte técnico de Hach a través de VPN certificado, únicamente mediante invitación y aprobación expresa del cliente
- Inicio de sesión de los administradores de Hach en el sistema Mobile Sensor Management mediante autenticación de 2 factores

Hach se reserva el derecho de consultar los datos de forma anónima para el desarrollo de productos.

Sus datos están seguros.

El servidor remoto de Hach mantiene un tiempo de disponibilidad del 99,9 %. El centro de datos gestiona todas las copias de seguridad y "switchover" en activo durante actualizaciones/fallos de hardware para garantizar que siempre tenga acceso a sus datos.

Los datos se almacenan en varios servidores en centros de datos distintos lo que garantiza una recuperación rápida de los datos si es necesario

- Los centros de datos se encuentran en ubicaciones geográficas diferentes para la recuperación en caso de fallo

Para garantizar que sus datos cuentan con el nivel de protección más alto, Hach se ha asociado con Microsoft, un experto reconocido y profesional con amplia experiencia en mantener sus datos protegidos, privados y seguros. Para obtener más información sobre el cumplimiento de las normativas internacionales por parte de Microsoft consulte:
https://azure.microsoft.com/en-us/support/trust-center/compliance

A continuación encontrará una lista de las normativas y directivas más importantes que han sido aplicadas por Hach:

- IEC 62433 (internacional)
- ISO/IEC 27001-27005 (internacional)
- NIST 800-34, 800-53, 800-82 (internacional)
- BSI IT Protection (Alemania)
- BDSG (BundesDatenSchutzGesetz, Alemania)
- AWWA G340 (EE. UU.)

DOC063.61.30367.Nov16