

Sécurité et confidentialité des données du système Mobile Sensor Management de Hach

Chez Hach®, notre première préoccupation est la sécurité et la confidentialité des données de nos clients. Les produits, processus de développement et opérations de Hach répondent aux directives internationalement reconnues sur la gestion de la sécurité des informations énoncées dans les normes ISO/CEI 27001, ISO/CEI 62443-4-1 et -4-2.

Vos données sont sécurisées.

Toutes les communications entre le matériel Mobile Sensor Management et le serveur distant de Hach utilisent des algorithmes de cryptage Secure Sockets Layer (SSL/TSL) 2048 bits, la référence du secteur, garantissant que seuls des points finaux connus et de confiance peuvent communiquer. Les pare-feu mis en place garantissent que tout autre trafic est ignoré, de sorte qu'aucun tiers non autorisé n'est en mesure d'accéder au système ou d'écouter la communication.

Toutes les données stockées sur le serveur (les données au repos) sont cryptées et protégées à l'aide des dernières technologies informatiques et des derniers processus opérationnels.

Il faut saisir un nom d'utilisateur et un mot de passe pour accéder à l'application. Nous appliquons le principe de séparation des privilèges et maintenons des politiques rigoureuses en matière de mot de passe pour nous assurer qu'aucun mot de passe ne peut être deviné ou compromis par une attaque en force.

Toutes les données sensibles des appareils Hach comme le SC1500 et le DR3900 sont stockées dans un « coffre-fort de données » (mémoire flash cryptée). Cela permet d'empêcher toute vulnérabilité, même si les appareils sont volés et si des tiers non autorisés y accèdent physiquement.

Vos données sont privées.

La confidentialité des données garantit que seuls vous et ceux que vous autorisez pouvez voir vos données. La politique de confidentialité des données de Hach est certifiée comme l'une des plus restrictives au monde. Elle comprend :

- La propriété exclusive de tout le matériel clé par le client
- Une séparation rigoureuse des données du client
- Le respect des règlements locaux en matière de confidentialité des données grâce à des serveurs locaux

- L'accès de l'assistance technique de Hach via un réseau privé virtuel basé sur certificat uniquement lorsque le client le demande explicitement et l'approuve
- La connexion des administrateurs de Hach au système Mobile Sensor Management via une authentification en deux étapes

Hach se réserve le droit d'interroger les données de façon anonyme à des fins de développement de produits.

Vos données sont en sécurité.

Le serveur distant de Hach assure un taux de disponibilité de 99,9 %. Le centre de données gère toutes les sauvegardes et les basculements importants au cours des mises à niveau/pannes de matériel, pour vous garantir un accès continu à vos données.

Les données sont stockées sur plusieurs serveurs dans différents centres de données, ce qui garantit une récupération rapide des données si nécessaire.

- Les centres de données se trouvent dans différentes régions géographiques à des fins de reprise après sinistre.

Afin d'assurer le plus haut niveau de protection de vos données, Hach s'est associé à Microsoft en tant qu'expert professionnel, reconnu et très expérimenté pour maintenir la confidentialité et la sécurité de vos données. Pour en savoir plus sur la conformité de Microsoft avec les règlements internationaux, visitez la page :

<https://azure.microsoft.com/en-us/support/trust-center/compliance>

Vous trouverez ci-dessous une liste des principaux règlements et directives appliqués par Hach :

- CEI 62433 (International)
- ISO/CEI 27001-27005 (international)
- NIST 800-34, 800-53, 800-82 (international)
- Protection informatique BSI (Allemagne)
- BDSG (BundesDatenSchutzGesetz, Allemagne)
- AWWA G340 (Etats-Unis)