# Hach Claros Whitepaper over beveiliging

## Managementoverzicht

Claros is het Water Intelligence Systeem van Hach® dat is ontworpen om organisaties in de watersector in staat te stellen laboratorium- en procesgegevens veilig om te zetten in bruikbare inzichten, om betere bedrijfsresultaten te realiseren. Claros combineert de oplossingen voor instrumentmanagement, datamanagement en procesmanagement van Hach in één platform. Hach realiseert zich dat het helpen beschermen van de data van onze klanten, het naleven van best-practice op het gebied van beveiligen en het beperken van potentiële risico's essentieel is voor het opbouwen van vertrouwen en het leveren van een hoog serviceniveau. Hach hanteert een risicogebaseerde benadering van beveiliging en in dit document wordt beschreven welke maatregelen en technologieën Claros gebruikt om de gegevens van onze klanten te beschermen.

Daarnaast wordt in dit document beschreven hoe Claros omgaat met fundamentele doelstellingen van informatiebeveiliging: vertrouwelijkheid, integriteit en beschikbaarheid, evenals de benadering van Hach op het gebied van beveiligingsarchitectuur en de verantwoordelijkheden van onze klanten. Binnen deze beveiligingscontext verwijst vertrouwelijkheid naar onze set regels voor beheer van toegang tot informatie, integriteit als nauwkeurigheid en betrouwbaarheid van de informatie en beschikbaarheid als betrouwbare toegang tot informatie door bevoegde gebruikers.

**Zie onderstaand overzicht van de hierin opgenomen onderwerpen:**

# De benadering van Hach

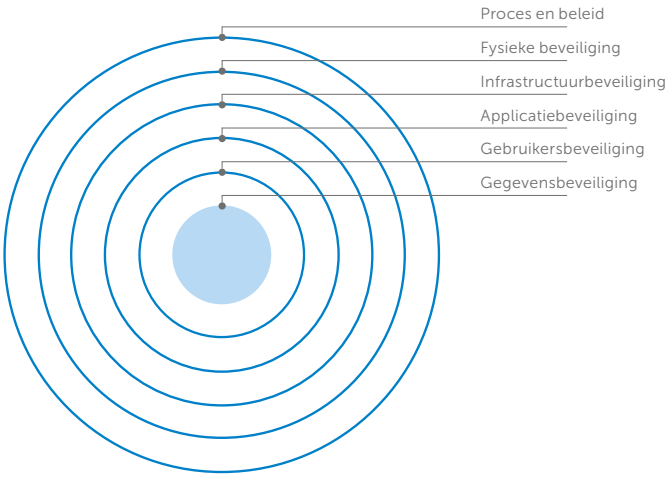
## Diepgaande verdediging

Claros is niet een systeem met afzonderlijke lagen die klantgegevens beschermen, maar een goed gearchiveerde oplossing die elke laag reguleert, vanaf de fysieke beveiligingsmaatregelen in het datacenter tot en met de toegangsrechten die bepalen tot welke gegevens een individuele gebruiker toegang heeft. Hach gebruikt deze meerlaagse beveiligingsstrategie om klantgegevens te beschermen.

*Diepgaande verdediging verwijst naar het gecoördineerde gebruik van meerdere beveiligingsmaatregelen om de integriteit van de informatieactiva in een onderneming te beschermen. Deze strategie is gebaseerd op het militaire principe dat het voor een vijand moeilijker is om een complex en meerlaags verdedigingssysteem te verslaan dan om een enkele barrière te doorbreken.*
*-TechTarget*

## Proces en beleid

De eerste verdedigingslaag bestaat uit een goed gedefinieerde en uitgebreide set beveiligingsprocessen en -beleidsregels, om de veiligheid van de gegevens van onze klanten en gebruikers te waarborgen. Het systeem voor informatiebeveiligingsmanagement (ISMS) van Hach omvat verschillende proces- en beleidsmaatregelen die ervoor zorgen dat beveiliging topprioriteit heeft en een kernwaarde vormt voor onze eigen mensen.




## Training

Medewerkers van Hach die bevoegd zijn om toegang te krijgen tot Claros volgen periodieke trainingen zodat zij het beveiligingsbeleid van Hach optimaal kunnen naleven en uitvoeren. Personeel van de afdelingen Development Operations, Research & Development en Technical Support and Services van Hach, die gevoelige klantgegevens en -informatie verwerken, doorlopen bijvoorbeeld regelmatig nalevings- en beveiligingsbewustzijnstrainingen om op de hoogte te blijven wat betreft relevante en opkomende beveiligingsrisico's.

## Geautoriseerde toegang

Naast het beperken van de toegang van personeel tot het productiegebied, heeft slechts een beperkte groep medewerkers van Hach Development Operations operationele toegang tot Claros. Toegang wordt beheerd via het bedrijfsnetwerk van Hach zodat alleen het personeel dat bevoegd is, toegang heeft tot gegevens. Al het personeel van Hach met fysieke of operationele toegang tot productieomgevingen doorloopt toepasselijke training en alle activiteiten worden geregistreerd ten behoeve van controleerbaarheid.

## Wijzigingsbeheer

Het formele wijzigingsbeheerproces van Hach zorgt ervoor dat wijzigingen en updates van Claros met zo min mogelijk risico kunnen worden uitgevoerd. Via dit proces kunnen wijzigingen in Claros worden gevolgd en kan worden geverifieerd of risico's zijn beoordeeld, of onderlinge afhankelijkheden zijn onderzocht en of noodzakelijke beleidsregels en procedures zijn overwogen en toegepast voordat enige wijziging wordt goedgekeurd. Hach documenteert alle wijzigingen in de releasenotes, die voorafgaand aan systeemwijzigingen of updates aan klanten worden gedistribueerd.

## Versterking van het systeem

Claros maakt gebruik van vele technologieën om onze service te leveren, maar toch zijn er veel functionaliteiten die niet nodig zijn. In overeenstemming met de best practices in de branche voert Claros Development Operations een grondige inspectie uit van de volledige oplossing, om onnodige services te identificeren en deze functionaliteiten te verwijderen en/of uit te schakelen om beveiligingsrisico's te voorkomen.

## Periodiek scannen op beveiligingslekken en penetratietesten uitvoeren

In overeenstemming met intern beleid en internationale kaders en normen op het gebied van cyberbeveiliging, voert Hach periodiek kwetsbaarheids- en penetratietesten uit met betrekking tot kritieke beveiligingsfouten, waaronder de OWASP Top 10, om beveiligingsrisico's te ondervangen.

## Beveiligingspatches

Hach heeft strenge beleidsregels en procedures geïmplementeerd om te waarborgen dat alle componenten van Claros, zoals besturingssystemen, hypervisors, middleware, databases, mobiele applicaties enz., worden bijgewerkt met beveiligingspatches van de leverancier. Deze activiteiten met betrekking tot beveiligingspatches worden gemonitord aan de hand van de norm IEC62443-4-1 voor controle van de levenscyclus van veilige productontwikkeling en zijn onderworpen aan strenge normen.

# Vertrouwelijkheid

## Verificatie

De Claros-architectuur is gebaseerd op een gecentraliseerd verificatie- en autorisatiebeveiligingskader om toegang tot services en de veldapparatuur te reguleren. Dit beveiligingskader maakt handhaving van beveiligingsbeleid mogelijk met algoritmen voor wachtwoordsterkte die vereisen om wachtwoorden in te stellen met een minimale lengte en complexiteit.

## Codering bij doorvoer

In- en uitgaand verkeer van Claros wordt gecodeerd voor optimale beveiliging van communicatie. Voor deze codering wordt gebruikgemaakt van een TLS/SSL-protocol (Transport Layer Security/ Secure Sockets Layer) waarbij SHA-2-algoritmen (Secure Hash Algorithm 2) of AES-algoritmen (Advanced Encryption Standard) worden toegepast. Dit houdt in dat gegevens die één van de vertrouwde eindpunten verlaten of bereiken bij overdracht via het internet op geen enkel moment ongecodeerd zijn.

## Codering in rust

De bescherming van de gegevens van onze klanten wordt zeer serieus genomen, alle Claros-gegevens worden opgeslagen op Microsoft Azure-servers en versleuteld met AES-256-bits versleuteling.

# Integriteit

## Gecontroleerde en rolgebaseerde toegang

Klanttoegang tot Claros wordt gereguleerd via gebruikersinterfaces (UI), API's (Application Programming Interface) en/of speciale tools. Voor het gebruik van een van deze toegangsmethoden zijn een gebruikersnaam en wachtwoord vereist en moet worden beschikt over de juiste rechten voor de gevraagde toegang. Accountbeheerders van Claros gebruiken Role Based Access Control (RBAC) om de juiste machtigingen in de hele Claros-infrastructuur af te dwingen. Klanten hebben geen root- of beheerderstoegang tot de Claros-technologiestack en toegang is toegestaan via de Claros-applicatielaag (UI of API).

## Toegang tot applicaties

Klantgegevens zijn toegankelijk via de Claros-applicatie. Bij elke soort toegang, of deze nu plaatsvindt via gebruikersinterfaces of via beschikbare API's, wordt RBAC afgedwongen om te waarborgen dat alleen geautoriseerde gebruikers en personeel bij de klantgegevens kunnen. Als zodanig biedt Claros geen directe toegang tot databases. Deze aanpak voorkomt dat ongeautoriseerde services of systemen per ongeluk of kwaadwillend klantgegevens kunnen opvragen of wijzigen.

## Communicatie

Communicatie met Claros wordt geïnitieerd door de veldapparatuur, zodat de klant alle communicatiepogingen van diens eigen netwerk naar de buitenwereld kan volgen en extra veiligheidsmaatregelen kan toevoegen aan het omringende netwerk. Elke communicatiepoging van en naar veldapparatuur richting Claros-gegevens wordt geverifieerd op authenticiteit.

## Firewalls

Alle netwerktoegang van en naar de veldapparatuur wordt beschermd door een meerlaagse firewall die is ingesteld in de modus Alles weigeren. Verbinding met het internet is alleen toegestaan via expliciet daarvoor geopende poorten en voor een slechts een deel van opgegeven virtuele hosts. Om een extra beveiligingslaag te creëren, bevinden alle databaseservers zich achter een extra firewall.

## Onnodige poorten en services

Alle poorten en services die niet nodig zijn voor de werking van Claros worden uitgeschakeld op alle servers en geïntegreerde veldapparatuur, waardoor extra mogelijkheden voor externe indringers worden geëlimineerd. Om Claros te kunnen gebruiken, hoeft slechts een handvol poorten en eindpunten te worden geopend in het klantnetwerk. In de volgende tabel vindt u een overzicht van de poorten en services die Claros gebruikt:

| Poort | Richting | Service | Doel |
|---|---|---|---|
| 1194 (UDP) | Uitgang | VPN | Externe toegang voor Hach-servicemonteurs |
| 5671 (TCP) | Uitgang | AMQPS | Berichten verzenden/ontvangen aan/van Claros |
| 123 (UDP) | Uitgang/ingang | NTP | Huidige datum/tijd ophalen van externe tijdserver |
| 80 (TCP) | Uitgang | HTTP | Versleutelde en ondertekende firmware-updates ophalen uit de database |
| 443 (TCP) | Uitgang | HTTPS | Toegang tot Claros UI |

# Beschikbaarheid

## Microsoft Azure

Claros maakt gebruik van Microsoft Azure Cloud Computing voor het leveren van haar services. Daarom profiteren alle klanten van Claros van de Service Level Agreement (SLA) van Microsoft Azure, die een uptime van 99,95% of meer waarborgt voor alle belangrijke Azure-services.

## Infrastructuur

Tussen de fysieke datacenterlaag en de applicatielaag van Claros bevindt zich de infrastructuur die onze oplossing ondersteunt. In de gehele infrastructuur wordt beveiliging op een uitgebreide en gecoördineerde manier geïmplementeerd om de veiligheid van klantgegevens te verbeteren.

## Conformiteit

Om onze klanten te helpen voldoen aan nationale, regionale en branchespecifieke vereisten met betrekking tot het verzamelen en gebruiken van individuele gegevens, biedt Microsoft Azure het meest uitgebreide pakket aan nalevingsfunctionaliteiten van alle cloudserviceproviders op brancheniveau.

Alle Microsoft Azure-datacenters zijn gecertificeerd volgens toonaangevende standaarden voor informatiebeveiliging. In de onderstaande tabel vindt u een overzicht:

| | |
|---|---|
| CDSA | Azure is gecertificeerd volgens de norm van de Content Delivery & Security Association voor beveiliging en bescherming van content. |
| CSA STAR Attestation | Azure en Intune zijn bekroond met Cloud Security Alliance STAR Attestation op basis van een onafhankelijke beoordeling. |
| GxP | Microsoft-cloudservices voldoen aan de Good Clinical, Laboratory en Manufacturing Practices (GxP). |
| ISO 9001 | Microsoft is gecertificeerd voor de implementatie van deze standaarden voor kwaliteitsmanagement. |
| EN 20000-1:2011 | Microsoft is gecertificeerd voor de implementatie van deze standaarden voor servicemanagement. |
| ISO 22301 | Microsoft is gecertificeerd voor de implementatie van deze standaarden voor bedrijfscontinuïteitsmanagement. |
| ISO 27001 | Microsoft is gecertificeerd voor de implementatie van deze standaarden voor informatiemanagement. |
| ISO 27017 | Deze Code of Practice voor informatiebeveiliging is geïmplementeerd in Microsoft-cloudservices. |
| ISO 27018 | Microsoft was de eerste cloudprovider die zich hield aan deze gedragscode voor cloudprivacy. |
| MPAA | Azure heeft met succes een formele evaluatie van de Motion Picture Association of America doorlopen. |
| Gedeelde evaluaties | Microsoft laat zien dat Azure in lijn is met dit programma aan de hand van CSA CCM versie 3.0.1. |
| SOC 1 | Microsoft-cloudservices voldoen aan de normen van Service Organization Controls voor operationele beveiliging. |
| SOC 2 | Microsoft-cloudservices voldoen aan de normen van Service Organization Controls voor operationele beveiliging. |
| SOC 3 | Microsoft-cloudservices voldoen aan de normen van Service Organization Controls voor operationele beveiliging. |
| WCAG 2.0 | Microsoft-cloudservices voldoen aan de richtlijnen voor toegankelijkheid van webinhoud 2.0. |

# Regionale implementaties

Microsoft Azure bestrijkt meer wereldwijde regio's dan welke andere cloudprovider dan ook. Het biedt de schaalbaarheid die nodig is om Claros-applicaties dichter bij gebruikers over de hele wereld te brengen, beschikbaarheid van gegevens te behouden en uitgebreide mogelijkheden voor naleving en flexibiliteit te bieden aan klanten. Om klanten te helpen de integriteit van hun gegevens te waarborgen en te voldoen aan regionale regelgeving, maakt Hach gebruik van Microsoft Azure-datacenters voor klanten in hun eigen regio of zo nabij als mogelijk.

**50** Regio's wereldwijd **140** Beschikbaar in 140 landen


Bron: Microsoft

Al deze datacenters zijn uitgerust met N+1 redundante HVAC en UPS (Uninterruptible Power Supply).

Fysieke beveiliging houdt zich aan de best practices in de branche en omvat:

- Protocollen voor keycards, biometrische scanprotocollen en binnen- en buitentoezicht 24 uur per dag
- Toegang is beperkt en uitsluitend voor geautoriseerd datacenterpersoneel – niemand kan het productiegebied betreden zonder voorafgaande toestemming en passende begeleiding
- Elke medewerker van het datacenter doorloopt grondige achtergrondcontroles

# Verantwoordelijkheden van de klant

## Gecontroleerde toegang en installatie

Om te zorgen dat Hach gegevens optimaal kan beveiligen, verwachten wij ook van onze klanten dat zij veiligheidsnormen in acht nemen. Hach vertrouwt erop dat klanten ervoor zorgen dat elke Claros-account is ingesteld met de juiste machtigingen en unieke toegangsrechten voor elke gebruiker. Het is de taak van elke klant om vast te stellen wie binnen de organisatie beheerderstoegang heeft en zorg te dragen voor het beheer van deze accounts op lange termijn.

## Fysieke bescherming

Klanten zijn verantwoordelijk voor fysieke bescherming van hun Hach instrumentatie en beveiligingsinfrastructuur,  maar ook voor de gecontroleerde toegang tot de relevante Hach-instrumentatie (bijv. controllers en sensors) en voor communicatienetwerken.

## Connectiviteit

Elke klant is zelf verantwoordelijk voor het realiseren van verbinding van Hach-instrumentatie met Claros op elke locatie. Voor een effectieve werking van Claros vereist de instrumentatie een mobiele of netwerkverbinding die de klant dient te onderhouden en deze verbinding dient afdoende beschermd te worden.

DOC180.56.10159.July20