

AV 2026 Bijlage 27 – eisen aan het remote beheer en monitoring platform

De leverancier dient een functioneel en veilig remote beheer- en monitoringplatform te leveren en onderhouden, dat voldoet aan de volgende specificaties:

On-premises implementatie:

- IVO Rechtspraak voert een SaaS-first beleid. Echter, de scope van dit beleid staat ter discussie. De gevraagde oplossing voor dit platform zou bij voorkeur zowel als SaaS als lokaal in het datacenter van de Rechtspraak moeten kunnen worden gerealiseerd.
- In het geval van een on-premises (lokale) variant is het wel wenselijk dat inschrijver het platform beheert conform SaaS-dienstverleningsconcept. D.w.z. leverancier is verantwoordelijk voor installatie en onderhoud van het platform inclusief upgrades, (security)patches en nieuwe functionaliteit.
- Een oplossing on-premises kan gebruik maken van IVO Rechtspraak IaaS diensten, virtual machine (Windows, Linux) of container, voor de hosting evenals remote toegang tot de oplossing.

Toegankelijkheid en beheer:

- Het platform moet op afstand toegankelijk zijn via een beveiligde verbinding (HTTPS).
- Het platform moet multi factor authenticatie ondersteunen.
- In het geval van SaaS moet een federatieve koppeling met de identity provider (IdP) van de Rechtspraak mogelijk zijn (Entra ID)
- Beheerders moeten via role-based access control (RBAC) toegangsniveaus kunnen instellen per gebruiker.

Monitoringfunctionaliteit:

- Realtime inzicht in de status van alle AV-componenten (zoals camera's, microfoons, DSP's, displays, switches)
- Automatische meldingen bij storingen, uitval of afwijkende prestaties.
- Predictieve monitoring: het systeem moet op basis van prestatiegegevens afwijkingen kunnen signaleren voordat deze leiden tot uitval
- Logging van systeemgebeurtenissen (minimaal 6 maanden terug).

Beheerfunctionaliteit:

- Mogelijkheid tot het op afstand (automatisch) herstarten, updaten en configureren van AV-apparatuur.
- Batch-configuratie en -beheer van meerdere locaties/apparaten
- periodiek maken van back-ups van configuratiegegevens en systeeminstellingen en gecontroleerd terugzetten als nodig
- Patch- en releasebeheer: het platform moet centraal uitgerolde firmware- en beveiligingsupdates ondersteunen voor aangesloten apparaten.

Ondersteuning en escalatie:

- Het platform moet geïntegreerd zijn met- of ondersteuning bieden voor een supportdesk die real-time monitoring uitvoert en op basis van impact prioriteiten stelt

- Bij onoplosbare incidenten op afstand moet het platform ondersteuning bieden voor het automatisch doorzetten naar field service (on-site interventie).

Rapportage:

- Het platform moet rapporten kunnen genereren over beschikbaarheid, storingen en gebruiksstatistieken (minimaal maandelijks).
- Trendanalyse: inzicht in systeemgezondheid, storingspatronen en voorspelling van toekomstige onderhouds- of vervangingsbehoeften.

Beveiliging en compliance:

- Zie de bijlage 13 PvE sheet security

Openheid en interoperabiliteit:

- Beschikbaarheid van een API voor integratie met bestaande IT-beheersystemen.
- Integratie met monitoringsysteem van de rechtspraak mogelijk

Besturings functionaliteit

Op termijn moet het voor de opdrachtgever mogelijk zijn om bepaalde functies, zoals het op afstand in- of uitschakelen en aansturen van een videoconferencing-set, centraal te beheren. Dit met als doel het verminderen van de benodigde handmatige handelingen. Deze functionaliteit dient centraal vanuit een regiekamer bij de opdrachtgever te kunnen worden uitgevoerd.