

ID	Thema	Onderwerp	Omschrijving	Inschrijver voldoet aan eis JA/NEE
T1	Techniek	Content tonen	Content moet getoond kunnen worden in een aparte BFCP gebaseerde stream en 1080p kunnen ondersteunen. Hoge resolutie is van belang vanwege de leesbaarheid van eventuele tekst die getoond wordt. De aparte BFCP stream is van belang vanwege de herkenning door videosystemen dat het een contentstream is, waardoor deze kan worden getoond op een specifiek scherm, bedoeld voor content.	
T2	Techniek	IAM	Microsoft Entra ID moet worden ondersteund als identity provider. Voor het federatief koppelen dient één van de volgende protocollen te worden gebruikt: OAuth OIDC 1.0, OAuth 2.0 of SAML 2.0. Dat moet ook mogelijk zijn met een ander IdP dan MS Entra ID.	
T3	Techniek	Security	Alle verbindingen vanaf een webbrowser naar de oplossing zijn gebaseerd op HTTPS en maken gebruik van HSTS	
T4	Techniek	Security	Alle verbindingen van en naar de oplossing maken gebruik van minimaal TLS 2.0 voor encryptie	
T5	Techniek	Security	Voor het opzetten van audio/videoverbindingen vanaf video endpoints wordt voor signalering gebruik gemaakt van SIPs en voor de media wordt gebruik gemaakt van sRTP.	
T6	Techniek	Standaardisatie	De oplossing biedt een API die voldoet aan de REST standaard of eventueel de SOAP standaard. De oplossing beschikt over een standaard API koppeling zodat eenvoudig een integratie met andere applicaties kan worden gerealiseerd. De Rechtspraak heeft een sterke voorkeur voor REST API-design rule.	
T7	Techniek	Standaardisatie	Als onderdeel van een optimale deelname ervaring moet het mogelijk zijn een kalender uitnodiging te sturen met daarin: - SIP URI in de vorm van een emailadres (zie ook https://www.forumstandaardisatie.nl/open-standaarden/uri-en-iri) conform <vergaderid>@domeinnaam, zodat de SIP URI direct is aan te kiezen zonder DTMF	
T8	Techniek	Standaardisatie	In geval van deelname aan een online zitting via SIP is deelnemen mogelijk door middel van een SIP URI in de vorm van een emailadres (zie ook https://www.forumstandaardisatie.nl/open-standaarden/uri-en-iri)> een vergaderid kan dan worden ingevoerd door middel van DTMF. Geplande afspraken worden minimaal als platte tekst in een e-mail verstuurd.	
T9	Techniek	Standaardisatie	De oplossing maakt het mogelijk dat provisioning van rechtbank medewerkers mogelijk is op basis van het SCIM 2.0 protocol waarbij minimaal de volgende standaard attributen worden synchroniseerd: - Voornaam - Achternaam - Email adres Het moet mogelijk zijn om een filter toe te passen op de synchronisatie. Deze eis is niet van toepassing als er geen gebruikers worden gesynchroniseerd van de gebruikersdirectory van de Rechtspraak naar de gebruikersdirectory van de oplossing.	
T10	Techniek	Standaardisatie	Voor het opzetten van audio/videoverbindingen vanaf een browser wordt gebruik gemaakt van WebRTC	
T11	Techniek	Standaardisatie	De oplossing moet minimaal de volgende video standaarden ondersteunen: H.263, H.263+, H.264	
T12	Techniek	Standaardisatie	De oplossing moet minimaal de volgende audio standaarden ondersteunen: G.711, G.722, G.722.1	
T13	Techniek	Video ervaring	De oplossing moet minimaal video resoluties ondersteunen van 720p. De oplossing borgt dat iedere individuele deelnemer met een zo optimaal mogelijke audio en video kwaliteit kan deelnemen. De algemene meeting kwaliteit wordt niet gedictieerd door de individuele deelnemer met een verbinding met beperkte capaciteit. Indien niet kan worden voldaan aan de minimale 720p-resolutie moet een individueel video device of client met beperkte bandbreedte adaptief een lagere video resolutie en/of framerate aangeboden worden, dusdanig dat de overige deelnemers met voldoende bandbreedte nog steeds met een optimale video resolutie kunnen deelnemen.	
T14	Techniek	Video ervaring	De oplossing realiseert een video framerate van minimaal 25FPS (wanneer de beschikbare bandbreedte dit toestaat).	
T15	Techniek	Video stream	De oplossing kan of met het Teams native AV protocol communiceren met het Teams Live event platform, of in staat zijn een RTMP stream uit te zenden naar de Teams Encoder van het Team Live event platform. Binnen IVO Rechtspraak is M365 Teams Live event vastgesteld als (live) streaming oplossing om een Online Zitten sessie openbaar te streamen. Wanneer de oplossing wordt gebruikt om een stream uit te sturen rechtstreeks naar eindgebruikers (en dus niet naar een streamingplatform) zijn één of meerdere van de volgende protocollen beschikbaar: HLS, MPEG-DASH en SRT.	
B1	Beheer	Identity and Accesmanagement	Opdrachtnemer voorziet IVO Rechtspraak in roll based access voor beheerders. Binnen uw oplossing bestaan beheersrollen met verschillende niveaus betreffende rechten. Elke gebruiker beschikt wel over dezelfde interface, maar instellingen die niet beschikbaar zijn binnen de rol, kunnen niet worden aangepast.	
B2	Beheer	Service level agreement	Beschikbaarheid van oplossing is 99,8% per rapportage maand op werkdagen binnen een service venster van 07:30 tot 17:30, zie concept SLA.	
B3	Beheer	Service level agreement	De volgende reactie en oplostijden zijn van toepassing op de oplossing, zie concept SLA: Reactietijd (norm 85%): Prio 1 1 uur Prio 2 2 uur Prio 3 2 uur Prio 4 2 uur Prio 5 2 uur Oplostijd (norm 85%): Prio 1 4 uur Prio 2 10 uur (1 werkdag) Prio 3 30 uur (3 werkdagen) Prio 4 50 uur (5 werkdagen) Prio 5 50 uur (15 werkdagen)	
B4	Beheer	Service level agreement	De volgende Impact en Urgentie matrix is van toepassing, zie concept SLA Impact: Hoog: voor een grote groep gebruikers is Attendant Console niet beschikbaar en/of de interfaces tussen Opdrachtgever en Attendant Console hebben niet of werken niet naar behoren. Midden: voor een beperkt aantal gebruikers is Attendant Console niet beschikbaar of is bepaalde functionaliteit van Attendant Console niet beschikbaar. Laag: voor één gebruiker is (bepaalde functionaliteit van) Attendant Console niet beschikbaar of het gemelde incident betreft een wens. Urgentie: Hoog: Het systeem functioneert niet of nauwelijks en er is geen workaround; Er is sprake van beschadigde data; De meeste of alle gebruikers hebben hier last van. Midden: De dienst biedt beperkte functionaliteiten; Workarounds mogelijk aanwezig. Laag: De dienst is niet aangetast.	
B5	Beheer	Dossier afspraken en procedures	Opdrachtnemer levert op basis van de overeengekomen SLA een Dossier Afspraken en Procedures (DAP) document op en rond deze af in samenspraak met de IVO Rechtspraak Service Delivery Manager.	
P1	Privacy	AVG	De Opdrachtnemer van de oplossing kan aantonen hoe de kwaliteit op het gebied van privacy in de tijd wordt behouden conform artikel 28 van de Algemene verordening gegevensbescherming (AVG). Dit wordt door Opdrachtnemer onderbouwd met documentatie voor zowel het interne proces als de ingezette techniek (Architectuuroverzicht, datamapping, autorisatietabel, ISAE3402 certificering, SOC rapportages en pentest rapportages.	
P2	Privacy	Gegevensverwerking	Uw oplossing biedt de mogelijkheid om, afhankelijk van het type (persoons-) gegevens, in te stellen of deze bewaard of verwijderd moeten worden en hoe lang deze bewaard moeten worden. Het al dan niet bewaren of verwijderen en de bewaartermijn per type (persoons-) gegevens wordt vastgelegd in de verwerkersovereenkomst.	
P3	Privacy	Locatie gegevensverwerking	De persoonsgegevens én meta data worden te alle tijde in de EU/EER verwerkt. Zie voor de definitie van verwerken artikel 4 lid 2 van de AVG. Eventuele diagnostische data moet worden geanonimiseerd.	
P4	Privacy	Rechten betrokkene	De oplossing van de opdrachtnemer maakt het mogelijk persoonsgegevens in te zien, te wijzigen en te verwijderen en geeft inzage in wie toegang heeft tot deze persoonsgegevens.	
P5	Privacy	Risicoanalyse	De Opdrachtnemer levert de Data Protection Impact Assessment (DPIA) die op het systeem is gedaan aan. Indien de Opdrachtnemer geen DPIA heeft gedaan op het systeem dan dient de Opdrachtnemer medewerking te verlenen aan het uitvoeren van (privacy-) risicoanalyses en laat de resultaten van deze analyses, indien noodzakelijk en mogelijk, doorwerken in de oplossing en/of dienstverlening.	
P6	Privacy	Verwerkersovereenkomst	De Opdrachtnemer is verplicht om een verwerkersovereenkomst af te sluiten met de verwerkingsverantwoordelijke van IVO Rechtspraak. De verwerkersovereenkomst wordt door IVO Rechtspraak aangeleverd en wordt tegelijk met de dienstverleningsovereenkomst getekend, voorafgaand aan de ingangsdatum van de licentie. Voor eventuele subverwerkers van persoonsgegevens waarmee de Opdrachtnemer samenwerkt gelden dezelfde vereisten als voor de Opdrachtnemer.	
S1	Security	Assurance	Opdrachtnemer beschikt over een SOC-2 type 2, ISAE 3402 type 2 of ISAE 3000 rapport. De SOC-2 type 2, ISAE 3402 type 2 of SAE 3000 rapport is van toepassing op de verwerker of sub-verwerken(s) die data verwerken, danwel opslaan. Indien verwerker niet beschikt over een dergelijk certificering of rapport, zorgt Opdrachtnemer dat een dergelijk rapport binnen een afgestemde periode wordt aangeleverd. Indien gebruik wordt gemaakt van sub-verwerkers wordt verzocht aan te geven middels een dataflow diagram welke verwerker/sub-verwerker toegang heeft tot welke data?	
S2	Security	Autorisatie	Opdrachtnemer heeft de oplossing zo ingericht dat beheerders alleen toegang kunnen krijgen tot de voor hun noodzakelijke gegevens. Tot de overige gegevens krijgen zij geen toegang. In overleg met de verwerkingsverantwoordelijke van IVO Rechtspraak wordt afgestemd welke medewerkers van de Opdrachtnemer geautoriseerd worden tot het inzien van de data, hierbij wordt een maximum aantal geautoriseerden afgesproken.	
S3	Security	Certificering	Opdrachtnemer (inclusief onderaannemers) beschikt over een geldig en voor de aangeboden oplossing/dienst van toepassing zijnde ISO27001 certificaat.	
S4	Security	Cryptografie	Data in -transport, -verwerking, en -at rest zijn versleuteld met adequate cryptografische maatregelen. Opdrachtnemer zorgt dat cryptografische sleutels/certificaten zijn opgeslagen in een afdoende beveiligde omgeving. Multi-Factor Authentication (MFA) is vereist om toegang te krijgen tot de cryptografische sleutels/certificaten. Toegang en gebruik van de beveiligde omgeving (digitale kluis) wordt gelogd en gemonitord. Afspraken rondom sleutelbeheer worden afgestemd tussen Opdrachtnemer en IVO Rechtspraak.	
S5	Security	Datascheiding	De oplossing van Opdrachtnemer biedt een dusdanige softwarematige zonering en segmentering binnen de aangeboden oplossing zodat IVO Rechtspraak een eigen afgeschermd omgeving heeft waar andere gebruikers van de oplossing (tenants) op geen enkele manier bij kunnen komen. Permanente isolatie van gegevens wordt gerealiseerd binnen een multi-tenant architectuur en patches en aanpassingen van applicaties en infrastructuur worden op een gecontroleerde wijze gerealiseerd. Isolatie van IVO-Rechtspraak gegevens wordt gegarandeerd door deze onder alle bedrijfsomstandigheden minimaal logisch te scheiden van de data van andere tenants.	
S6	Security	Interoperabiliteit en portabiliteit	Opdrachtnemer stelt de gegevens van IVO Rechtspraak beschikbaar middels gedocumenteerde Invoer- en uitvoerinterfaces in een formaat conform geldende industriestandaarden, waarbij de integriteit van de data aantoonbaar is geborgd. Met de gevens wordt bedoeld de inhoudelijke data, de gegevens die nodig zijn om toegang te krijgen en de logging gegevens.	
S7	Security	Koppelvlakken	Opdrachtnemer treft adequate maatregelen in op koppelpunten met externe of onvertrouwde zones om mogelijke aanvallen te signaleren en hierop te reageren.	
S8	Security	Logging	Opdrachtnemer zorgt dat er adequate logging is van elke handeling (toevoeging, wijziging, verwijdering) en dat deze herleidbaar is tot de eindgebruiker of beheerder. Het minimum wat gelogd moet worden: • Gebeurtenis; • Benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon (gebruiker of beheerder); • Resultaat van de handeling; • Datum en tijdstip van de gebeurtenis; • Duur van een handeling wordt gelogd, bijv. door het opslaan van een begin- en eindtijd; • Indien mogelijk ook het gebruikte apparaat.	
S9	Security	Malware-protectie	Opdrachtnemer heeft beheersmaatregelen geïmplementeerd voor detectie, preventie en herstel van malware-infecties; dit in combinatie met een passend bewustzijn van de gebruikers.	
S10	Security	Penetratietest	Opdrachtnemer beschikt over een recente (maximaal een jaar oud) penetratietest of is bereid om een penetratietest te laten uitvoeren. Opdrachtnemer is bereid om IVO Rechtspraak jaarlijks inzage te geven in de resultaten van penetratietesten.	
S11	Security	Security	Voor alle interactie met DNS servers wordt gebruik gemaakt van DNSSEC	
S12	Security	Security	Het onderliggende netwerk van de oplossing maakt voor publieke IP-adressen gebruik van RPKI	
I1	Inkoop	Licentiemanagement	Opdrachtnemer voorziet in licentiemanagement waarbij minimaal aangegeven wordt: * Naam van de licentie * Aantal licenties * Definitie gebruikte licentiemetriek * Gebruiksvoorwaarden * Rapportage licentieconsumptie uitgesplitst naar verbruikers * Licentie/abonnement verloop data * Thresholds ten aanzien van bijstelling van aantal benodigde licenties	