Functioneel gebruik

Nr.	Omschrijving	Toelichting
Werkplekken		
1.1	Rollen en rechten kunnen flexibel worden ingericht	Bepaalde collega's, zoals managementassistenten of facilitair medewerkers, moeten langer vooruit kunnen reserveren dan standaardmedewerkers. De rollen moeten flexibel in te richten zijn, bijvoorbeeld met de mogelijkheid om anderen uit te nodigen voor specifieke werkplekken.
Nieuw	Werkplek reservering moet mogelijk zijn via een integratie in Microsoft Outlook, Microsoft Teams, een mobiele App, of via een website.	
Nieuw	Gebruikers van het reserveringssysteem moeten inzichtelijk hebben wie waar zit en ook anderen op kunnen zoeken.	Om eventueel collega's op te zoeken moet er realtime op een plattegrond inzichtelijk zijn waar iemand zou kunnen zitten.
1.2	Er moet een mogelijkheid zijn om meerdere werkplekken in één keer te reserveren, bijvoorbeeld voor teams of projectgroepen	Indien nodig moet het reserveren van werkplekken voor groepen beperkt kunnen worden tot specifieke rollen
1.3	De beschikbaarheid van werkplekken moet inzichtelijk zijn, zodat gebruikers in real-time kunnen zien welke plekken beschikbaar zijn	Gebruikers moeten inzicht hebben in hoe lang werkplekken beschikbaar blijven, zodat ze kunnen zien tot wanneer een plek gereserveerd of vrij is
1.4	Er moet de mogelijkheid zijn om in te stellen hoeveel dagen of uren van tevoren een werkplek gereserveerd mag worden	
1.5	Er dient een functie te zijn die aangeeft wanneer een werkplek als no-show (is niet ingecheckt) wordt beschouwd, indien deze na een bepaalde tijd (bijvoorbeeld xx minuten) niet in gebruik is genomen. Tevens moeten de rapportages uitgebreidere informatie over no-shows verschaffen	De werkplek moet automatisch worden vrijgegeven na xx minuten als iemand niet opdraagt
1.6	Er moet een reserveermogelijkheid zijn voor aangepaste werkplekken voor collega's die arbovoorzieningen nodig hebben	Bijvoorbeeld speciale stoelen, stofvrije omgevingen, etc.
1.7	Medewerkers moeten kunnen inchecken met een QR sticker bij de werkplek, en een app.	
1.8	Er moeten uitgebreide rapportagemogelijkheden zijn, waarbij de minimale vereisten bestaan uit bezetting per uur en per dag, verdeeld over teams/afdelingen. Evenals gegevens over no-shows	Er moet inzicht zijn op zowel afdelings- als teamniveau
1.9	Het werkplekreserveringsoverzicht (plattegrond) moet naadloos integreren met het ruimtereserveringsoverzicht	Het moet één softwarepakket zijn waarin medewerkers zowel werkplek- als ruimtereserveringen kunnen beheren
Vergaderruimten en zalen		
1.10	Bij vergaderzalen moet er een voorziening zijn, zoals een room panel (display), waarmee in real-time de status van de vergaderkamer kan worden weergegeven (bezet, beschikbaar, aankomende reserveringen voor de dag).	
1.11		
1.12	Er moeten selectiemogelijkheden zijn die informatie bieden over de grootte en beschikbare voorzieningen van vergaderkamers. Dit moet omvatten het aantal personen dat in de kamer past, evenals de aanwezigheid van faciliteiten zoals een beeldscherm, camera en tekenborden, voor het ondersteunen van digitaal vergaderen	Er moet informatie beschikbaar zijn over het aantal plaatsen, Grote ruimte, videoconference, tekenborden, en andere voorzieningen die relevant zijn voor digitaal vergaderen.
1.13	Er moet een integratie met Microsoft Outlook en Teams zijn, zodat reserveringen eenvoudig in de agenda's van gebruikers kunnen worden weergegeven. Dit geldt voor Outlook online alsook de Outlook desktop applicatie (plug-in). Bij het maken van een afspraak in Outlook moeten er meteen mogelijkheden zijn om ook de catering en voorzieningen te boeken. Dit mag geen aparte handeling zijn.	De beschikbare vergaderkamers moeten weergegeven en geselecteerd kunnen worden tijdens het plannen van een afspraak
1.14	De ruimte moet als no-show worden gemarkeerd als deze na 15 minuten nog niet in gebruik is.	De ruimte moet automatisch worden vrijgegeven als er niemand komt opdagen
1.15	De no show moet ook gesignaleerd worden door aanwezigheidssensoren in de ruimte.	
1.16	Het reserveringssysteem moet óf 1) de aanwezigheidssensoren van bestaande Yealink Teams Rooms systemen ondersteunen, óf 2) door middel van nieuwe te-installeren ruimtesensoren. De hardware specificaties voor deze eventuele nieuwe sensoren zijn opgenomen in een aparte hardware eis.	

1.17	Reserveren moet mogelijk zijn in (meerdere) eenheden van 15 minuten	
1.18	Het moet mogelijk zijn om meerdere reserveringen vooruit te maken	Bijvoorbeeld met de mogelijkheid om elke twee weken of met een andere frequentie te reserveren
1.19	Het moet mogelijk zijn om bepaalde medewerkers overstijgende authorisaties te geven over reserveringen van bepaalde ruimtes (een workflow voor goedkeuring van de gewenste reservering)	Bv de raadzaal. Deze is te reserveren, maar na goedkeuring van de bodes, zij hebben inzicht in andere planning. Zo ook voor het Posthuis theater, waar deze medewerkers met hun eigen planning software werken die zij moeten cross-checken alvorens een reservering finaal kan worden gemaakt.
1.20	Per vergaderruimte kunnen afwijkende 'openingstijden' gelden, dit moet in te regelen en zichtbaar zijn voor de gebruiker.	
Divers		
1.21	Bij het reserveren van een vergaderruimte moet het ook mogelijk zijn om koffie, thee of lunch mee te reserveren	
1.22	Bij het reserveren van een vergaderruimte moet het ook mogelijk zijn om faciliteiten te regelen, zoals beamer, flipover enz	
1.23	Er moet een mogelijkheid zijn om autorisaties aan te brengen bij medewerkers. BV: niet iedere medewerker heeft de mogelijkheid om catering te bestellen; ledere medewerker heeft wél de mogelijkheid om faciliteiten te regelen.	
1.24	Wanneer er een reservering is gemaakt waarbij catering of andere diensten/producten moeten worden geleverd, dan moeten deze aangevraagde items bij specifieke personen terechtkomen (bodes, facilitair) binnen het reserveringssysteem als zijnde taken. Deze moeten voor de reserverende gebruiker ook inzichtelijk zijn qua status (Goedgekeurd, afgehandeld, afgewezen).	
1.25	Er moet een mogelijkheid zijn om lijstwerk oid te kunnen uitdraaien van afgenomen cateringdiensten ivm interne facturering.	
1.26	Het moet mogelijk zijn om een reservering te maken voor een andere persoon (iemand moet gemachtigd/gedelegeerd worden met reserveringsrechten).	Een managementassistente moet in staat zijn om reserveringen te maken namens xxx
1.27	Er moeten duidelijke plattegronden beschikbaar zijn, zodat elke verdieping en vleugel gemakkelijk te vinden is	
1.28	In het reserveringsplatform moet de mogelijkheid zijn om foto's van werkplekken en vergaderruimtes weer te geven	
1.29	Er moet een dashboard zijn met rapportages over de bezetting, afgenomen cateringdiensten, en producten.	
1.30	Er moet een mogelijkheid tot koppeling met Power BI zijn	
1.31	Er moet een mogelijkheid tot exporteren zijn van rapportages naar Excel format.	
Digital signage		
1.32	Op vier strategische locaties in het gemeentehuis wordt via beeldschermen inzichtelijk gemaakt waar op de verdieping nog beschikbare werkplekken en vergaderruimtes zijn.	
1.33	De display informatie op de digital signage schermen moet aangepast kunnen worden naar wens, zodat bijvoorbeeld niet volledige namen van personen of vergaderingen worden weergeven, maar slechts ‘bezet’ of ‘vrij’ per vergaderruimte.	
Extra opties		
1.34	Inchecken moet mogelijk zijn via stickers met QR code of eenvoudigweg in de app op een apparaat.	
Overige		
1.35	De reserveringsapp/web moet digitoegankelijk zijn, zodat ook visueel gehandicapten er gebruik van kunnen maken	zie ook www.digitoegankelijk.nl

Functioneel beheer

Nr.	Omschrijving	Toelichting
Functioneel beheerprocessen en -taken		
2.1	Beheertaken moeten kunnen worden uitgevoerd zonder invloed op de werking van de oplossing voor andere gebruikers. Gebruikers moeten ingelogd kunnen blijven en volledig gebruik kunnen maken van de oplossing tijdens deze beheerwerkzaamheden	
2.2	Alle beheertaken moeten door de gemeente kunnen worden uitgevoerd via een gebruiksvriendelijke grafische gebruikersinterface (GUI)	
2.3	Er moet een duidelijke en up tot date online help center zijn waarbij een functioneel beheerder eenvoudig zelf documentatie kan zoeken en doornemen,	
2.4	De plattegronden met beschikbare werkplekken en vergaderruimten moeten eenvoudig en door de gemeente zelf aanpasbaar zijn. Plattegronden moeten óf getekend kunnen worden in het reserveringssysteem, óf geupload kunnen worden in gangbare bestandsformaten (PDF, dwg, svg, bmp, jpg).	
2.5	Er moeten adminrechten zijn die het mogelijk maken om andere rollen en rechten aan te maken en toe te wijzen	Opdrachtgever creëert zelf de verschillende rollen met bijbehorende rechten en wijzen deze toe aan de betreffende collega's
2.6	De helpdesk dient Nederlands te spreken	
2.7	Alle benodigde software-updates, inclusief beveiligings- en functionele updates, dienen gedurende de contractperiode kosteloos te worden geleverd en zijn inbegrepen in de totaalprijs.	

Technisch (beheer)

Nr.	Omschrijving	Toelichting
Configuratie		
3.1	De leverancier verzorgt de technische implementatie.	
3.2	De applicatie wordt aangeboden als een Software-as-a-Service (SaaS) oplossing	
3.3	Gebruikers van het reserveringssysteem worden provisioned middels een SCIM koppeling met een onze IDP systemen; HelloID of via Entra ID.	
3.4	Gebruikers van het reserveringssysteem worden geauthentiseerd middels Single Sign-On (SSO) op basis van Microsoft Entra ID.	
3.5	Leverancier stelt een online helpcenter (Nederlands) beschikbaar waar de gemeente kan vinden wat er benodigd is voor de functionele en technische inrichting.	
3.6	Displays voor vergaderplekken dienen te voldoen aan de volgende hardware eisen: • Scherm: 10” Touchscreen. • Voeding: via 230V (al dan niet met adapter) • Connectiviteit: ethernet, Wi-Fi 6 (802.11ax) • Security: 802.1x ondersteuning o.b.v. apparaat certifcaten • OS: Geen Eisen, anders dan up-to-date software/security ondersteuning voor de looptijd van het contract • Provisioning/management via Intune, of via de aanbestedende reserveringssoftware • Montage: display moet zowel op een muur als glas gemonteerd kunnen worden. Additionele eisen voor displays voor kleine spreekkamers en vergaderplekken • Scherm: maximaal 7 ” Touchscreen	
	Voor de Digital Signage schermen gelden de volgende eisen:	

3.7	• Scherm: 32 tot 43 inch • Deze schermen dienen geschikt te zijn voor langdurig gebruik en continu aan te kunnen staan tijdens kantoortijden (digitale signage): 07:30-18:00 • Voeding: 230V • Connectiviteit: ethernet en/of WiFi 6 (802.11ax) • Security: 802.1x ondersteuning • Remote management mogelijkheid via web-interface of eigen management software • Montage: Wand- of plafondbeugel (in overleg)	
3.8	Ruimtesensoren : • Voeding: 230V of via batterij. PoE is *niet* mogelijk • Montage: plafond • Connectiviteit: Wi-Fi 6 (802.11ax) of andere (radio) verbinding met bijv. een room display • Security: indien Wi-Fi; 802.1x o.b.v. certificaat	
Platform		
3.9	Eventuele benodigde plug-ins voor integratie in Microsoft Outlook en Teams ondersteunen de Stable Channel van de Microsoft 365 desktop apps voor Windows.	
3.10	Eventuele benodigde plug-ins voor integratie met Microsoft Outlook en Teams werken óók in de web omgevingen van deze applicaties.	
3.11	De oplossing ondersteunt minimaal de één-na-laatste versies van Microsoft Edge browser.	
3.12	Een mobiele app-oplossing voor mobiele apparaten ondersteunt zowel iOS als Android	
3.13 3.14	Aanleveren security methodiek van de ruimtesensoren ter toetsing voor de CISO. Score op internet.nl moet boven de 95% uitkomen	
Support		
3.15	De leverancier biedt een deskundige servicedesk voor IT-meldingen en vragen, die fungeert als tweedelijnsondersteuning. Deze servicedesk staat rechtstreeks in contact met de gemeentelijke servicedesk en beheerders van gemeente. De medewerkers van de servicedesk moeten het Nederlands zowel mondeling als schriftelijk goed beheersen.	
3.16	De leverancier levert een schematische weergave van de gehele installatie (reserveringssysteem, displays, roomsensoren, en de afhankelijkheden/communicatie flows tussen deze).	Beschrijft hoe de informatie naar de tablets in het gebouw en naar de apps op de devices gecommuniceerd, hoe zit het met beveiliging van de informatie. Tevens de technische informatie voor de lan/wifi communicatie van room-displays, sensoren met het internet/reserveringssysteem.

Informatieveiligheid

Nr.	Omschrijving	Toelichting
Standaarden, wet- en regelgeving		
5.1	De leverancier dient een goedgekeurde verwerkersovereenkomst (als onderdeel van de hoofdovereenkomst) van de VNG te hebben (vereniging nederlandse gemeente)	
5.2	De leverancier zorgt dat de applicatie en de onderliggende ICT-infrastructuur voldoet aan de eisen op het gebied van de informatiebeveiliging die zijn vastgelegd in de Baseline Informatiebeveiliging Overheid.	Aantoonbaar via certificering. ISO 27001
5.3	De leverancier garandeert dat de applicatie en de ondersteunende processen voldoen aan de Algemene Verordening Gegevensbescherming (AVG). Daarnaast levert de leverancier een overzicht van alle genomen privacymaatregelen, bijvoorbeeld in de vorm van een risicoanalyse	
5.4	De leverancier kan input leveren aan een DPIA	
Logging		

5.5	De leverancier biedt uitgebreide loggingsmogelijkheden die voldoen aan de vereisten van de Baseline Informatiebeveiliging Overheid	
Autorisatie		
5.6	Autorisaties worden verstrekt volgens de hierarchie van Active Directory-management en Office 365 (zoals OneDrive, Teams, etc.)	
5.7	Er is een duidelijke scheiding tussen gebruikersautorisaties en beheer-/adminautorisaties	
5.8	Beheer-/adminrollen moeten voldoen aan de eisen van het gemeentelijke wachtwoordbeleid en moeten kunnen worden gekoppeld aan MFA-toepassingen	
Technische documentatie & conformiteit		
5.9	Leverancier levert vóór gunning een technisch dossier	systeemarchitectuur (componenten, interfaces, netwerkdiagrammen, dataflows), overzicht beveiligingsmaatregelen (crypto, authenticatie/autoristatie, hardening), cybersecurity-risicobeoordeling met mitigaties, testresultaten (laatste 12 maanden) incl. pentest-/fuzzingrapport(en) en remediate-status, proces kwetsbaarhedenbeheer en update-keten (inclusief signing).
5.10	Leverancier levert een beheer- en installatiemanual met veilige standaardconfiguratie, roll-back, en factory-reset naar secure baseline	
5.11	De leverancier garandeert dat er geen persoonsgegevens worden (laten) verwerken buiten de EER	
5.12	De leverancier voldoet aan de in de BIO 1.04 gestelde eisen die aan de leverancier worden toegekend voor een BBN 2 oplossing.	
5.13	De leverancier is ISO27001 gecertificeerd en kan hiervoor de VVT ook aanleveren.	
5.14	De ISO27001 wordt jaarlijks door en auditverklaring als een ISAE3402 type 2 of SOC 2 aan te leveren.	Door de auditverklaring te kunnen leveren kan de opdrachtgever controleren of de in de ISO27001 gedefineerde maatregelen ook over de gecontroleerde periode afdoende zijn gebleken.
5.15	Gebruik van algoritmen in de oplossing gedurende de looptijd worden vooraf open en transparant aan de opdrachtgever voorgelegd en de opdrachtgever kan beoordelen of deze algoritmen mogen worden toegepast in de omgeving van de opdrachtgever.	
Security by design & default		
5.16	Oplossing wordt geleverd met secure-by-default instellingen: alle niet-noodzakelijke services/interfacen uit.	Niet alleen op de software componenten maar ook op de hardware onderdelen van de oplossing van toepassing.
5.17	Levering gebeurt zonder bekende, exploiteerbare kwetsbaarheden	
5.18	De leverancier draag zorg dat ook bij eventuele onderaannemers of gebruikte componenten het security by design principe wordt geborgd.	
Kwetsbaarhedenbeheer & updates		
5.19	Security-updates worden geleverd kosteloos gedurende de afgesproken ondersteuningsperiode (minimaal 5 jaar na oplevering) en los van feature-updates wanneer technisch mogelijk.	

5.20	De leverancier heeft een proces hoe om te gaan met patching van security kwetsbaarheden in de oplossing gedurende de periode dat de oplossing wordt geleverd.	Welke garanties worden er door de leverancier aangehouden met betrekking tot kwetsbaarheden die aangetroffen worden in de oplossing. Daarbij rekening houdende dat bepaalde kwetsbaarheden voor de opdrachtgever belangrijk zijn dat ze zo spoedig mogelijk opgelost moeten worden maar ook dat kwetsbaarheden in de software die niet extern misbruikt kunnen worden maar wel bijvoorbeeld een CVSS score van 7 of hoger zouden hebben.
5.21	Welke termijn (jaren) garandeert de leverancier (security) updates op de gehele oplossing? Voor de opdrachtgever is het uitgangspunt dat dit minimaal 5 jaar na oplevering zou moeten zijn tenzij anders overeengekomen.	Er mag in dit overzicht onderscheid per component worden aangegeven en de termijn waarop de onderdelen worden voorzien van security updates.
Testen & acceptatie (security assurance)		
5.22	Onafhankelijke pentest (CREST/TIBER/ vergelijkbaar) op backend, API en devices ≤ 12 maanden oud;	
5.23	Jaarlijkse laten uitvoeren van technische security testen tijdens contractduur van de oplossing, Deze testen hoeven niet specifiek op de oplossing van de oplossing van de opdrachtgever te zijn uitgevoerd maar mogen generiek zijn uitgevoerd; rapporten gedeeld met opdrachtgever.	
5.24	Leverancier kan aantoonbaar maken dat gebruikte derde partij oplossingen ook jaarlijks worden onderworpen aan technische security testen.	
Logging, monitoring & tijdsync		
5.25	Security-relevante gebeurtenissen worden gelogd (auth/z, config-wijzigingen, admin-acties, update-events, device-status)	
5.26	Logs onveranderbaar opgeslagen ≥ 180 dagen en hier vind ook een controle op dat deze niet zijn/worden gemuteerd tijdens die periode.	
5.27	Alle componenten gebruiken betrouwbare tijdssynchronisatie	
Toegang & identiteit		
5.28	Voor de gebruikers toegang wordt er gebruik gemaakt van SSO op basis van EntraID.	
5.29	Voor beheerders toegang beschikt de applicatie over de mogelijkheid om via Thycotic toegang tot de beheerders oplossingen.	
5.30	Toegang tot onderdelen van de oplossingen wordt geregeld middels RBAC en zijn ingericht op basis van least-privilege toegang.	
Data- en privacybescherming		
5.31	Encryptie: data in rust AES-256 (of gelijkwaardig) en tijdens Transport Layer Security (TLS) Beveiligingsrichtlijnen versie 2025-05 met HSTS/modern ciphers.	De leverancier volgt ook eventuele aanpassingen en updates op de richtlijn van het NCSC over de SSL beveiliging
5.32	Dataminimalisatie en retentiebeleid (bewaartermijnen & purge-mechanismen) zijn gedocumenteerd en kunnen met de opdrachtgever worden gedeeld.	
5.33	De leverancier kan input leveren aan een DPIA	
5.34	De leverancier dient een goedgekeurde verwerkersovereenkomst (als onderdeel van de hoofdovereenkomst) van de VNG te hebben (vereniging nederlandse gemeente)	
Software supply chain & SBOM		
5.35	Leverancier levert SBOM in SPDX of CycloneDX (machine-leesbaar) met minimaal top-level dependencies en versies.	
5.36	Leverancier heeft een proces om SBOM actueel te houden en impactanalyses te leveren binnen 10 werkdagen na nieuwe CVE's.	
5.37	Richtlijn voor gebruik van open-source (licenties, update-beleid); geen end-of-life libraries.	
Fysieke componenten		
5.38	Secure boot, signed firmware en over-the-air updates met rollback.	
5.39	Kiosk-mode: fysieke poorten (USB, debug, SD) uit of policy-gecontroleerd; alleen noodzakelijke netwerkpoorten open.	
5.40	802.1X-support of gelijkwaardig voor netwerktoegang; device attestation waar mogelijk.	
5.41	Remote beheer via MDM/EMM of vendor tooling met auditable acties.	

5.42	Tamper-detectie en veilige factory reset.	
Beschikbaarheid & weerbaarheid		
5.43	Essentiële functies blijven beschikbaar bij storing (fail-safe/queued check-ins op devices)	Welke maatregelen zijn er genomen om uitval, of gedeeltelijke uitval, van onderdelen in de gehele oplossing te mitigeren.
Incidentrespons & communicatie		
5.44	Leverancier stelt een 24×7 meldpunt beschikbaar voor security-incidenten/kwetsbaarheden.	
5.45	De leverancier hanteert de volgende meldingstermijnen bij informatiebeveiligings- en privacy-incidenten: initiële melding binnen 24 uur, vervolgrapport binnen 72 uur en eindrapport binnen 14–30 dagen (incl. oorzaak, impact, mitigaties).	
Ondersteuning & toekomstbestendigheid		
5.46	levenscyclusbeheer van minimaal 5 jaar die security-updates, helpdesk, compatibiliteit waarborgen alsmede de levenscyclusbeheer van fysieke componenten in de oplossing worden hierin geborgd.	
5.47	Hoe organiseert u levenscyclusbeheer en ondersteuning (bijv. 5–10 jaar)?	
5.48	Einde-levensduur beleid met migratiepad en dataverwijdering.	
5.49	Leverancier committeert zich om uiterlijk in 2027 volledig te voldoen aan de verplichtingen voortvloeiend uit de Cyber Resilience Act.	
5.50	Leverancier levert een roadmap waarin is opgenomen hoe het systeem compliant wordt en blijft aan de Cyber Resilience Act.	
Contractueel & audits		
5.51	Opdrachtgever heeft recht op een jaarlijkse security-review/audit (redelijke aankondiging) incl. inzage in relevante stukken (SBOM, testresultaten, patchlog).	
5.52	De leverancier is verantwoordelijk dat alle gestelde eisen in de aanbesteding ook toepasbaar zijn op eventuele onderaannemers die in de verwerkingsovereenkomst moeten zijn opgenomen alsmede dat gebruikte (standaard) componenten van de oplossing hieraan voldoen.	