

Provincie Noord-Brabant

Programma van Eisen - SMT - Versie 1

ID	ONDERDEEL	BESCHRIJVING	PRIO
FUNCTIONEEL			
FUNC-1	Algemeen	SMT biedt de mogelijkheid aan gebruikers om zelf meldingen aan te maken, daarnaast kunnen back-end users meldingen voor een ander aanmaken onder zijn/haar naam.	EIS
FUNC-2	Algemeen	SMT biedt een overzicht, import en zoekmogelijkheden van alle objecten behorende bij een medewerker of computerID. Zoals: Welke laptop, smartphone, artikelcode, e.d.	EIS
FUNC-3	Algemeen	De aangeboden SMT moet worden geïnstalleerd op de Azure IaaS omgeving van de provincie Noord-Brabant.	EIS
FUNC-4	Algemeen	SMT moet de mogelijkheid bieden om aanvullende, aangepaste velden toe te voegen, zodat de inrichting kan worden afgestemd op specifieke behoeften van de organisatie.	EIS
FUNC-5	Algemeen	SMT moet standaard voorzien zijn van een workflow-functionaliteit die flexibel kan omgaan met verschillende vormen van procesrouting. Hierbij moet de mogelijkheid bestaan om processtappen zowel parallel, sequentieel, conditioneel als iteratief te laten verlopen.	EIS
FUNC-6	Algemeen	SMT moet de mogelijkheid bieden om SLA-diensten automatisch te koppelen aan meldingen en de KPI's van deze diensten op te nemen in rapportages, zodat de prestaties ten opzichte van de overeengekomen servicelevels inzichtelijk zijn.	EIS
FUNC-7	Algemeen	SMT moet de mogelijkheid bieden om sjablonen te gebruiken die gebruikers ondersteunen bij verschillende processen, zodat consistentie wordt gewaarborgd en de efficiëntie wordt verhoogd.	EIS
FUNC-8	Algemeen	SMT moet meldingen automatisch kunnen registreren wanneer deze via het Self Service Portal of per e-mail worden ingediend, zodat het proces voor het indienen van meldingen eenvoudig en efficiënt verloopt.	EIS
FUNC-9	Algemeen	SMT biedt de mogelijkheid om de bron vast te leggen van de binnengekomen melding. Denk aan SSP, telefonisch, mail, etc.	EIS
FUNC-10	Algemeen	SMT biedt de mogelijkheid om bijlagen te kunnen uploaden in zowel de Self Service Portal als in de back-end bij de verschillende type meldingen.	EIS
FUNC-11	Algemeen	SMT moet de mogelijkheid bieden om via een audit trail de belangrijkste activiteiten en handelingen binnen de procesflows te registreren, zodat inzicht in de geschiedenis wordt verkregen en bewijsvoering is geborgd.	EIS
FUNC-12	Algemeen	SMT moet aanpasbare nagenoeg realtime dashboards bieden, afgestemd op de specifieke behoeften van verschillende rollen of teams, met relevante prestatie-indicatoren en operationele gegevens	EIS
FUNC-13	Algemeen	SMT moet de integratie tussen verschillende processen ondersteunen, inclusief het koppelen/relateren van meldingen zoals incidenten, problemen, changes en releases, om een naadloze samenwerking en gegevensuitwisseling tussen deze processen te waarborgen.	EIS
FUNC-14	Algemeen	SMT moet de mogelijkheid bieden om prioriteiten voor incidenten, problemen, changes en releases in te stellen op basis van impact en urgentie, zodat de juiste volgorde van afhandeling wordt gewaarborgd.	EIS
FUNC-15	Algemeen	SMT moet ondersteuning bieden voor het classificeren van meldingen in categorieën en subcategorieën, zodat een gestructureerde indeling en efficiënte afhandeling mogelijk is	EIS
FUNC-16	Algemeen	SMT moet de mogelijkheid bieden om workflows automatisch te routeren op basis van de classificatie van meldingen, zodat taken efficiënt aan de juiste behandelaar of afdeling worden toegewezen.	EIS
FUNC-17	Algemeen	SMT moet de mogelijkheid bieden om de prioriteitenmatrix per proces en per leverancier aan te passen, zodat de prioritering nauwkeurig kan worden afgestemd op de specifieke eisen van elk proces en iedere leverancier.	EIS
FUNC-18	Algemeen	SMT moet out-of-the-box ondersteuning bieden voor ITIL-processen, zodat best practices direct kunnen worden toegepast zonder uitgebreide maatwerkconfiguratie.	EIS
FUNC-19	Algemeen	SMT biedt de mogelijkheid om vanuit één melding meerdere taken uit te kunnen zetten naar meerdere oplosgroepen.	EIS
FUNC-20	Gebruikersinterface	SMT moet een functie bieden om in alle beschikbare data te zoeken vanuit één enkel zoekveld, waarbij rekening wordt gehouden met de autorisaties van de gebruiker.	EIS
FUNC-21	Gebruikersinterface	De webinterface van de SMT moet voldoen aan responsive webdesign, zodat de interface zich automatisch aanpast aan het apparaat waarop deze wordt gebruikt.	EIS
FUNC-22	Gebruikersinterface	SMT moet notificaties kunnen genereren en versturen, zowel handmatig als automatisch, op basis van vooraf gedefinieerde gebeurtenissen binnen het systeem.	EIS
FUNC-23	Gebruikersinterface	Notificaties die worden gegenereerd en verzonden, moeten worden vastgelegd bij de specifieke gebeurtenis die de notificatie heeft veroorzaakt, zodat de volledige communicatiehistorie inzichtelijk blijft.	EIS
FUNC-24	Gebruikersinterface	Notificaties moeten vooraf kunnen worden gedefinieerd en door beheerders aangepast, waarbij in de inhoud van de notificatie waarden uit velden binnen het systeem kunnen worden opgenomen voor gepersonaliseerde en contextspecifieke communicatie.	EIS
FUNC-25	Autorisatie	SMT moet een Role Based Access Control (RBAC) model ondersteunen voor zowel data als functionaliteit, op minimaal persoon- en rolniveau.	EIS
FUNC-26	Autorisatie	SMT moet verschillende autorisatieniveaus ondersteunen, zodat toegang tot gegevens en functionaliteiten afhankelijk kan worden gemaakt van de rol of bevoegdheid van de gebruiker.	EIS
FUNC-27	Autorisatie	SMT moet ervoor zorgen dat een gebruiker in de gebruikersinterface geen opties ziet waarvoor hij/zij niet is geautoriseerd, zodat de interface overzichtelijk en toegespitst blijft op de toegestane functionaliteiten.	EIS
FUNC-28	Self service	De SMT-tool beschikt over een Selfservice portal.	EIS
FUNC-29	Self service	Vanuit de Selfservice portal is toegang tot de knowledge database mogelijk.	EIS
FUNC-30	Self service	SMT moet ervoor zorgen dat (eind)gebruikers op basis van hun rol en autorisatie alleen de items van de servicecatalogus zien waarvoor zij rechten hebben, zodat de interface relevant en overzichtelijk blijft.	EIS
FUNC-31	Self service	SMT biedt de mogelijkheid om vanuit de Selfservice portal een melding naar de (interne) helpdesk te sturen.	EIS
FUNC-32	Self service	SMT biedt de mogelijkheid om vanuit de selfservice Request Fulfilment bestellingen te plaatsen en volgen.	EIS
FUNC-33	Self service	SMT biedt de mogelijkheid de status van meldingen en/of bestellingen op te vragen (zowel individueel als rol gebaseerd).	EIS
ITIL - ICT			
ITIL-1	Asset & Configuration Management	SMT moet in staat zijn om vanuit de geborgde processen informatie te ontsluiten vanuit en naar het CMDB.	EIS
ITIL-2	Asset & Configuration Management	SMT moet de mogelijkheid bieden om het CMDB automatisch bij te werken naar aanleiding van wijzigingen aan een configuratie-item (CI), of wanneer een CI nieuw wordt uitgegeven of ingenomen, zodat de gegevens altijd actueel zijn.	EIS
ITIL-3	Asset & Configuration Management	SMT moet de mogelijkheid bieden om de status van configuratie-items (CI's) bij te houden, zoals 'operationeel', 'onderhoud' of 'buiten gebruik', zodat de actuele status altijd inzichtelijk is.	EIS
ITIL-4	Change Management ITIL	SMT moet de mogelijkheid bieden om autorisatieflows voor changes in te richten op basis van impact en prioriteit, zodat de juiste personen betrokken worden bij besluitvorming afhankelijk van de ernst en het belang van de change.	EIS
ITIL-5	Change Management ITIL	SMT moet ondersteuning bieden voor de verslaglegging binnen change management, waaronder impactanalyse, informatieadvies, plan van aanpak (PvA), en testverslagen, zodat het gehele proces goed gedocumenteerd en traceerbaar is.	EIS
ITIL-6	Change Management ITIL	SMT moet een change-kalender bieden die een overzicht geeft van alle geplande wijzigingen, zodat betrokkenen tijdig inzicht hebben in aankomende veranderingen en de impact op andere processen kunnen beoordelen.	EIS

ITIL-7	Change Management ITIL	SMT moet ondersteuning bieden voor verschillende typen changes, zoals standaard, spoed en normale changes, met elk hun eigen autorisatieprocedures, zodat het changeproces flexibel kan worden afgestemd op de specifieke urgentie en aard van de wijziging.	EIS
ITIL-8	Knowledge Management	SMT moet een kennisdatabase bieden die oplossingen en handleidingen bevat, zodat gebruikers en behandelaars snel toegang hebben tot relevante informatie voor probleemoplossing en ondersteuning.	EIS
ITIL-9	Release Management	SMT moet ondersteuning bieden voor release management waarbij changes gebundeld kunnen worden voor planningsdoeleinden, zodat wijzigingen efficiënt en gecoördineerd kunnen worden doorgevoerd.	EIS
FACILITAIR			
FACI-1	Reserveringen	Via de SMT is het mogelijk om ruimtes te reserveren, wijzigen of annuleren. Hierbij kan worden aangegeven voor hoeveel personen de reservering is en welke ruimtes voor dergelijk aantal daarbij passen.	EIS
FACI-2	Reserveringen	SMT voorziet bij het reserveren van een ruimte in een overzicht waarbij per dag en tijdseenheid te zien is welke ruimtes beschikbaar zijn.	EIS
FACI-3	Reserveringen	SMT biedt de mogelijkheid om, d.m.v. een bidirectionele koppeling tussen smt en software, via schermen in de hal en bij displays bij de vergaderruimtes de dagstaat met gereserveerde ruimtes te tonen. Bij de vergaderdisplays is het mogelijk om de reservering te bekijken, wijzigen of annuleren.	EIS
FACI-4	Reserveringen	Via de SMT is het mogelijk om objecten te reserveren, wijzigen of annuleren zoals: Workshopkoffers, NS Businesscards, Representatiepassen, leenfietsen of verbruiksartikelen (via catering).	EIS
FACI-5	Reserveringen	SMT biedt de mogelijkheid tot een overzicht van alle reserveringen. Dit voor specifieke accounts zoals front office zodat zij rerveringen eventueel kunnen verschuiven wanneer nodig.	EIS
FACI-6	Reserveringen	SMT biedt de mogelijk om repeterende reserveringen aan te maken.	EIS
FACI-7	Reserveringen	SMT biedt de mogelijkheid om objecten/artikelen te koppelen aan een gereserveerde ruimte. Denk daarbij aan een flipover.	EIS
FACI-8	Reserveringen	Het reserveren van catering of ondersteuning van evenementen verloopt via het systeem. Voor deze reservering wordt een prijscalculatie gemaakt. Hiervoor moeten de voorzieningen kunnen worden voorzien van een prijs en moet er een selectie/rapportage gemaakt kunnen worden van de kosten van evenementen per periode/event.	EIS
FACI-9	Bestellingen	SMT biedt de mogelijkheid om voor jezelf of een ander, artikelen te bestellen. Wat men kan bestellen is per account verschillend (gebruiker of manager). Artikelen zijn o.a.: Relatiegeschenken, bloemen, cadeaukaarten.	EIS
FACI-10	Bestellingen	SMT biedt de mogelijkheid om in de voorraad, producten toe te voegen of bij te werken.	EIS
FACI-11	Bestellingen	SMT voorziet gedurende de afhandeling van een bestelling, de aanvrager van statusupdates	EIS
FACI-12	Catalogi	Er is onderscheid tussen meerdere groepen (medewerkers, managers) die uit verschillende catalogi kunnen kiezen, zoals catering en ruimtes en met verschillende kostenplaatsen.	EIS
ARCHITECTUUR			
ARCH-1	Standaarden	SMT dient te voldoen aan de webrichtlijn zoals in WCAG 2.1 weergegeven.	EIS
ARCH-2	Koppelingen	SMT moet ondersteuning bieden voor realtime informatie-uitwisseling met leveranciers en hun SMT-systemen, via API's of andere integraties, om processen te koppelen aan elkaar en naadloze samenwerking en actuele gegevensuitwisseling te faciliteren.	EIS
ARCH-3	Koppelingen	SMT moet ondersteuning bieden voor koppelingen via API's of e-mail, zodat het SMT kan integreren met andere interne systemen bij de provincie Noord-Brabant, zoals SAP, DataWarehouse en Azure DevOps, om gegevens op te halen of te ontsluiten voor een efficiënte informatie-uitwisseling.	EIS
ARCH-4	Data	Gegevens over het ontstaan, de beveiliging, de beschikbaarheid, het gebruik, het beheer en de verwijdering van informatie moeten worden vastgelegd in gegevens. Service Management Tool moet hiervoor ingericht zijn, of worden ingericht.	EIS
ARCH-5	Data	Data en systemen worden geacht te voldoen aan het backup-beleid van de provincie Noord-Brabant.	EIS
ARCH-6	Data	Inschrijver moet aansluiten op de centrale back-up voorziening van de provincie Noord-Brabant (Commvault Metallic).	EIS
ARCH-7	Ontwikkelstraat	Er is minimaal A(acceptatie) of Pre-productie omgeving beschikbaar, waarop getest kan worden.	EIS
BEVEILIGING			
BEVE-1	Beveiliging	De inschrijver is BIO compliant. De BIO is een uitbreiding op de ISO27001/02 welke betrekking heeft op de dienstverlening.	EIS
BEVE-2	Beveiliging	De inrichting en levering van de dienst / systeem is conform de maatregelen die van toepassing zijn, zoals gesteld in de Baseline Informatiebeveiliging Overheid afgekort BIO.	EIS
BEVE-3	Beveiliging	Het basisbeveiligingsniveau vanuit de BIO voor de inrichting van de dienstverlening / systeem is minimaal BBN2. De BIO vermeld welke maatregelen binnen deze classificatie vallen. De classificatie of Basis Beveiligingsniveau zoals beschreven in de BIO wordt bepaald aan de hand van een BIA (Beveiliging Informatie Analyse). Minimaal voldoen aan onderstaande regel in BIO: De beschikbaarheid wordt als volgt gekwantificeerd: • Kantoorautomatisering en organisatiespecifieke systemen hebben tijdens openingstijden een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes. • Maximaal dataverlies 24 uur. • Maximale hersteltijd in geval van incidenten is binnen 16 werkuren (twee dagen van 8 uur).	EIS
BEVE-4	Beveiliging	De SMT wordt geleverd conform gestelde richtlijnen inzake informatiebeveiliging vanuit de provincie Noord-Brabant waar die van toepassing zijn. Deze richtlijnen zijn uitwerkingen van maatregelen vanuit de BIO door de provincie Noord-Brabant en zijn vastgesteld door de directie.	EIS
BEVE-5	Beveiliging	Bij de inrichting van de SMT moet deze worden geconfigureerd volgens de overheidsstandaarden zoals die zijn gesteld door het Forum Standaardisatie vanuit de Rijksoverheid. Zie ook link in acceptatiecriteria.	EIS
BEVE-6	Beveiliging	Bij Azure IaaS configuratie en/of applicaties dient de inrichting van de ICT-infrastructuur (door de leverancier) minimaal te voldoen aan de structuur zoals beschreven in de Blauwdruk Security Architectuur, opgesteld door de provincie Noord-Brabant of beter.	EIS
BEVE-7	Beveiliging	Alle communicatie tussen, met en naar SMT vindt plaats over beveiligde verbindingen.	EIS
BEVE-8	Beveiliging	Data opslag, data verwerking en syste(e)m(en) bevinden zich binnen de grenzen van de Europese Economische Ruimte: EER / EU landen.	EIS
BEVE-9	Beveiliging	De data binnen SMT wordt versleuteld opgeslagen.	EIS
BEVE-10	Beveiliging	De SMT heeft een mechanisme dat ingebrachte data controleert op mogelijke malware.	EIS
BEVE-11	Beveiliging	Er is een actief patch- en updatebeleid waarin beveiligingsupdates worden geprioriteerd.	EIS
BEVE-12	Beveiliging	Kwetsbaarheden, waarbij zowel de kans als het risico hoog is aangemerkt, worden binnen 5 dagen na het uitkomen van updates bijgewerkt. Tot die tijd worden er mitigerende maatregelen ingezet.	EIS
BEVE-13	Beveiliging	De inschrijver zorgt dat het N, N-1 beleid actief wordt ingevuld. Dit houdt in dat, aangezien de provincie Noord-Brabant een stabiele omgeving wenst, de softwareversies op versie N zijn (= huidige beschikbare productversie van de software), en alleen bij uitzondering (tijdelijk) N-1 mag zijn. Daarbij worden (ook) alle applicaties, die worden aangeboden vanuit de Microsoft Store, automatisch bijgewerkt zodra er een update beschikbaar komt. De configuratie moet dusdanig zijn, dat de eindgebruiker hier niet/minimaal door wordt lastig gevallen, waarbij het werk wordt onderbroken.	EIS
BEVE-14	Beveiliging	De authenticatie voldoet aan Modern Authentication (AAD).	EIS

BEVE-15	Beveiliging	Om te kunnen inloggen in het beheer-gedeelte van de website/omgeving is Multi Factor Authentication (MFA) toepasbaar. Dit kan via SSO van de opdrachtgever of MFA van de leverancier.	EIS
BEVE-16	Beveiliging	MFA moet minimaal gelden voor alle toegang op provincie Noord-Brabant gegevens vanaf een onvertrouwde zone.	EIS
BEVE-17	Beveiliging	Step-up authenticatie: de gebruiker krijgt te maken met meerdere authenticatie levels. Bijvoorbeeld MFA of inloggen op een beveiligde laag via een secundair account.	EIS
BEVE-18	Beveiliging	Wijzigen van toegangsrechten en verwijderen van accounts dient enkel te gebeuren in opdracht en na goedkeuring van de provincie Noord-Brabant	EIS
BEVE-19	Beveiliging	De inschrijver heeft een monitoringsbeleid en handelt hier (pro-)actief naar.	EIS
BEVE-20	Beveiliging	Monitoring op processen die bij de inschrijver zijn belegd en afspraken (SLA) die zijn overeengekomen.	EIS
BEVE-21	Beveiliging	De inschrijver biedt logging op gebied van security. De inschrijver heeft dit zodanig geregeld dat de volledig logging welke zuiver en alleen voor de provincie Noord-Brabant is.	EIS
BEVE-22	Beveiliging	Incidenten aangaande informatiebeveiliging worden geregistreerd en periodiek gerapporteerd aan de provincie Noord-Brabant. Afhankelijk van de grootte, aard en de impact van het incident wordt er een escalatie pad gevolgd waarin de provincie Noord-Brabant tijdig en zo volledig mogelijk wordt betrokken.	EIS
BEVE-23	Beveiliging	De inschrijver zorgt voor automatische rapportage van autorisatie en toegang	EIS
BEVE-24	Beveiliging	De provincie Noord-Brabant is ten allen tijden gerechtigd om een audit te laten uitvoeren door een externe auditor over de geleverde dienst. Bevindingen komende uit de audit worden door inschrijver opgelost op kosten van inschrijver.	EIS
BEVE-25	Beveiliging	Data relevant voor de verwerking van cases dienen conform relevante wet- en regelgeving en de BIVP classificatie versleuteld te worden in transport, verwerking, en in rust (inclusief kopieën en/of backups van deze data).	EIS
BEVE-26	Beveiliging	Data relevant voor de werking van de ITSM tool dient conform relevante wet- en regelgeving en de BIVP classificatie volledig, consistent, en betrouwbaar te blijven, zowel in transit, als in rust.	EIS
BEVE-27	Beveiliging	Data relevant voor de werking van de ITSM tool dient conform relevante wet- en regelgeving en de BIVP classificatie benaderbaar en/of afgeschermd te worden op een 'need-to-know' en 'need-to-have' basis.	EIS
BEVE-28	Beveiliging	Data relevant voor de werking van de ITSM tool dient conform relevante wet- en regelgeving en de BIVP classificatie bewaard en/of beschikbaar te zijn.	EIS
BEVE-29	Beveiliging	Data relevant voor de verwerking van cases dient conform relevante wet- en regelgeving en de BIVP classificatie bewaard en/of beschikbaar te zijn.	EIS
BEVE-30	Beveiliging	Data relevant voor de werking van de ITSM tool, inclusief kopieën en/of backupdata, dient conform relevante wet- en regelgeving en de BIVP classificatie verwijderd en/of afgevoerd te kunnen worden. Bijvoorbeeld AVG: recht op vergetelheid.	EIS
BEVE-31	Beveiliging	Data relevant voor de verwerking van cases, inclusief kopieën en/of backupdata, dient conform relevante wet- en regelgeving en de BIVP classificatie opgeslagen en verwerkt te worden. Bijvoorbeeld AVG: persoonsgegevens van EU burgers.	EIS
BEVE-32	Beveiliging	Toegang tot beheeromgevingen, webbased portalen, beheersoftware, en/of andere interfaces om functioneel beheer uit te voeren, dient afgeschermd te kunnen worden zodat alleen geautoriseerde bronnen toegang hebben tot de bovengenoemde functionaliteiten.	EIS
BEVE-33	Beveiliging	Authenticatie van gebruikers dient plaats te vinden via ENTRA-ID.	EIS
BEVE-34	Beveiliging	Autorisatie van gebruikers dient plaats te vinden via ENTRA-ID.	EIS
BEVE-35	Beveiliging	De oplossing biedt ondersteuning voor ENTRA SSO.	EIS
BEVE-36	Beveiliging	Cases met gevoelige inhoud voor organisatie of medewerker(s) dienen afgeschermd te kunnen worden zodat alleen individueel aangewezen personen toegang tot de informatie hebben.	EIS
BEVE-37	Beveiliging	Oplossing dient de standaard provincie Noord-Brabant namingconventie en herleidbaarheid van accounts te ondersteunen.	EIS
BEVE-38	Beveiliging	De oplossing dient een volledige audittrail te bieden. Alle activiteiten moeten bovendien naar een persoonlijk account herleidbaar zijn.	EIS
BEVE-39	Beveiliging	De oplossing dient een volledige audittrail te bieden. Alle activiteiten moeten bovendien naar een persoonlijk beheeraccount herleidbaar zijn.	EIS
BEVE-40	Beveiliging	Inschrijver past security best practises op het gebied van software ontwikkeling en secure coding.	EIS
BEVE-41	Beveiliging	Toegang tot beheeromgevingen, webbased portalen, beheersoftware, en/of andere interfaces om technisch beheer uit te voeren, dient afgeschermd te kunnen worden zodat alleen geautoriseerde bronnen toegang hebben tot de bovengenoemde functionaliteiten.	EIS
BEVE-42	Beveiliging	Inschrijver laat regelmatig code reviews, pentesting, compliance review, en andere relevante controles uitvoeren door interne en externe partijen. Inschrijver is bereid om uitkomsten van deze controles in te laten zien of uit te laten voeren door partijen aangewezen door de provincie Noord-Brabant.	EIS
RAPPORTAGE			
RAPP-1	Rapportage	SMT moet standaardrapportages bieden en de mogelijkheid om zelf rapportages te maken, zodat er gerapporteerd kan worden over SLA-prestaties, trends en andere relevante gegevens.	EIS
RAPP-2	Rapportage	Rapportages dienen geëxporteerd te kunnen worden in Excel- en PDF-formaat.	EIS
INSCHRIJVER			
INSC-1	SLA	De inschrijver verklaart vanaf oplevering van de SMT, op basis van de overeengekomen SLA, resultaatverantwoordelijkheid op zich te nemen voor de overeengekomen dienstverlening.	EIS
INSC-2	Support	De inschrijver biedt ten behoeve van IT meldingen en vragen een deskundige servicedesk aan, die als aanspreekpunt rechtstreeks in contact staat met Ons Loket van de provincie Noord-Brabant. Deze servicedesk moet het Nederlands in woord en geschrift goed beheersen.	EIS
INSC-3	Samenwerking	Het moment van het doorvoeren van een update van SMT in de productieomgeving gaat altijd in overleg met de provincie Noord-Brabant waarbij de releasenotes van te voren gedeeld zijn.	EIS
IMPLEMENTATIE - BEHEER			
IMPL-1	High Level Design	Het HLD beschrijft hoe en waar de aangeboden oplossing overeenkomt met de wensen, eisen en doelstellingen in dit PVE.	EIS
IMPL-2	High Level Design	Het HLD beschrijft in voldoende mate de visie, uitgangspunten, principes en hoofdontwerpkeuzes die aan de aangeboden oplossing ten grondslag liggen.	EIS
IMPL-3	High Level Design	Het HLD dient in te gaan op hoe de integratie (onderlinge samenhang) tussen de werkplek, netwerk- en security componenten tot stand komt. Maar denk ook aan koppelingen met andere platforms, applicaties al dan niet ondergebracht bij andere partijen.	EIS
IMPL-4	High Level Design	Het HLD biedt een compleet overzicht van alle componenten van het door de provincie Noord-Brabant gevraagde en door de inschrijver aangeboden oplossing. De mate van detaillering is hierbij van het juiste niveau. Dat wil zeggen dat het voor de provincie Noord-Brabant duidelijk en volledig is waarbij alle relevante componenten worden geraakt, benoemd en zijn uitgewerkt.	EIS
IMPL-5	Low Level Design	Het LLD dient te beschrijven hoe componenten zijn ingericht en ingesteld om invulling te geven aan het HLD.	EIS
IMPL-6	Change proces	Inschrijver dient te conformeren aan het change proces van de provincie Noord-Brabant.	EIS
IMPL-7	Service integratie	Inschrijver dient met haar dienst te integreren in de service organisatie van de provincie Noord-Brabant.	EIS
IMPL-8	Installatie	Azure resources wordt als IaC (Infrastructure as Code) uitgerold.	EIS
IMPL-9	SLA	Inschrijver levert zijn dienst overeenkomstig de Service Level Agreement (SLA) die is bijgevoegd.	EIS
IMPL-10	Samenwerking	Afspraken m.b.t. samenwerking zijn minimaal vastgelegd in het DAP. Wijzigingen in het DAP worden onderling afgestemd en akkoord bevonden.	EIS
IMPL-11	Interfaces/koppelingen	Inschrijver is verantwoordelijk voor het beheer en ontwikkeling van de interfaces/koppelingen benoemd in het beschrijvend document SMT.	EIS

IMPL-12	Onderhoudswindow	De provincie Noord-Brabant heeft invloed op het onderhoudswindow wanneer onderhoud leidt tot onbeschikbaarheid van de SMT.	EIS
IMPL-13	Beheer	De dienstverlening bestaat uit functioneel en applicatie beheer zoals beschreven in het beschrijvend document SMT	EIS