

Bijlage A – Programma van Eisen

Het Programma van Eisen (PvE) vormt een bijlage bij het Beschrijvend document voor de Europese Aanbesteding 'Publieksdiensten' van de KB, hierna te noemen Opdrachtgever.

Door ondertekening van het Uniform Aanbestedingsdocument (UEA) (Bijlage I) gaat Inschrijver akkoord met hetgeen hierin is gesteld, eventueel gewijzigd door middel van een Nota van Inlichtingen.

Inhoudsopgave

Hieronder treft u de eisen aan die Opdrachtgever stelt aan Inschrijver en Opdrachtnemer inzake het beheer van de publieksomgeving. Achtereenvolgens komen de volgende onderwerpen aan bod:

Bijlage A – Programma van Eisen.....	1
Inhoudsopgave	1
1. Oplossing.....	3
2. Implementatie	4
3. Publieke werkplekken, aanverwante randapparatuur & faciliteiten.....	6
4. Configureerbaarheid.....	16
5. Toegankelijkheid.....	16
6. Beschikbaarheid	17
7. Onderhoud en beheer	18
8. Servicemanagement.....	19

9.	Beveiliging	23
10.	Privacy	30
11.	Exit strategie	31
12.	Algemene eisen.....	32
13.	Juridische eisen.....	35
14.	Facturatie.....	36

1. Oplossing

1.	Oplossing	De Opdrachtgever wenst de Oplossing, die bestaat uit een combinatie van hard- en software af te nemen als dienst. Hosting van software, indien relevant, wordt verzorgd door de Opdrachtnemer. De aansluitingen tussen de Oplossing en omgeving van de Opdrachtgever worden beschreven in de aanbestedingsstukken.
2.	Oplossing – Bestaande programmatuur	Opdrachtnemer biedt, gedurende de contractperiode, altijd de meest actuele versie van de Oplossing aan, waarbij deze de werking van alle functionaliteiten garandeert. Inschrijven op basis van toekomstige releases is niet toegestaan.
3.	Oplossing – Dienstverlening	Opdrachtnemer is vanuit het oogpunt van Opdrachtgever verantwoordelijk voor de gehele Oplossing. Als er gebruik wordt gemaakt van dienstverlening van derden (bijvoorbeeld voor datacenterdienstverlening of trainingen/opleidingen) is Opdrachtnemer alsnog het aanspreekpunt en kan er niet worden doorverwezen naar derden.
4.	Oplossing – Limieten	In de Oplossing zijn geen beperkingen of limieten opgenomen die voor Opdrachtgever leiden tot additionele kosten om van de Oplossing gebruik te kunnen maken. Daarmee wil Opdrachtgever voorkomen dat Opdrachtnemer additionele kosten rekent vanaf een bepaald aantal records, documenten of andere limitaties. Uiteraard maken Opdrachtgever en Opdrachtnemer afspraken over excessief gebruik.
5.	Oplossing – Taal	De communicatie met de Opdrachtgever geschiedt in de Nederlandse taal. Eventueel is communicatie in het Engels mogelijk als dat expliciet is afgesproken met Opdrachtgever.

2. Implementatie

6.	Implementatie – Aanpak	Door Opdrachtnemer worden de projectmanagementrol en implementatieconsultantrol door minimaal twee verschillende personen uitgevoerd, omdat belangen in deze rollen kunnen conflicteren bij de projectuitvoering.
7.	Implementatie planning en uitvoering	Opdrachtgever verwacht een planning te ontvangen in 1 ^e helft februari 2025, deze wordt hierna besproken met Opdrachtnemer. In deze planning wordt aangegeven welke werkzaamheden/acties dienen te gebeuren (en door wie) en op welke wijze de implementatie dient te verlopen. Duidelijkheid is geboden of een gefaseerde overgang mogelijk is of op welke andere wijze. Het streven is om zoveel mogelijk werkzaamheden buiten de reguliere openingstijden van de leesalen te verrichten, zodat klanten in de leesalen zo min mogelijk hinder ondervinden.
8.	Implementatie – Documentatie	Opdrachtnemer voert het project op gecontroleerde wijze uit, dit betekent dat Opdrachtgever een aantal documenten verwacht gedurende het project. Opdrachtnemer is (mede)verantwoordelijk voor het opstellen en onderhouden van: - Het projectplan; - Het implementatieplan; - Het trainings- en opleidingsplan; - Overdrachtsdocumentatie; - Het communicatieplan; - Testplannen; - Het risicobeheerplan; - Acceptatiecriteria (Opdrachtgever in de lead); - Configuratie- en change management documentatie; - Gegevensmigratieplan; Opdrachtgever wil duidelijk maken dat documenteren geen doel op zich is en waar mogelijk kunnen zaken gecombineerd of hergebruikt worden.

2. Implementatie

9.	Implementatie – Migratie	Opdrachtnemer stelt samen met Opdrachtgever een gegevensmigratieplan op waarin de acties en stappen zijn beschreven die bij de migratie zijn voorzien, inclusief het plaatsen, aansluiten en testen van de vernieuwde hardware. Opdrachtgever is verantwoordelijk voor het aanleveren van stamgegevens en historische gegevens vanuit de huidige systemen. Opdrachtnemer ondersteunt hierbij en is verantwoordelijk voor de import naar de nieuwe Oplossing. Opdrachtnemer waarborgt dat dit op een gecontroleerde en veilige wijze en zonder verlies van gegevens wordt uitgevoerd en dat de gegevensbestanden worden vernietigd nadat deze zijn verwerkt in de Oplossing. Opdrachtnemer laat door middel van een rapport zien dat de migratie succesvol is uitgevoerd. Opdrachtgever verwacht een planning te ontvangen in 1^e helft februari 2025, deze wordt hierna besproken met Opdrachtnemer. Het streven is om zoveel mogelijk werkzaamheden (zoals ook het plaatsen, aansluiten en testen van de nieuwe hardware) buiten de reguliere openingstijden van de leeszaal te verrichten, zodat klanten in de leeszaal zo min mogelijk hinder ondervinden. Migratie van gegevens, zoals: • <i>het opgewaardeerde saldo van de klant/KB pas (staat niet op de pas zelf opgeslagen, maar staat bij de huidige leverancier in de Cloud).</i> • <i>Kassaverkopen van 2024 – heden</i> • <i>Toegangsgegevens (poortjes leeszaal) van de laatste maand, deze worden momenteel maar 1 maand bewaard (i.v.m. connectie klant)</i>
10.	Implementatie – In productie name	Opdrachtnemer stelt Opdrachtgever in staat om voordat de Oplossing in productie wordt genomen een acceptatietest uit te voeren. Ook het testen van de gegevensmigratie dient onderdeel te zijn van de acceptatietest.

3. Publieke werkplekken, aanverwante randapparatuur & faciliteiten

11.	Algemeen	Basis voor het aantal publieke werkplekken zijn 44 werkstations. De invulling van de functie van de publieke werkplek wordt nader bepaald (wel/geen kioskfunctie met statische website etc.) Zie ook: Werkstations.
12.	Algemeen	Alle werkstations en aanverwante randapparatuur zijn via een tijd- en datum schema in te stellen (aan/uit) en tonen bij gebruik het vooraf ingestelde startscherf/profiel met een KB-look & feel.
13.	Algemeen	Het gebruik van de huidige KB (lidmaatschap)pas met NXP MIFARE Classic® EV1 S50 1 KB pas (4NUID) is mogelijk voor alle diensten/dienstverlening waar dit vereist/ingesteld is.
14.	Algemeen	Voor het gebruik van veel diensten en/of faciliteiten is door de KB een inlog vereist gesteld aan eindgebruikers (KB pashouders), door middel van de KB gehanteerde authenticatie voorziening én autorisatie op basis van het KB Klantregistratiesysteem [KRS] wordt toegang verleend [mits aan de gestelde voorwaarden wordt voldaan].
		Werkstations:
15.	Werkstation	Een werkstation moet minimaal uitgerust zijn met: Processor: I5 Core, intern (werk)Geheugen: 16 GB, Opslag: 256 GB, OS: Windows 11, nieuwste generatie.
16.	Werkstation	Een werkstation bestaat uit een pc, een monitor, een toetsenbord (bedraad), een muis (bedraad), waarvan de linker- en rechtermuisknop gebruikt kan worden. Het gebruik van de usb aansluiting t.b.v. usb-stick/harddisk moet mogelijk zijn, dienen o.a. gebruikt te kunnen worden voor externe opslag.
17.	Werkstation	Een werkstation toont aan wie ingelogd is (bijvoorbeeld d.m.v. een 'profile pagina')

3. Publieke werkplekken, aanverwante randapparatuur & faciliteiten

18.	Werkstation	Een werkstation heeft een instelbare automatische uitlog, na (een instelbare) inactiviteit.
19.	Werkstation	Een werkstation bevat ingestelde (windows)applicaties/programma's/software, opstarten, waarbij de functionaliteit & gebruik werken. (office, browsers etc.)
20.	Werkstation	Een werkstation heeft 3 (actuele) browsers beschikbaar, welke te allen tijde in incognito venster/modus opstarten en bieden gebruik van het internet. Dit zijn: Edge, Chrome & Firefox
21.	Werkstation	Een klant heeft de mogelijkheid op het werkstation bestanden tijdelijk op te slaan, deze opslag is persoonlijk (na inlog) en wordt dus niet gedeeld met anderen. Het is ook mogelijk bestanden op een extern medium van de eindgebruiker op te slaan. Het tijdelijke bestand wordt automatisch gewist via een ingestelde tijd dezelfde dag.
22.	Werkstation	Een werkstation geeft geen mogelijkheid tot het starten en/of installeren van .exe bestanden of programma's/software anders dan ingesteld door Opdrachtgever.
23.	Werkstation	Aan een werkstation is randapparatuur compatible via gangbare poorten (USB/c, HDMI, Display)
24.	Werkstation	Aan 2 werkstations is een CD/CD-rom spelers aangesloten (alleen afspelen/lees faciliteiten)
25.	Werkstation	Een klant kan de sessie in 'pauze' zetten (afhankelijkheid welke dienst/faciliteit gebruikt wordt). Zodat de klant voor een korte tijd deze bezet kan houden zonder hiervoor hoeft uit te loggen. Deze pauze tijd is

3. Publieke werkplekken, aanverwante randapparatuur & faciliteiten

		instelbaar (d.m.v. invoer zoals bij 1 ^e keer inloggen, kan de klant het werkstation weer vrij geven en in gebruik nemen).
26.	Werkstation	Een werkstation heeft de mogelijkheid om meerdere beeldschermen te koppelen (aan 1 werkstation).
27.	Inloggen	Om een werkstation te kunnen gebruiken waar een inlog is bepaald/ingesteld, geschiedt dit door invoering van het geldende gebruikersnaam en wachtwoord, koppeling via de authenticatievoorziening van Opdrachtgever, dit is niet noodzakelijk voor werkstations waar geen inlog is bepaald/ingesteld.
28.	Inloggen	Een werkstation met office/internet, waarop inloggen noodzakelijk is, kan alleen gebruikt worden door KB jaarpashouders met een geldend lidmaatschap. Er verschijnt een duidelijke melding (geen toegang) indien de gestelde voorwaarden onjuist zijn.
29.	Inloggen	Het is mogelijk om werkstations in te stellen zonder een (beveiligde) inlog, maar met een speciaal thema/profiel als startpagina.
30.	Uitloggen	Een klant kan het werkstation zelf uitloggen of wordt automatisch uitgelogd na een instelbare inactiviteit. Hierna toont het werkstation de ingestelde startpagina/startscherm/profiel.
31.	Uitloggen	Een werkstation wordt te allen tijde bij het uitlog/herstart proces “schoon” opgeleverd, er zijn geen sporen van eerder gebruik aanwezig van bestanden, websites en/of vorige gebruiker/klantgegevens
32.	Printopdrachten	Op een werkstation wordt een printerdriver geïnstalleerd voor de MFC printer.

3. Publieke werkplekken, aanverwante randapparatuur & faciliteiten

33.	Software	Een workstation bevat i.i.g. de volgende software: Office (incl. taalinstellingen, knipprogramma, paint etc.), PDF reader, Videoplayer, Adobe digital editons, Kladblok, Wordpad. Een workstation gekoppeld aan een flatbed/bookscanner bevat de scansoftware van de leverancier van de scanner. Het beschikbaar stellen van software geschiedt ten alle tijde met goedkeuring Opdrachtgever.
34.	Software	Eén workstation voor klanten met een visuele beperking beschikt over de software Supernova.
35.	MFC	De Opdrachtnemer dient gebruik te maken van de aanwezige/bestaande MFC's. De aansturing hiervan dient te geschieden in overleg met Opdrachtgever, het contract van de huidige MFC's loopt tot 8-2-2028.
36.	MFC faciliteit (printen, kopiëren, scannen)	De klant kan zich met een KB pas aanmelden, ziet dat hij/zij ingelogd is en het apparaat wordt vrijgegeven voor gebruik, bij het verwijderen van de KB pas wordt het apparaat direct geblokkeerd voor gebruik. Na het beëindigen van de transactie wordt de sessie afgesloten en wordt opnieuw het startscherm getoond.
37.	MFC faciliteit (printen, kopiëren, scannen)	De Opdrachtnemer zorgt voor een printer integratie met het betaalsysteem zodat de opdracht van de klant in de queue wordt geplaatst van de MFC faciliteit. Hierbij wordt de privacy gewaarborgd van de klanten.
38.	MFC faciliteit (printen, kopiëren, scannen)	Er kan uitsluitend worden gekopieerd/geprint bij voldoende saldo (op de RFID chip) en/of bij een directw betaling/betaalmogelijkheid.
39.	MFC faciliteit (printen, kopiëren, scannen)	Een ingegeven printopdracht kan de klant na betaling printen volgens de ingegeven voorkeuren.

3. Publieke werkplekken, aanverwante randapparatuur & faciliteiten

40.	MFC (web-UI voor printen)	De Oplossing heeft een Web-UI (met KB look & feel), waarmee klanten die ingelogd zijn op het KB wifi een printopdracht kunnen versturen naar de MFC-printqueue. Minimaal worden de volgende bestandsformaten ondersteund: Word (doc/docx), Excel (xls/xlsx), Powerpoint (ppt/pptx), PDF, png, jpg/jpeg.
41.	MFC faciliteit (printen, kopiëren, scannen)	De klant kan voor het betalen van de kopieer- of printopdracht gebruik maken van de KB pas (RFID chip) of via een nader te bepalen betaalmogelijkheid. (bijvoorbeeld via pin/creditcard). De inschrijver kan beide mogelijkheden 'aanbieden', waarbij naderhand een keuze kan worden gemaakt door de Opdrachtgever.
42.	MFC faciliteit (printen, kopiëren, scannen)	Aangegeven staat hoe de klant zich bekend maakt, gegevens van de klant zijn na aanmelding zichtbaar.
43.	MFC faciliteit (printen, kopiëren, scannen)	De printvoorziening toont de tarieven voor kopiëren, scannen en/of printen (of dat er geen vergoeding nodig is)
44.	MFC faciliteit (printen, kopiëren, scannen)	De klant kan zelf een keuze maken welk bedrag er op de KB pas (RFID chip) opgewaardeerd moet worden (afhankelijk van welke betaalvoorziening beschikbaar is), klant wordt via een menu eenvoudig door het proces geleid.
45.	MFC faciliteit (printen, kopiëren, scannen)	De klant ontvangt een transactie bon van het saldo op de KB pas is opgewaardeerd. De klantgegevens & gegevens organisatie zijn in overleg met Opdrachtgever bepaald.
46.	MFC faciliteit (printen, kopiëren, scannen)	De klant kan voor het opwaarderen van het saldo op de KB pas met een betaalvoorziening via pin, contactloos, visa en mastercard betalen.

3. Publieke werkplekken, aanverwante randapparatuur & faciliteiten

		Het gebruik van een beheerapplicatie van de publieksomgeving:
47.	Beheer werkstations	Het gebruik van en de toegang tot de beheerapplicaties is alleen toegankelijk voor geautoriseerde KB medewerkers.
48.	Beheer werkstations	Alle werkstations en eventueel randapparatuur zijn ingevoerd en overzichtelijk qua taak, locatie & beschikbaarheid zichtbaar
49.	Beheer werkstations	Individueel en/of per groep is zichtbaar indien een werkplek in gebruik is en door welke klant
50.	Beheer werkstations	De werkstations kunnen te allen tijde per groep, deel van een groep of individueel worden aan- en uitgezet/herstart of uitgeschakeld
51.	Beheer werkstations	Indien een klant ingelogd is op een werkstation, zich toegang heeft verschaft tot de leesalen of gebruik maakt van de faciliteiten (zoals scannen) dan is voor de geautoriseerde medewerker zichtbaar welke klant dit is. Indien een klant uitlogt, dan zijn deze gegevens niet meer zichtbaar.
52.	Beheer werkstations	Alle printopdrachten van de klant zijn (voor een instelbare periode) toegankelijk voor de geautoriseerde (balie)medewerker en de printopdracht kan worden gereset worden (indien deze door omstandigheden niet goed is uitgevoerd door de MFC).
53.	Beheer werkstations	Alle ingestelde profielen, plattegronden etc. van de werkstations en randapparatuur kunnen hieruit beheerd, bewerkt worden.

3. Publieke werkplekken, aanverwante randapparatuur & faciliteiten

54.	Beheer werkstations	Er kunnen tekstuele berichten naar alle pc's (ad hoc en ingestelde), naar een groep en deel van een groep of naar een individueel workstation gestuurd worden. De ontvanger/ontvangers zien dit bericht in de vorm van een pop-up.
		Toegangspoortjes:
55.	Toegangspoortjes	De oplossing verleent toegang tot de leeszaal van Opdrachtgever via de bestaande toegangspoortjes, klanten bieden hiervoor de KB pas aan via een paslezer voor toegang of verlaten van de leeszaal. Voor toegang tot de leeszaal wordt een autorisatie op basis van pasnummer een controle gedaan met de KB-autorisatie API.
56.	Toegangspoortjes	Op basis van het beheer van alle registraties (verleende toegangen m.b.v. de KB pas) zijn per toegangspoortje overzichten met statistische tellingen samen te stellen. (voorkeur via Excel-export). De bewaartermijn is instelbaar (bijvoorbeeld: nu 1 maand). Voor de statistische tellingen zijn minimaal nodig: datum/pasnummer/tijd.
		Kassaregister:
57.	Kassa	De inschrijver dient er van uit te gaan dat een nieuw kassasysteem dient te worden geleverd. Na gunning wordt dit verder bepaald.
58.	Kassa	De Opdrachtnemer kan het kassasysteem van Opdrachtgever beheren, het ontvangen van betalingen verloopt via de payment provider Equens (huidige situatie).
59.	Kassa	De kassa registreert alle aankopen, afrekenen gaat direct via pin/contactloos/creditcard (Visa & Mastercard), de betaling geschiedt momenteel via Equens.

3. Publieke werkplekken, aanverwante randapparatuur & faciliteiten

60.	Kassa	Retourpin(nen) is mogelijk
61.	Kassa	Een (optionele) transactie bon bevat (instelbare) klant/organisatie gegevens
62.	Kassa	Alle artikelen van de KB winkel & overige producten kunnen ingevoerd worden.
63.	Kassa	De voorraad van de producten is in te voeren.
64.	Kassa	Artikel groepen kunnen aangemaakt worden.
65.	Kassa	Korting op product/artikel kan aangegeven worden.
66.	Kassa	Dag/maandverkopen (rapportages) zijn te genereren (voorkeur excel), een bewaartermijn van de kassaregistraties is vastgelegd.
67.	Kassa	Scannen van producten (barcode op product) is mogelijk.

3. Publieke werkplekken, aanverwante randapparatuur & faciliteiten

68.	Kassa	Er zijn koppeling(en) - middels API's, met een financieel systeem, zoals bijvoorbeeld Exact of soortgelijke financiële applicatie, mogelijk. Er wordt momenteel binnen de KB een nieuw financieel pakket aangeschaft, welke operationeel zal zijn vanaf januari 2026. Hier zullen minimaal de navolgende gegevens als: de verkoopadministratie, verkoop kassa systeem, voorraadbeheer (webwinkel en fysieke winkel) onderdeel zijn. Van Opdrachtnemer wordt verwacht dat deze koppelingen, in samenwerking met Opdrachtgever worden gerealiseerd.
		Integratie:
69.	Integratie	Voor de onderdelen van de oplossing waar de klant zichzelf identificeert met de KB-pas, wordt, gebruikt de oplossing de autorisatie-API van Opdrachtgever om te bepalen of de dienst verleend mag worden.
70.	Integratie	Eindgebruikers loggen op webdiensten en de werkstations met hun bibliotheek-account in op de landelijke inlogvoorziening (AV). Het inlogprotocol is OpenID Connect.
71.	Integratie/Maatwerk	Voor het gebruik van het KB wifi wordt door de Opdrachtnemer een captive portal ontworpen (met KB look & feel), toegang hiertoe (KB wifi) geschiedt via de IAM authenticatie (AV) en autorisatie op basis van KB KRS.
72.	Integratie/Maatwerk	De Opdrachtnemer heeft kennis om verschillende profielen (web UI) voor werkstations te maken en toe te passen (met KB look & feel) op diensten van Opdrachtgever, specifieke websites, in de leeszaal opgestelde collecties en/of databanken.
73.	Integratie/Maatwerk	De oplossing heeft een Web-UI voor eenvoudige toegang tot diensten voor de wifi-gebruikers (zoals bijvoorbeeld printen).

3. Publieke werkplekken, aanverwante randapparatuur & faciliteiten

74.	Integratie	De bestaande MFC Ricoh IM C3000 blijft gehandhaafd, dus een koppeling dient verzorgt te worden met kopieer/printbeheer & het betaalverkeer. Momenteel verloopt dit via de payment provider Equens.
75.	Integratie	Betaalzuil/automaat (of andere optie) gekoppeld aan IAM authenticatie, speciaal voor tegoed plaatsen gekoppeld aan de KB pas of directe betaling via pinpas/creditcard.
76.	hardware	Paslezer van de Opdrachtnemer moeten overweg kunnen met de KB pas / RFID: PVC 0,76 mm wit NXP MIFARE Classic® EV1 S50 1 KB pas (4NUID) – huidige leverancier: DCP
		Hieronder ter algemene informatie de huidige gebruikte (inmiddels verouderde) hardware:
77.	hardware	Werkstation: Merk HP Type Prodesk 400 G5 Desktop mini Serial no: 8CC9370FZF Extra pc computer beugel / externe Disk drive (CD-rom)
78.	hardware	Monitor: Merk HP Type P244 23.8 Inch Serial CB 492803P7
79.	hardware	Pas lezer: Merk ACS Type ACR112 Serial S/N RR 171-281049
80.	hardware	Kassa: Merk 4POS Type Vesa 100 Koppeling met Pin terminal CCV, VX820ITS en Pas lezer
81.	hardware	Flatbedscanner: Book pavilion (Plustek opticbook a300)

4. Configureerbaarheid

82.	Configureerbaarheid – Functioneel Beheer	De Oplossing beschikt over schermen voor Functioneel Beheer (FB) voor de uitvoer van alle beheertaken, bijvoorbeeld gegevensbeheer, autorisatiebeheer, configuratie van workflows, dashboards, monitoring, inzien logging, foutdetectie, tests.
83.	Configureerbaarheid – Functioneel Beheer	De Oplossing zorgt dat Functioneel Beheer (FB) op een begrijpelijke en eenduidige wijze inzicht krijgt in relevante foutmeldingen zodat gericht actie kan worden ondernomen door FB.
84.	Configureerbaarheid – Archivering	De Oplossing biedt de mogelijkheid om bewaartermijnen te definiëren en deze aan gegevens te koppelen.

5. Toegankelijkheid

85.	Toegankelijkheid	De oplossing voldoet steeds aantoonbaar aan de eisen voor digitale toegankelijkheid zoals omschreven in de meest actuele versie van de Europese standaard EN 301 549, waarvan de internationale richtlijnen voor toegankelijkheid, de Web Content Accessibility Guidelines, deel uitmaken. Opdrachtgever vraagt hierbij WCAG niveau AA.
86.	Toegankelijkheid – Schaalbaar en responsive	De gebruikersinterface van de Oplossing is schaalbaar en responsive zodat die zich automatisch aanpast aan verschillende scherm-/vensterformaten. De gegevens moeten op een herkenbare en leesbare wijze getoond worden aan de Gebruiker.
87.	Toegankelijkheid – Foutmelding	De Oplossing geeft foutmeldingen op een éénduidige manier weer (op het scherm) aan de Gebruiker met een omschrijving wat de reden van de foutmelding is en met daarbij eventueel advies welke acties nodig zijn voor een correcte uitvoering.

5. Toegankelijkheid

88.	Toegankelijkheid – Foutmelding	De foutmeldingen die de Oplossing weergeeft aan de Gebruiker bevatten geen technische of inhoudelijk gevoelige informatie zodat misbruik op basis van deze informatie wordt voorkomen. Foutmeldingen worden, met relevante technische informatie, gelogd zodat nader onderzoek/analyse mogelijk is.
89.	Toegankelijkheid – Toetsenbord en muis	De gebruikersinterface van de Oplossing dient zowel met de muis als met toetsenbordcombinaties te bedienen te zijn.
90.	Toegankelijkheid – Helpfunctie	De gebruikersinterface van de Oplossing beschikt over een algemene helpfunctie die voor de Gebruiker vanuit ieder scherm benaderd kan worden. Vanuit specifieke schermen/velden kan gerichte instructie worden opgevraagd met informatie over het betreffende veld en/of scherm waar de Gebruiker zich bevindt.

6. Beschikbaarheid

91.	Beschikbaarheid – Omgeving	Het minimale beschikbaarheidspercentage exclusief tijd voor onderhoud is 99,5% per maand. In de Supportdocumentatie wordt uitgewerkt hoe wordt omgegaan met geplande en ongeplande (bijvoorbeeld bij een security incident) onderhoudsvensters. De beschikbaarheid van de werkstations en aanverwante apparatuur is gekoppeld aan een uur vóór openingstijden leeszaal KB en een kwartier na sluitingstijd, de beschikbaarheidsuren zijn ten allen tijde aanpasbaar. In ieder geval meldt Opdrachtnemer geplande downtime, bijvoorbeeld als gevolg van onderhoudswerkzaamheden of het installeren van een nieuwe release, minimaal 48 uur van tevoren bij Opdrachtgever. Wanneer werkzaamheden binnen werkuren van Opdrachtgever plaatsvinden die downtime met zich meebrengen, vraagt Opdrachtnemer eerst instemming van Opdrachtgever voordat de werkzaamheden worden uitgevoerd.
92.	Beschikbaarheid – Monitoring	Opdrachtnemer zorgt voor monitoring van de beschikbaarheid en performance van de Oplossing en dat Opdrachtgever direct gealarmeerd wordt bij onder andere (niet uitputtend): uitval, performanceproblemen, (D)DOS-aanvallen, onverklaarbare toename in verkeer naar internet, verlopen van beveiligingscertificaten,

6. Beschikbaarheid

		ongeautoriseerde wijzigingen aan configuratiebestanden, ongeautoriseerde wijzigingen aan systeembestanden etc. De Oplossing omvat een Intrusion Detection of Intrusion Prevention Systeem.
93.	Beschikbaarheid – Scheiding	Opdrachtnemer zorgt ervoor dat de gegevens van Opdrachtgever tijdens transport, bewerking en opslag duurzaam geïsoleerd zijn van beheerfuncties en anderen die gebruikmaken van dezelfde infrastructuur. Opdrachtnemer voorkomt dat Opdrachtgever performance-hinder ondervindt bij eventueel inzet van gedeelde componenten.
94.	Beschikbaarheid – Back-up en herstel	Opdrachtnemer garandeert adequate back-up- en restorevoorzieningen van de Oplossing, waarbij in het geval een restore van gegevens nodig is, de afgesproken dienstverlening binnen 8 uur (Recovery Time Objective) kan worden gecontinueerd. Er mag sprake zijn van maximaal 24 uur dataverlies (Recovery Point Objective). Back-ups worden gemaakt terwijl de volledige Oplossing 'online' is.
95.	Beschikbaarheid – Back-up en herstel	Opdrachtnemer voorziet in een back-up voorziening van de Oplossing waarbij de back-up zich op een locatie bevindt die niet geraakt wordt door een incident op een andere locatie. In geval van corrupte gegevens voorziet Opdrachtnemer in het uitvoeren van een herstel/rollback naar een eerdere (consistente) staat van de Oplossing. Opdrachtnemer dient periodiek, minimaal eens per jaar, aan te tonen dat de back-up en restore voorziening correct functioneert en voldoet aan de maximale hersteltijden en het maximaal toegestaan gegevensverlies. De resultaten hiervan worden vastgelegd door Opdrachtnemer in een rapport en hij stelt deze aan Opdrachtgever beschikbaar.

7. Onderhoud en beheer

96.	Onderhoud en beheer – Doorontwikkeling	Opdrachtnemer voert doorontwikkeling uit zonder additionele kosten. Onder deze doorontwikkeling wordt, naast correctief en preventief, ook verstaan: - Het onderhoud dat erop gericht is te zorgen dat de Oplossing blijft voldoen aan geldende wet- en regelgeving; - Het volgen van marktontwikkelingen in nieuwe digitale technologieën en mogelijkheden;
-----	--	---

7. Onderhoud en beheer

		- Het verbeteren van de Oplossing op het gebied van bijvoorbeeld functionaliteit of veiligheid bij het ontstaan van nieuwe (veiligheid) risico's.
97.	Onderhoud en beheer – Updates	Opdrachtnemer verstrekt zonder meerkosten updates en upgrades van de Oplossing. Dit is onderdeel van de licentieprijs en/of beheerkosten. Opdrachtgever wil voorkomen dat voor vernieuwde functionaliteiten additionele kosten worden gevraagd. Ook wil Opdrachtgever voorkomen dat oplossingen voor incidenten en wijzigingen niet doorgevoerd kunnen worden omdat er een betaalde update of upgrade niet is afgenomen.
98.	Onderhoud en beheer – Documentatie koppelingen	Opdrachtnemer dient een technische beschrijving van alle gerealiseerde koppelingen, integraties en de daarbij toegepaste configuraties aan te leveren voor afronding van de implementatie en deze vervolgens te onderhouden. De beschrijving omvat minimaal een specificatie van de uitgewisselde gegevens en de wijze waarop dit gebeurt.
99.	Onderhoud en beheer – Logging	Opdrachtnemer voorziet in de mogelijkheid dat Functioneel Beheer van Opdrachtgever binnen de Oplossing inzicht kan krijgen in de logging en dat er de mogelijkheid is om met behulp van filtering een lograpportage te genereren (bijvoorbeeld voor een externe audit partij).

8. Servicemanagement

100.	Servicemanagement – Taal	Opdrachtnemer voorziet in Nederlandstalige gebruiksdokumentatie en de servicedesk communiceert in de Nederlandse taal. Tijdens de implementatie wordt door Opdrachtnemer een DAP opgesteld.
101.	Acceptatie-omgeving	Een acceptatie-omgeving is niet nodig, aangezien wijzigingen eenvoudig buiten de openingstijden van de leeszaal getest kunnen worden op de productie-omgeving.
102.	Servicemanagement – technisch beheer	Opdrachtnemer is verantwoordelijk voor het technisch beheer en applicatiebeheer van de Oplossing.

8. Servicemanagement

103.	Servicemanagement – invulling Supportdocumentatie	De afspraken met betrekking tot het technisch beheer en applicatiebeheer worden nader uitgewerkt in Supportdocumentatie (SLA of soortgelijk document waarin procedures en dienstverleningsniveau 's zijn vastgelegd). Opdrachtnemer is, ten aanzien van de Oplossing, minimaal verantwoordelijk voor: - Installatie van aanbevolen updates en upgrades van de Oplossing. Ook de onderliggende componenten zoals het operating systeem, eventueel gebruikte middleware en het basic input/output system; - Informatiebeveiliging; - Bewaken en controleren van de infrastructuur; - Configuratiemanagement op het Cloud platform; - Beheer van opslagcapaciteit.
104.	Servicemanagement – invulling Supportdocumentatie	Voordat de Oplossing in beheer (fase in het project) wordt genomen, wordt in (concept) Supportdocumentatie (SLA of soortgelijk document waarin procedures en dienstverleningsniveau 's zijn vastgelegd) minimaal de volgende punten concreet en in detail uitgewerkt, waarbij relevante eisen in dit PvE van toepassing blijven: - Incidentmanagementprocedure, waarin in ieder geval, maar niet uitsluitend, aandacht is voor het rapporteren over (beveiligings)incidenten, problemen, datalekken en wijzigingen; - Incidentmatrix (prioriteiten, norm oplostijden, norm reactietijden (dienstverleningsniveau), terugkoppelingswijze); - Kanalen waarlangs vragen, verzoeken, incidenten, changes, klachten, enhancements etc. gemeld kunnen worden;
105.	Servicemanagement – Servicedesk	Opdrachtnemer verzorgt een servicedesk waar Opdrachtgever terecht kan voor technische en functionele ondersteuning. De servicedesk is het centrale punt voor het melden van incidenten, het stellen van vragen, indienen van wijzigingsvoorstellen en geeft informatie/inzicht in de afhandeling daarvan. De servicedesk is in ieder geval telefonisch en via e-mail bereikbaar. Voor contact met de servicedesk zal er 1 centraal telefoonnummer en 1 vast e-mailadres beschikbaar worden gesteld.

8. Servicemanagement

		Onderdeel van de servicedesk is een online webportaal waarin meldingen, vragen, incidenten en wijzigingsverzoeken gemeld en (op)gevolgd kunnen worden door Opdrachtgever.
106.	Servicemanagement – Servicedesk	De servicedesk is op Werkdagen (maandag t/m vrijdag) van minimaal 09.00 uur tot 17.00 uur, Nederlandse tijd beschikbaar. Een uitzondering hierop vormen in Nederland algemeen erkende feestdagen in de zin van de Algemene Termijnenwet. Buiten het servicewindow is het, met uitzondering van telefonisch contact, uiteraard wel gewoon mogelijk om via de diverse kanalen meldingen aan te maken.
107.	Servicemanagement – Servicedesk	Opdrachtgever kan onbeperkt incidenten en wijzigingsverzoeken indienen. Excessen of vermeend misbruik wordt besproken, maar er worden geen kosten in rekening gebracht. Opdrachtgever wil hiermee voorkomen dat er additionele kosten worden gerekend voor incidenten en standaard wijzigingen.
108.	Servicemanagement – Afhandelen incidenten	Opdrachtnemer biedt de volgende servicelevels of vergelijkbaar dan wel beter op incidenten: - Prioriteit kritiek: Opdrachtgever kan niet meer werken met de Oplossing. Reactietijd en oplossen binnen 4 uur. - Prioriteit hoog: Opdrachtgever kan met een kritisch proces niet meer werken. Reactietijd en oplossen binnen 8 uur. - Prioriteit midden: Opdrachtgever kan werken met een tijdelijke workaround. Reactietijd en oplossen binnen 16 uur. - Prioriteit laag: Opdrachtgever kan gewoon doorwerken, de verstoring treft minder dan 10% van de gebruikers en het getroffen proces is niet kritisch. Reactietijd binnen 4 uur, oplostijd in overleg.

8. Servicemanagement

		Opdrachtnemer zorgt dat bij 90% van de incidenten die kritiek, hoog of midden zijn, de reactietijd verstoring niet worden overschreden. Tevens levert Opdrachtnemer, bij kritische en hoge incidenten, binnen 5 Werkdagen een Root Cause Analysis (RCA) op. RCA moet minimaal de volgende onderdelen bevatten: omschrijving/oorzaak verstoring; tijden & duur van de verstoring; genomen acties ten aanzien van de oplossing; genomen maatregelen ter voorkoming van herhaling.
109.	Servicemanagement – Standaard wijzingen	Standaard wijzingen kennen een maximale oplostijd van 2 Werkdagen vanaf moment van aanmelden. Niet-standaard wijzingen worden binnen 5 Werkdagen opgevolgd met een inschatting van de doorlooptijd en kosten.
110.	Servicemanagement – Security en privacy incident	Opdrachtnemer dient onverwijld maar binnen 24 uur Opdrachtgever te informeren wanneer er sprake is van een gegevens-/datalek of security incident.
111.	Servicemanagement – Training en opleiding	Opdrachtnemer kan trainingen en opleidingen verzorgen aan Gebruikers van Opdrachtgever (Eindgebruikers, Key Users en Functioneel Beheerders) ten behoeve van het werken met de Oplossing, dit gedurende de looptijd van het contract. Opdrachtnemer verzorgt een training(en) voor Functioneel Beheerders en (test)Gebruikers bij de start van de implementatie van de Oplossing. Aan de overige Gebruikers wordt voordat de Oplossing in productie wordt genomen een training verzorgd. De kosten voor de initiële trainingen die plaatsvinden voordat de Oplossing in productie wordt genomen zijn in de prijsstelling voor de implementatie opgenomen. De kosten voor aanvullende trainingen of opleidingen daarna dienen separaat in rekening te worden gebracht.
112.	Servicemanagement – Rapportage	Minimaal ieder kwartaal levert Opdrachtnemer een Financiële en Service Level Rapportage op aan Opdrachtgever, welke naast een overzicht van de kosten, minimaal de maandelijkse uptime en een overzicht van (security)incidenten, wijzigingen en problemen bevat met hun response en oplostijden. Deze rapportage dient als input voor de jaarlijkse evaluatie.

8. Servicemanagement

113.	Servicemanagement – Evaluatie	Eens per jaar wordt een evaluatie ingepland tussen Opdrachtgever en Opdrachtnemer. Deze evaluatie leidt tot een beeld van de dienstverlening die is geleverd en leidt tot inzicht in gezamenlijk gedragen verbeteringen die kunnen worden doorgevoerd. Deze evaluatie zal in verslag door Opdrachtnemer worden weergegeven en binnen 20 Werkdagen worden opgeleverd aan Opdrachtgever. Opdrachtnemer neemt het initiatief om deze jaarlijkse evaluatie in te plannen. Innovatie op de lange termijn (+1 jaar), de roadmap voor het nieuwe jaar en eventuele verlenging van de dienstverlening zijn hierbij vaste onderwerpen.
------	-------------------------------	---

9. Beveiliging

114.	Beveiliging – Authenticatie	Opdrachtnemer houdt bij welke personen namens Opdrachtnemer toegang hebben tot de Oplossing en kan op verzoek van Opdrachtgever een overzicht hiervan verschaffen aan Opdrachtgever.
115.	Beveiliging – Authenticatie integratie	Opdrachtnemer zorgt ervoor dat medewerkers van Opdrachtgever zich kunnen authenticeren bij de Oplossing met behulp van Single Sign On (SSO) die loopt via de authenticatie management oplossing (Microsoft Entra ID) van Opdrachtgever. Toegang tot de Oplossing is enkel mogelijk na succesvolle login en Multi Factor Authenticatie (MFA).
116.	Beveiliging – Authenticatie	De Oplossing biedt mogelijkheden tot het automatisch uitloggen van Gebruikers wanneer de Gebruiker een bepaalde periode inactief is. Deze periode is configurabel.
117.	Beveiliging – Authenticatie	Opdrachtnemer zorgt ervoor dat de wachtwoorden die worden toegepast, die niet worden beheerd binnen de Microsoft Entra ID van Opdrachtgever, minimaal voldoet aan de wachtwoord criteria die Opdrachtgever hanteert. Deze criteria zijn configurabel.
118.	Beveiliging – Autorisatiebeheer	De Oplossing biedt Opdrachtgever de mogelijkheid om, als onderdeel van het Functioneel Beheer, zelf het autorisatiebeheer uit te voeren. Onder autorisatiebeheer wordt in ieder geval verstaan het verschaffen, aanpassen en blokkeren van toegang van Gebruikers tot specifieke onderdelen, modules

9. Beveiliging

		en/of specifieke informatie binnen de Oplossing. Functioneel Beheer van Opdrachtgever heeft de mogelijkheid om een overzicht te verkrijgen van ingestelde Gebruikers en bijbehorende autorisaties.
119.	Beveiliging – Autorisatie rollen	De Oplossing biedt de mogelijkheid om met behulp van zelf te definiëren autorisatie rollen (overeenkomstig het RBAC model) Gebruikers toegang te geven tot specifieke functionaliteiten, waaronder ook de workflow functionaliteit. Een optie/functionaliiteit waar de Gebruiker niet voor geautoriseerd is, is niet beschikbaar voor de Gebruiker.
120.	Beveiliging – Autorisatie rollen	De Oplossing biedt de mogelijkheid om functiescheiding toe te passen op basis van autorisatie rollen en bedrijfsregels.
121.	Beveiliging – Mail	Waar in de Oplossing gebruik wordt gemaakt van e-mail die namens Opdrachtgever wordt verstuurd of ingelezen, dan wordt daarvoor bij voorkeur aangesloten op de Microsoft Graph API en vindt autorisatie plaats op basis van OpenID Connect (OAuth 2.0) om toegang te verkrijgen tot het e-mailplatform Exchange Online van Opdrachtgever voor het verzenden of uitlezen van e-mail. In het geval dat een e-mailvoorziening wordt toegepast die niet verloopt via het e-mailplatform van de Opdrachtgever, dan zorgt Opdrachtnemer ervoor dat de e-mail herkenbaar is, op basis van domeinnaam van Opdrachtgever, als e-mail van de Opdrachtgever.
122.	Beveiliging – Mail	Waar de Oplossing gebruik maakt van e-mailverkeer dat namens Opdrachtgever plaatsvindt (intern dan wel extern) voldoet de implementatie blijvend aan aanvullende beveiligingsmaatregelen als SPF, DKIM, DMARC en DANE (eventueel na implementatie door Microsoft).
123.	Beveiliging – Encryptie	Data-in-flow wordt beveiligd middels transportversleuteling conform NCSC richtlijnen v2.1 (o.a. TLS 1.2/1.3 met sterke cipher suites)
124.	Beveiliging – Encryptie	Binnen de Oplossing worden gegevens versleuteld opgeslagen (data-at-rest) op basis van adequate encryptiestandaarden (minimaal AES-256). Dit is ook van toepassing op back-ups.

9. Beveiliging

125.	Beveiliging – File upload	De Oplossing stelt beperkingen aan de bestanden die geüpload worden, deze zijn gelimiteerd tot een vaste locatie en worden gefilterd op verwachte extensies (zoals Word, Excel, PDF, JPG, PNG, CSV, ZIP) en maximaal te verwachten bestandsgrootte. Op de geüploade bestanden vindt malware scanning plaats en worden bestanden indien nodig in quarantaine geplaatst.
126.	Beveiliging – Invoervalidatie	De Oplossing voorziet in checks die zien op volledigheid, verplichting en validatie op toegestane waarde(n) en helpen bij het voorkomen van fouten in de invoer door een Gebruiker. De Oplossing controleert de inhoud van een (HTTP-) request door deze te valideren alvorens die te gebruiken. Invoervalidatie moet de meest recente relevante dreigingen van OWASP met betrekking tot invoer afvangen, zoals SQL-injections en cross site request forgery.
127.	Beveiliging – Procedure	Opdrachtnemer hanteert een escalatieprocedure bij inbreuken op de informatiebeveiliging en faciliteert de verwerkingsverantwoordelijke daarmee in haar verplichting datalekken te melden.
128.	Beveiliging – Maatregelen	Opdrachtnemer heeft aantoonbaar passende en evenredige technische en organisatorische beveiligingsmaatregelen getroffen om beschikbaarheid, integriteit en vertrouwelijkheid van de Oplossing te kunnen garanderen.
129.	Beveiliging – Right to audit	Opdrachtgever heeft het recht om bij Opdrachtnemer een (onafhankelijke) audit uit te (laten) voeren naar de opzet, het bestaan en de werking van informatiebeveiligingsmaatregelen. Opdrachtnemer gaat akkoord met een audit door een medewerker van Opdrachtgever of een door Opdrachtgever ingehuurd accountants- of onderzoeksbureau. Opdrachtnemer gaat hierbij ook akkoord met het feit dat dit periodiek uitgevoerd wordt. Opdrachtnemer heeft de mogelijkheid om een audit rapport van een onafhankelijke 3rd-party auditor te overleggen.
130.	Beveiliging – BIO	Opdrachtnemer heeft maatregelen, processen en procedures ingericht ten aanzien van de Oplossing die Opdrachtgever in staat stelt te voldoen aan de Baseline Informatiebeveiliging Overheid (BIO). Opdrachtnemer kan door middel van certificering en rapportage aantonen in control te zijn.

9. Beveiliging

131.	Beveiliging – Pentest	De Oplossing die naar productie wordt gebracht, dient ten tijde van vrijgeven en bij alle majeure wijzigingen vrij te zijn van bekende kwetsbaarheden, waaronder minimaal de kwetsbaarheden genoemd in de actuele 'OWASP top 10' en de 'SANS/CWE top 25 most dangerous software errors'. Opdrachtnemer toont dit aan door een preventieve vulnerability scan en/of een penetratietest.
132.	Beveiliging – Pentest	Opdrachtnemer zorgt dat de digitale infrastructuur (hardware en software) van de Oplossing continu gemonitord wordt op kwetsbaarheden. Patches worden aangebracht conform de volgende criteria: - Binnen één week voor critical security patches (CVSS 9+), - Binnen twee weken voor high security patches (CVSS 7.0-8.9) en - Bij het eerstvolgende onderhoudswindow in andere gevallen (CVSS kleiner dan 7.0). Indien de toepassing extern-facing is of het de werkplek betreft gelden de volgende tijdwindows: - Direct en i.i.g. binnen 24 uur voor critical security patches (CVSS 9+), - Binnen één week voor high security patches (CVSS 7.0-8.9) en - Bij het eerstvolgende onderhoudswindow in andere gevallen (CVSS kleiner dan 7.0). Opdrachtnemer zal tenminste jaarlijks in de Oplossing gebruikte webapplicaties en API's door een onafhankelijke penetratietest laten controleren op kwetsbaarheden. Opdrachtnemer rapporteert ieder kwartaal over aangetroffen kwetsbaarheden en ondernomen acties en tenminste jaarlijks over de penetratietest en ondernomen actie dienaangaande. Opdrachtnemer stelt op verzoek van Opdrachtgever de originele rapportage van de vulnerability scan en penetratietest beschikbaar.
133.	Beveiliging – Preventie	Opdrachtnemer implementeert beheersmaatregelen tegen cyberaanvallen voor detectie, preventie en herstel in combinatie met een passend risicobewustzijn bij de eigen medewerkers.

9. Beveiliging		
134.	Beveiliging – Assurance	Opdrachtnemer beschikt over, dan wel levert na 1 jaar, een onafhankelijke Service Organization Control (SOC) 2 Type 2 dan wel SOC 3 rapportage of een ISAE 3402 type II verklaring om aan te tonen in control te zijn. Opdrachtnemer zorgt ervoor dat de Assurance-verklaring onderhouden wordt.
135.	Beveiliging – Certificering	Inschrijver heeft een geldig ISO 27001 certificaat voor de geboden dienst / oplossing en onderhoudt deze tijdens de contractduur [A1].
136.	Beveiliging – Hardening	Componenten waaruit de Oplossing bestaat (zoals maar niet beperkt tot (Cloud)platforms, hypervisors, containerplatforms, (besturings)systemen, database platforms) dienen door Opdrachtnemer afdoende te zijn gehardened aan de hand van CIS benchmarks of vergelijkbare voorschriften van de fabrikant (comply or explain).
137.	Beveiliging – Updates	Opdrachtnemer hanteert een degelijk patchschema om alle componenten waaruit de Oplossing bestaat (zoals firmware, operating systems, applicaties) actueel te houden, om verbeteringen door te voeren en bekende fouten op te lossen. De componenten die onderdeel zijn van de Oplossing worden door de desbetreffende leverancier/fabrikant ondersteund, minimaal op het gebied van security updates.
138.	Beveiliging – Cookies en HTTP Secure Headers	Waar de Oplossing gebruik maakt van Cookies of HTTP verkeer worden adequate beveiligingsinstellingen toegepast. Cookies dienen te zijn voorzien van de 'secure' en 'httponly' flags. Tevens bevatten cookies geen persoonlijke informatie en vindt de uitwisseling altijd via adequate transportbeveiliging conform E22.14 plaats. De Oplossing is vrij van tracking cookies. HTTP Secure Headers worden overeenkomstig met Best Practices (bijvoorbeeld op basis van OWASP Secure Headers Project) toegepast.
139.	Beveiliging	Bij wireless netwerkvoorzieningen voor gebruikers wordt verzekerd dat geen rechtstreekse verbindingen tussen gebruikers mogelijk zijn.

9. Beveiliging		
140.	Beveiliging	Voor het beveiligen van een systeem zijn overbodige functies en ongeoorloofde toegang uitgeschakeld. Deze hardening vindt plaats middels CIS Benchmarks.
141.	Beveiliging	Klokken van alle relevante informatieverwerkende systemen binnen de oplossing zijn gesynchroniseerd met één referentietijdbron. De maximale afwijking van de lokale standaardtijd (UTC) bedraagt 500 ms.
142.	Beveiliging	Gebeurtenissen en activiteiten worden gelogd. Een logregel bevat minimaal: (a) de gebeurtenis; (b) de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; (c) het gebruikte apparaat; (d) het resultaat van de handeling; (e) een datum en tijdstip van de gebeurtenis.
143.	Beveiliging	Logbestanden zijn beschermd tegen manipulatie.
144.	Beveiliging	Ter bescherming tegen malware zijn beheersmaatregelen voor preventie, detectie en herstel geïmplementeerd.
145.	Beveiliging	De gebruikte antimalwaresoftware en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.
146.	Beveiliging	Computers en media worden als voorzorgsmaatregel routinematig gescand. De uitgevoerde scan behoort te omvatten:

9. Beveiliging

		(a) Alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware scannen. (b) Bijlagen en downloads vóór gebruik.
147.	Beveiliging	Informatie over technische kwetsbaarheden wordt tijdig verkregen, geëvalueerd en opgevolgd met passende maatregelen.
148.	Beveiliging	Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC classificatie kwetsbaarheidswaarschuwingen), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.
149.	Beveiliging	1: Opdrachtnemer zorgt voor volledige logcorrelatie tussen het besturingssysteem en haar eigen oplossing waarbij volledige toerekenbaarheid van gebruikersacties wordt gerealiseerd. 2: Opdrachtnemer voorziet in adequate scheiding van de omgevingen van tenants in de oplossing. 3: Opdrachtnemer voorziet in adequate scheiding van de gegevens van gebruikers van tenants in de oplossing.
150.	Beveiliging	Client (access) devices binnen de geboden oplossing hebben een zero data footprint of zijn voorzien van adequate schijfverleuteling (ook bij een tijdelijke data footprint).
151.	Beveiliging	Ten behoeve van privacy wordt dataminimalisatie, privacy by design en privacy by default toegepast.
152.	Beveiliging	Biometrie is niet toegestaan.

9. Beveiliging

153.	Beveiliging	Voor alle door gebruikers binnen de oplossing gegenereerde of opgeslagen (persoons)gegevens is Opdrachtnemer verwerker. Opdrachtnemer committeert zich die niet voor eigen doeleinden te verwerken.
154.	Beveiliging	Opdrachtnemer voorziet in het verwijderen van alle gebruikershistorie na uitloggen door de gebruiker.
155.	Beveiliging	Retentie van centraal opgeslagen bestanden van gebruikers bedraagt maximaal 24 uur.
156.	Beveiliging	Opdrachtnemer voorziet in een mogelijkheid om disclaimer/gebruiksvoorwaarden te presenteren na inloggen, met als mogelijke acties expliciete acceptatie (met vastlegging) of uitloggen.

10. Privacy

157.	Privacy – Procedure	Opdrachtnemer heeft processen en procedures ingericht om te borgen dat de verwerkingen van persoonsgegevens in de Oplossing en door Opdrachtnemer conform de AVG en UAVG kunnen plaatsvinden. Opdrachtnemer garandeert naleving van de geldende wet- en regelgeving op het gebied van het gegevensbeschermingsrecht.
158.	Privacy – Binnen de EER	Opdrachtnemer zal alle (persoons)gegevens slechts binnen de EER (laten) verwerken. N.B. dit betreft alle verwerkingen, niet alleen opslag.
159.	Privacy – Datalek	Opdrachtnemer garandeert dat er geen doorgifte van persoonsgegevens van Opdrachtgever aan een onbevoegde derde partij plaats zal vinden, en dat persoonsgegevens van Opdrachtgever alleen worden verwerkt voor diens doeleinden.

10. Privacy

160.	Privacy – Procedure	Het verlenen van (tijdelijke) toegang tot persoonsgegevens aan medewerkers van de Opdrachtnemer wordt beperkt op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar.
161.	Privacy – Anonimiseren	Als het gaat om gegevens die in aanmerking komen voor anonimiseren (in het kader van en in de zin van de AVG), dan heeft de Oplossing de mogelijkheid om gegevens te kunnen anonimiseren en een rapport te genereren waaruit blijkt dat dit heeft plaatsgevonden.
162.	Privacy – Dataminimalisatie	De Oplossing biedt de mogelijkheid om het kopiëren en exporteren van persoonsgegevens te minimaliseren of te beperken. Als persoonsgegevens wél gekopieerd of geëxporteerd worden, dient dit gelogd te worden.
163.	Privacy – Opslagbeperking	Als persoonsgegevens uit de Oplossing worden verwijderd, moeten deze uit alle systemen/back-ups van Opdrachtnemer worden verwijderd. Voor backups geldt dat dit mag najlen tot maximaal de termijn waarbinnen Opdrachtnemer gehouden is nog te kunnen herstellen vanuit backups.
164.	Privacy – DPIA	Opdrachtnemer werkt mee met het uitvoeren van een Data Protection Impact Assessment (DPIA) volgens het model van Opdrachtgever.

11. Exit strategie

165.	Exit strategie – Algemeen	Opdrachtnemer verklaart dat hij bij het beëindigen van de Opdracht medewerking zal verlenen bij een soepele overgang van de dan bestaande dienstverlening naar Opdrachtgever en/of een (nieuwe) contractpartij.
166.	Exit strategie – Plan	Het exitplan beschrijft de wijze waarop de dienstverlening van Opdrachtnemer kan worden beëindigd. Als ook de wijze waarop Opdrachtnemer na beëindiging, samen met Opdrachtgever zal zorgen voor een continuering van deze dienstverlening bij Opdrachtgever of een door Opdrachtgever aan te wijzen dienstverlener. Het exitplan wordt initieel opgesteld door Opdrachtnemer voorafgaand aan de

11. Exit strategie

		ingebruikname van de Oplossing. Het exitplan wordt periodiek herzien en indien relevant geactualiseerd. Periodiek is (minimaal) jaarlijks of wanneer de situatie daartoe aanleiding geeft.
167.	Exit strategie – Plan	Het exitplan bevat een gedetailleerde weergave van alle uit te voeren activiteiten om de exit transitie tot een succes te maken. Dit omvat onder meer de wijze waarop Opdrachtnemer zorgdraagt dat Opdrachtgever de beschikking krijgt over de in de Oplossing opgeslagen gegevens en documenten. De doorlooptijd van de exit transitie is (maximaal) 3 maanden na de aanvang van de transitie.
168.	Exit strategie – Verwijderen data	Na afsluiting van de exit transitie zal door Opdrachtnemer de gehele omgeving worden 'geschoond', met andere woorden alle gegevens worden vernietigd/verwijderd. Opdrachtnemer levert hier bewijs van en zal op geen enkele wijze gegevens of informatie achterhouden. De geheimhoudingsplicht van Opdrachtnemer blijft ook na de exit transitie bestaan.
169.	Exit strategie – Overgangstermijn	Opdrachtnemer houdt rekening met een minimale overgangstermijn van 6 maanden na contracteinde. In deze periode behoudt Opdrachtgever het recht om de Oplossing op die wijze te gebruiken zoals deze zich op de datum van contracteinde voordeed. Hiermee wil Opdrachtgever borgen dat eventueel lopende procedures afgerond kunnen worden en dat bij implementatie van een Oplossing van een opvolgende leverancier op de informatie teruggevallen kan worden. De aanvullende kosten hiervoor worden bij de prijsstelling opgenomen.

12. Algemene eisen

170.	Algemene eisen – Vast contactpersoon	Opdrachtnemer stelt, ten behoeve van alle zaken met betrekking tot de uitvoering van de Opdracht één vaste contactpersoon beschikbaar voor de gehele duur van de Opdracht. Deze persoon beheerst uitstekend de Nederlandse taal in woord en geschrift.
171.	Algemene eisen – Proactief informeren	Opdrachtnemer brengt de Opdrachtgever zodra Opdrachtnemer weet of behoort te weten dat de nakoming van de opdracht niet of niet tijdig of niet naar behoren plaatsvindt, onmiddellijk schriftelijk én telefonisch op de hoogte onder vermelding van de omstandigheden.

12. Algemene eisen

172.	Algemene eisen – Communicatie-uitingen	Opdrachtnemer zal geen communicatie-uitingen doen over het contract of de relatie met Opdrachtgever zonder schriftelijke toestemming van Opdrachtgever.
173.	Proactiviteit	Opdrachtnemer informeert Opdrachtgever proactief over eventuele problemen rondom de beveiliging van aangeboden producten en/of diensten.
174.	Verwerkersovereenkomst	Opdrachtnemer wordt aangemerkt als ‘verwerker’ daarvoor sluiten partijen een Verwerkersovereenkomst af. De Verwerkersovereenkomst wordt gesloten conform Bijlage D.
175.	Wifi	Inzake het in- en uitloggen in de wifi-omgeving ligt het in de bedoeling dat Opdrachtgever deze werkzaamheden zelf wil gaan uitvoeren. In overleg met de Opdrachtnemer zal het moment en de wijze waarop deze overgang naar het inbesteden van deze dienst worden besproken Vanaf het moment van inbesteden zal een minder prijs op de maandfactuur gaan gelden.
176.	Correctheid gegevens	Opdrachtnemer verklaart dat alle bij Inschrijving overlegde gegevens juist, volledig en naar waarheid zijn ingevuld en gestand kunnen worden gedaan gedurende de gehele looptijd van de Overeenkomst inclusief eventuele verlengingen van de Overeenkomst
177.	Gebruik van naam en logo	Opdrachtnemer mag zonder uitdrukkelijke voorafgaande schriftelijke toestemming van Opdrachtgever in publicaties, reclame-uitingen of anderszins geen gebruik maken van de naam en/of het logo van Opdrachtgever.
178.	Onderaanneming	De inzet van onderaannemers voor de uitvoering van Leveringen en/of Diensten is alleen toegestaan na schriftelijke toestemming vanuit Opdrachtgever. Opdrachtnemer blijft bij de inzet van onderaannemers verantwoordelijk voor de algehele Overeenkomst. Opdrachtgever zal in geen geval rechtstreeks schakelen met onderaannemers van Opdrachtnemer

12. Algemene eisen

179.	Overlegstructuur	Opdrachtnemer en Opdrachtgever komen tijdens de implementatie van de dienstverlening een nadere overlegstructuur overeen. Deze overlegstructuur voldoet minimaal aan de volgende uitgangspunten: 1. Tactisch: Partijen organiseren minimaal 1x per 3 maanden een voortgangsoverleg. Tijdens het tactisch overleg wordt de uitgevoerde dienstverlening inhoudelijk geëvalueerd. Opdrachtnemer draagt zorg voor verslaglegging van de overlegmomenten. 2. Strategisch: Partijen organiseren minimaal 1x per jaar een strategisch overleg. Tijdens dit overlegmoment vindt formele evaluatie van de Overeenkomst plaats en wordt gezocht naar mogelijkheden om de samenwerking te verbeteren en/of te versterken. Opdrachtnemer draagt zorg voor verslaglegging van de overlegmomenten.
180.	Personeel	Opdrachtnemer garandeert dat de bij de uitvoering van de opdracht in te zetten medewerkers, die in contact staan met Opdrachtgever en/of werkzaamheden uitvoeren op een (externe) locatie van Opdrachtgever, de Nederlandse taal in woord en geschrift machtig zijn.
181.	Geheimhouding	Opdrachtnemer gaat ermee akkoord dat medewerkers die werkzaamheden op een (externe) locatie van Opdrachtgever verzocht kunnen worden om een geheimhoudingsverklaring te tekenen. Opdrachtnemer is verantwoordelijk voor naleving van de geheimhoudingsverklaringen
182.	VOG	Opdrachtnemer garandeert dat medewerkers die werkzaamheden op een (externe) locatie van Opdrachtgever uitvoeren de beschikking hebben over een Verklaring Omtrent Gedrag (VOG). De verantwoordelijkheid voor opvragen c.q. toetsen van de VOG's berust bij Opdrachtnemer. Op eerste verzoek van Opdrachtgever moet een medewerker van Opdrachtnemer de VOG kunnen overhandigen. Er mogen door Opdrachtnemer geen aanvullende kosten in rekening worden gebracht voor het opvragen van de VOG.
183.	Opvolgen huisregels en voorschriften	Opdrachtnemer garandeert dat medewerkers die werkzaamheden uitvoeren op (externe) locaties van Opdrachtgever, de van toepassing zijnde huisregels en voorschriften opvolgen. Medewerkers volgen

12. Algemene eisen

		daarnaast de instructies van medewerkers van Opdrachtgever (of door Opdrachtgever aangewezen partijen) op.
184.	Verpakkingen hardware	Opdrachtnemer zorg ervoor dat er zoveel mogelijk herbruikbare verpakking worden ingezet. De verpakkingen die Opdrachtnemer inzet dienen vrij te zijn van CFK. Opdrachtnemer draagt zorg voor een milieuvriendelijke verwerking/recycling van alle verpakkingen.
185.	Energy Star	Opdrachtnemer garandeert dat de te leveren producten voldoen aan de meest recente Energy Star-criteria die van toepassing zijn voor de desbetreffende productgroep.
186.	Beperking van klimaat impact	Opdrachtnemer neemt een proactieve rol aan met betrekking tot de verdere beperking van de klimaatimpact; gericht op zowel het logistieke proces als de hardware componenten die door Opdrachtgever afgenomen worden. Opdrachtnemer maakt minimaal éénmaal per jaar kenbaar welke interne en externe maatregelen er genomen kunnen worden om de klimaatimpact verder terug te dringen, Zie ook Beschrijven document, vraag Duurzaamheid .

13. Juridische eisen

187.	Juridische eisen – Inkoopvoorwaarden	De algemene en/of verkoopvoorwaarden van de Inschrijver worden nadrukkelijk van de hand gewezen. In de Inschrijving van de inschrijver wordt niet (deels) naar andere juridische voorwaarden verwezen.
188.	Wet- en regelgeving	Opdrachtnemer garandeert dat de aan te bieden Producten en/of Diensten voldoen aan alle van toepassing zijnde Nederlandse en Europese wet- en regelgeving.

14. Facturatie

189.	Facturatie	Opdrachtnemer verzendt, na volledige verrichting en acceptatie door Opdrachtgever, onder vermelding van de overeenkomst en het inkoopopdracht-nummer een factuur per uitgebrachte offerte met betrekking tot de (aanvullende) werkzaamheden.
190.	Facturatie – Betaling	Betaling vindt plaats na acceptatie van de resultaten van de Opdracht/levering van het product.
191.	Facturatie – Betalingstermijn	Opdrachtgever hanteert een betalingstermijn van dertig dagen na factuurdatum, mits de factuur onbetwist is.
192.	Facturatie – Gegevens	Een factuur bevat minimaal de volgende gegevens: Gegevens Opdrachtnemer - Bedrijfsnaam - Adres - Telefoonnummer - KvK-nummer - Btw-nummer - IBAN-rekeningnummer - Debiteurnummer - Btw-nummer Gegevens KB - Organisatienaam - Adres - Contractnummer

14. Facturatie

		Factuur gegevens - Factuurdatum - Factuurnummer - Ordernummer - Periode waar de factuur betrekking op heeft - Totaal factuurbedrag exclusief BTW - BTW-percentages - BTW-bedrag factuur - Totaal factuurbedrag inclusief BTW Kostenoverzicht als bijlage. Gegevens zoals gespecificeerd in de eis met betrekking tot het kostenoverzicht. De definitieve inhoud en opmaak van de verzamelfacturen wordt gedurende de implementatiefase in overleg tussen Opdrachtgever en de Opdrachtnemer vastgesteld.
193.	Facturatie – E-factuur	Facturen worden uitsluitend onder vermelding van het inkoopordernummer als e-factuur, volgens de UBL 2.1 standaard, via Peppol of digitaal in pdf-formaat aan digifez@kb.nl verstuurd.
194.	Facturatie - Afhandeling	Indien een factuur niet voldoet aan de Aanbestedingsstukken genoemde voorwaarden wordt de Opdrachtnemer hiervan binnen 14 kalenderdagen na ontvangst schriftelijk op de hoogte gebracht. De betreffende factuur wordt pas in behandeling genomen op het moment dat deze voldoet aan de in de Aanbestedingsstukken genoemde voorwaarden.
195.	Facturatie - Verrekening	Opdrachtgever is gerechtigd om indien er sprake is van door de Opdrachtnemer verschuldigde bedragen (creditering(en)) deze te verrekenen met bedragen die Opdrachtnemer verschuldigd is aan Opdrachtgever.