Bijlage 1 – Programma van Eisen

Het Programma van Eisen vormt een bijlage bij het Beschrijvend document voor de Europese aanbesteding Online cursussen Verdiepende Digitale basisvaardigheden van de KB. Het Programma van Eisen betreft enkel eisen aan de uitvoering van de Opdracht.
De met hoofdletter geschreven woorden refereren naar de definities zoals opgenomen in het "Beschrijvend Document"

Inhoudsopgave

1. Algemene eisen	
Eis 1.1.	Alle communicatie, documenten en correspondentie in het kader van deze Opdracht en de Nadere Opdrachten moeten in de Nederlandse taal worden gevoerd en/of opgesteld.
Eis 1.2.	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.
Eis 1.3.	Opdrachtnemer is voor de KB telefonisch en per e-mail bereikbaar op werkdagen tussen 08:00 uur en 18:00 uur.
Eis 1.4.	Opdrachtnemer brengt de KB, 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.
Eis 1.5.	Opdrachtnemer zal geen communicatie-uitingen doen over de Raamovereenkomst of de relatie met de KB zonder schriftelijke toestemming van de KB.
Eis 1.6.	Opdrachtnemer verklaart en staat er jegens KB voor in dat de Content geen inbreuk maakt op de rechten van Derden. Opdrachtnemer vrijwaart KB tegen elke rechtsvordering die gebaseerd is op de bewering dat (inhoud van de) Content en het in deze Overeenkomst bedoelde gebruik daarvan geheel of gedeeltelijk op enige wijze inbreuk maken op de (intellectuele eigendoms-) rechten van Derden.
Eis 1.7.	Opdrachtnemer is verantwoordelijk voor een afdracht aan de auteurs en eventuele andere makers en/of rechthebbenden van de Content voor de in deze Overeenkomst aan de KB verleende licentie en vrijwaart de KB tegen aanspraken ter zake hiervan.
Eis 1.8.	Opdrachtnemer verklaart en staat er jegens KB voor in dat zij geen met onderhavige Overeenkomst strijdige Overeenkomst heeft gesloten en volledig gerechtigd en bevoegd is de licentie te verlenen.

2. Dienstverlening	
	Licentie/Oefenmateriaal
Eis 2.1	Opdrachtnemer biedt ondersteuning voor bibliotheekmedewerkers: een handleiding voor gebruik van het volgsysteem en de mogelijkheid tot gebruik van een helpdesk van de Opdrachtnemer.
Eis 2.2	Het oefenmateriaal zoals genoemd in het beschrijvend document is geschikt om onder begeleiding te gebruiken in de bibliotheek, en is daarnaast ook zelfstandig te gebruiken
Eis 2.3	Het oefenmateriaal is volledig digitaal, op NT1 niveau en Nederlandstalig
Eis 2.4	Het oefenmateriaal voldoet aan eisen die aan de gehele Collectie gesteld worden (diversiteit en pluriformiteit)

Eis 2.5	Opdrachtnemer biedt minimaal 20 online cursussen met verschillende tijdskaders en werkvormen (bijvoorbeeld een uitgebreide cursus in meerdere delen, maar ook losse modules over één onderwerp), en is aan te passen aan de leerdoelen van de Actieve Gebruiker.
Eis 2.6	Het aangeboden pakket blijft actueel gedurende de gehele looptijd en wordt doorontwikkeld op basis van actualiteit daar waar van toepassing door de Opdrachtnemer in afstemming met de KB.
Eis 2.7	Het oefenmateriaal is geschikt voor de Doelgroep. Het oefenmateriaal bevat taken en Opdrachten die aansluiten op het niveau(s) van de Actieve Gebruikers binnen deze Doelgroep.
Eis 2.8	Opdrachtnemer verleent de gebruiksrechten als bedoeld in dit artikel mede aan de Staat der Nederlanden, nu KB het inkopen van de Content voor de Landelijke Digitale Bibliotheek verricht namens de Staat conform artikel 18 lid 1 jo. artikel 22 lid 2 Wsob (of het overeenkomende artikel in de meest recente versie van de Wsob). De gebruiksrechten als bedoeld in dit artikel gelden tevens voor Lokale Bibliotheken.
Eis 2.9	Opdrachtnemer beschikt over een platform bestaande uit een leeromgeving met oefenmateriaal voor cursisten en een volgsysteem voor begeleiders.
Eis 2.10	Opdrachtnemer stelt een interface van het platform beschikbaar waarop enkel het aanbod voor openbare bibliotheek en KB wordt getoond en het bredere aanbod van de Opdrachtnemer niet te zien is.
Eis 2.11	De verschillende interfaces van het platform moeten responsive zijn zodat de interfaces goed werken op beeldscherm, laptop, tablet/iPad en smartphone.
Eis 2.12	Een Actieve Gebruiker moet de eigen voortgang terug kunnen zien in het account
Eis 2.13	Thuisgebruik en bibliotheekgebruik is mogelijk
Eis 2.14	Het oefenmateriaal is beschikbaar voor bibliotheekleden en niet leden, via de bibliotheek
	Communicatie
Eis 2.15	Het is Lokale Bibliotheken, de KB en andere partijen, die de online cursussen beschikbaar stellen, toegestaan om merk en/of logo, beeltenis en metadata van de online-cursus en de Opdrachtnemer te gebruiken voor onder meer het aanbieden en promotiedoeleinden.
Eis 2.16	Opdrachtnemer communiceert twee weken van te voren over updates en inhoudelijke wijzigingen naar de KB, en werkt mee aan door de KB geïnitieerde Webinars/informatieoverdrachten naar bibliotheekmedewerkers. Daarnaast werkt de Opdrachtnemer mee aan in het kader van gebruiksonderzoek enquêtes uit te zetten na gebruik van de content (effectmeting).
Eis 2.17	Opdrachtnemer stelt zich op als meewerkend, proactieve partner van de KB. Zo helpt Opdrachtnemer de KB bij vraagstukken en vervolgacties rondom thema's als communicatie, marketing en onderzoek.
Eis 2.18	Op verzoek van De KB faciliteert Opdrachtnemer vervolgonderzoek onder de Actieve Gebruikers van de digitale Leeromgeving. .

Eis 2.19	De Opdrachtnemer verleent aan de KB een licentie die voorziet in het aanbieden en ontsluiten van de licentie aan Actieve Gebruikers, via de Landelijke Digitale Bibliotheek en de aangesloten Websites van Lokale bibliotheken. Lokale Bibliotheken, KB en andere partijen kunnen promotie maken voor en naar het aanbod van online cursussen.
	Toegang
Eis 2.20	Een Gebruiker heeft een account nodig. Deze kan de Gebruiker zelf aanmaken of met behulp van een Bibliotheekmedewerker.
Eis 2.21	Bibliotheekmedewerkers vanuit de bibliotheek kunnen accounts van de Actieve Gebruiker beheren, hebben inzicht in gebruikersvoortgang en -resultaten, en de mogelijkheid om modules/oefeningen klaar te zetten voor de deelnemer(s).
Eis 2.22	Partijen komen overeen dat de Content zal worden aangeboden in het Basispakket en dat deze door de Opdrachtnemer voor Gebruikers toegankelijk zal worden gemaakt.
Eis 2.23	De Opdrachtnemer zorgt ervoor dat op termijn (in afstemming met KB) het aangeboden platform is voorzien van de Authenticatievoorziening die aansluit op de Authenticatie voorziening (Landelijke inlogvoorziening, op basis van OIDC of SAML) van de KB waarmee Actieve Gebruikers kunnen inloggen op het platform.
Eis 2.24	De Opdrachtnemer zorgt ervoor dat op termijn (in afstemming met KB) door bibliotheekmedewerkers op het aangeboden platform kan worden ingelogd met het EenLogin systeem van de KB (Microsoft Entra ID).
Eis 2.25	Zolang er nog geen koppeling is met EenLogin van de KB wordt er gebruikt gemaakt van 2FA voor het inloggen door de bibliotheekmedewerker.
	Gebruikersgegevens
Eis 2.26	Voor elke Dienst levert de Opdrachtnemer periodiek en op verzoek van de KB de logging-gegevens of reeds geaggregeerde/geprepareerde gegevens met betrekking tot gebruik, deelnemers, aantal gestarte cursussen, aantal afgeronde cursussen, aantal hits per Bibliotheek ISIL c.q. per klant (appid) aan, in Excel, zodat de gebruiksgegevens direct opgenomen kunnen worden in het KB Datatheek. Indien er in een ander formaat dan Excel geleverd kan worden dan eerst overleg met de KB.
Eis 2.27	Opdrachtnemer biedt inzage in maandelijkse Actieve Gebruikersgegevens van online-cursussen via dashboard functie. In de dashboardfunctie is minimaal het volgende opgenomen: Aantal ingeschreven deelnemers, aantal deelnemers dat gestart is, Actieve Gebruikers, aantal gestarte cursussen, aantal afgeronde cursussen, top 10 gestarte cursussen, top 10 afgeronde cursussen. Deze indicatoren worden bij ingang van de Raamovereenkomst afgestemd, periodiek geëvalueerd en indien nodig bijgesteld zonder dat daar kosten aan verbonden zijn. De KB werkt toe naar het publiceren van gebruiksgegevens in het e-content dashboard voor openbare Bibliotheken, waarin aantallen per bibliotheekorganisatie inzichtelijk worden.

	Servicemanagement
Eis 2.28	De Leeromgeving en de aangeboden content is doorlopend beschikbaar (24 uur per dag, 7 dagen per week), met een minimaal beschikbaarheidspercentage van 99,5% per maand.
Eis 2.29	Het platform en het materiaal kunnen minimaal 5.000 Actieve Gebruikers tegelijkertijd aan.
Eis 2.30	Opdrachtnemer biedt de volgende servicelevels of vergelijkbaar dan wel beter op incidenten: Prioriteit hoog: de KB kan met een kritisch proces niet meer werken. Reactietijd en start oplossen binnen 1 uur. Maximale duur verstoring is 16 uur na melden. Prioriteit midden: de KB kan werken met een tijdelijke workaround. Reactietijd en start oplossen binnen 4 uur. Maximale duur verstoring is 24 uur na melden. Prioriteit laag: de KB kan gewoon doorwerken, de verstoring treft minder dan 10% van de Gebruikers en het getroffen proces is niet kritisch. Reactietijd en start oplossen binnen 8 uur. Opdrachtnemer zorgt dat bij 90% van de incidenten die hoog of midden zijn, de reactietijd en de tijd van de 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.
Eis 2.31	Opdrachtnemer garandeert adequate back-up- en restorevoorzieningen van de Leeromgeving, 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.
Eis 2.32	Opdrachtnemer zorgt ervoor dat de Oplossing in 95% van de gevallen een maximale wachttijd voor het opbouwen van een regulier scherm van 0,5 seconde heeft. In 99% van de gevallen bedraagt de wachttijd maximaal 1 seconde. Hierbij wordt er van uitgegaan dat de Gebruiker beschikt over voldoende bandbreedte (>1Mbit) en een lage latency (<60ms) aan de gebruikerszijde. Er mag geen performance degradatie plaatsvinden na verloop van tijd.
Eis 2.33	De Opdrachtnemer levert gedurende de looptijd van de opdracht periodiek rapportages aan de KB om de gezondheid van de applicatie te laten zien. In deze rapportage komen o.a. performance, incidenten, oplostijden naar voren.

Eis 2.34	Gedurende de looptijd van de Raamovereenkomst vindt minimaal tweemaal per jaar een strategisch en tactisch evaluatieoverleg plaats tussen een binnen de KB aangewezen functionaris en de accountmanager van Opdrachtnemer.
Eis 2.35	Opdrachtnemer is verantwoordelijk voor de schriftelijke vastlegging van de overleggen met de afgesproken acties en verbeterpunten en het (digitaal) aanleveren hiervan uiterlijk één week na het overleg. De KB is verantwoordelijk voor de agenda van dit overleg.
Eis 2.36	Opdrachtnemer sluit met de KB een Service Level Agreement (SLA) en indien van toepassing een Dossier Afspraken en Procedures (DAP). Inclusief afspraken over incident- en escalatiematrix, overlegstructuur en rapportages. De door de KB aangeleverde conceptversies van de SLA en DAP zijn daarin leidend. Voor zover niet afwijkend geregeld in het PvE, zijn de SLA-bepalingen leidend.
	Beëindiging
Eis 2.37	Opdrachtnemer verklaart dat hij bij het beëindigen van de Raamovereenkomst medewerking (bereidwillig en kosteloos) zal verlenen bij een soepele overgang van de dan bestaande dienstverlening naar de KB en/of een (nieuwe) Raamcontractpartij, waarover geen (extra) kosten in rekening kunnen worden gebracht bij de KB.
Eis 2.38	De Opdrachtnemer verwijdert bij het beëindigen van de Opdracht alle aanwezige data van gebruikers en bibliotheekmedewerkers (ook van back-ups) en kan aantonen dat dit ook is gebeurd.

3. Juridisch	
Eis 3.1.	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.
Eis 3.2.	Opdrachtnemer voert werkzaamheden uit in lijn met de geldende wet- en regelgeving.

4. Digitale toegankelijkheid	
Eis 4.1.	De dienst die door Opdrachtnemer wordt geleverd, wordt digitaal toegankelijk by design ontwikkeld. De dienst voldoet aantoonbaar aan de eisen voor digitale toegankelijkheid zoals omschreven in de Europese standaard EN 301 549 (meest recente versie), waarvan de internationale richtlijnen voor toegankelijkheid, de Web Content Accessibility Guidelines (WCAG), deel uitmaken. De dienst is ontwikkeld volgens de meest recente WCAG-richtlijnen, niveau A en AA.
Eis 4.2.	Opdrachtnemer levert bij oplevering een audit rapport waaruit blijkt dat getest is volgens een betrouwbare evaluatiemethode: WCAG-EM of een gelijkwaardige methode. Indien Opdrachtnemer niet volledig voldoet aan alle punten, dan garandeert Opdrachtnemer door het akkoord gaan met deze eis dat binnen het eerste jaar van de overeenkomst volledig zal worden voldaan aan de gestelde toegankelijkheidseisen.

Eis 4.3.	Iedere 3 jaar levert de Opdrachtnemer opnieuw een auditrapport volgens de WCAG-EM. Opdrachtnemer rapporteert minimaal halfjaarlijks over de oplostermijn en implementatie van de resterende geaccepteerde verbeterpunten, en over eventuele nieuwe verbeterpunten na uitbreiding van de dienst.

5. Duurzaamheid	
Eis 5.1.	Opdrachtnemer neemt een proactieve rol aan met betrekking tot de verdere beperking van de klimaatimpact.
Eis 5.2.	Opdrachtnemer maakt minimaal éénmaal per jaar kenbaar welke interne en externe maatregelen er genomen kunnen worden om de klimaatimpact verder terug te dringen.

6. Privacy (AVG)	
Eis 6.1.	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.
Eis 6.2.	Opdrachtnemer schrijft in via een Europese rechtspersoon. Opdrachtnemer en zijn subverwerkers, verwerken gegevens van de KB alleen binnen de EER (Europese Economische Ruimte).
Eis 6.3.	Indien Opdrachtnemer kwalificeert als Verwerker sluiten Partijen een Verwerkersovereenkomst af. Voordat Opdrachtnemer overgaat tot het verwerken van persoonsgegevens van de KB, is de Verwerkersovereenkomst afgesloten.
Eis 6.4.	De concept Verwerkersovereenkomst is van toepassing (zoals bijgevoegd bij de aanbestedingsdocumenten).
Eis 6.5.	Het verlenen van 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.
Eis 6.6.	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.
Eis 6.7.	De Oplossing biedt de mogelijkheid om bewaartermijnen in te schakelen en configureren voor het geautomatiseerd verwijderen van persoonsgegevens, zodanig dat het naleven van de geldende wet- en regelgeving door Opdrachtnemer wordt ondersteund. Als persoonsgegevens uit de Oplossing worden verwijderd, moeten deze uit alle systemen/back-ups van Opdrachtnemer worden verwijderd.
Eis 6.8.	Gegevens van de productie omgeving worden in beginsel niet gebruikt in een acceptatie/test of demo omgeving. Als voor bepaalde situaties

	productiegegevens toch nodig zijn in een andere omgeving, dan dient dit vooraf met de KB afgestemd te worden. Opdrachtnemer waarborgt dat bij het overzetten (uit de productieomgeving naar een andere omgeving) van de persoonsgegevens, deze worden geanonimiseerd, zodat gegevens niet meer te herleiden zijn naar natuurlijke personen.
Eis 6.9.	Opdrachtnemer is niet gerechtigd om de verkregen data, informatie en/of andere inzichten welke voortkomen uit het aangaan van deze Raamovereenkomst te gebruiken voor andere doeleinden (waaronder productverbetering) zonder nadrukkelijke schriftelijke toestemming door de KB.
Eis 6.10.	De KB is gerechtigd om de naleving van het Programma van Eisen bij Opdrachtnemer te toetsen of te laten toetsen door een onafhankelijke partij. Opdrachtnemer werkt hier volledig aan mee, onder meer door gevraagde documentatie aan te leveren en toegang te verlenen tot de gegevensbestanden en systemen waarbinnen de gegevens verwerkt worden. De KB mag maximaal één audit per jaar laten uitvoeren.
Eis 6.11.	Opdrachtnemer werkt -indien mogelijk- mee aan het uitvoeren van een Data Protection Impact Assessment (DPIA) volgens het model van de KB.
Eis 6.12.	Opdrachtnemer draagt zorg voor een adequate overdracht van alle relevante gegevens aan de KB of een door de KB aan te wijzen derde partij.

7. Informatiebeveiliging	
Eis 7.1.	Opdrachtnemer is verplicht om voorafgaande schriftelijke toestemming van de KB te verkrijgen indien de geleverde dienst of het product gebruikmaakt van een kunstmatige intelligentie (AI-systeem), zoals gedefinieerd in de AI-verordening (Verordening (EU) 2024/1689). Dit geldt zowel bij de initiële levering als bij iedere latere toevoeging, wijziging of activatie van een AI-component, inclusief situaties waarbij medewerkers van de Opdrachtnemer anderszins toegang krijgen tot AI zoals bijvoorbeeld via een koppeling met een AI-systeem van een derde partij. De Opdrachtnemer dient volledig te voldoen aan de AI-verordening, ook indien bepaalde bepalingen hiervan ten tijde van de aanbesteding nog niet van kracht zijn.
	Veilige softwareontwikkeling
Eis 7.2.	Opdrachtnemer scant broncode tijdens de ontwikkelcyclus regelmatig op kwetsbaarheden. Hierbij wordt gebruikgemaakt van ten minste een Static Application Security Testing (SAST) tool.
Eis 7.3.	Opdrachtnemer zorgt ervoor dat wijzigingen in broncode te allen tijde worden gereviewd middels een peer-review. Broncode mag slechts worden gepubliceerd naar productie na toepassen van het vierogenprincipe.
	Cookies
Eis 7.4.	Waar in de Oplossing gebruik wordt gemaakt van cookies dienen deze voorzien te zijn van de 'secure' en 'httponly' flags. Tevens bevatten cookies geen persoonlijke informatie en vindt de uitwisseling altijd via een beveiligde verbinding (HTTPS) plaats. De Oplossing is vrij van tracking cookies.

	Beveiligingstesten & het verhelpen van kwetsbaarheden
Eis 7.5.	Minimaal eens per jaar worden alle webapplicaties in scope van de dienstverlening onderworpen aan een penetratietest uitgevoerd door een gekwalificeerde externe partij. Opdrachtnemer stelt op verzoek van de KB de rapportage van de penetratietest beschikbaar.
Eis 7.6.	Minimaal eens per jaar worden alle API's in scope van de dienstverlening onderworpen aan een penetratietest uitgevoerd door een gekwalificeerde externe partij. Opdrachtnemer stelt op verzoek van de KB de rapportage van de penetratietest beschikbaar.
Eis 7.7.	Minimaal eens per jaar worden alle mobiele applicaties in scope van de dienstverlening onderworpen aan een penetratietest uitgevoerd door een gekwalificeerde externe partij. Opdrachtnemer stelt op verzoek van de KB de rapportage van de penetratietest beschikbaar.
Eis 7.8.	Minimaal eens per kwartaal wordt de digitale infrastructuur van de Oplossing gecontroleerd door Opdrachtnemer op zwakheden door middel van een vulnerability scan. Opdrachtnemer stelt op verzoek van de KB de rapportage van de vulnerability scan beschikbaar.
Eis 7.9.	Opdrachtnemer zorgt dat kwetsbaarheden zoals geïdentificeerd via een vulnerability scan (of via een ander medium) tijdig worden verholpen aan de hand van een door de KB geaccordeerd verbeterplan. Voor het oplossen van kwetsbaarheden worden geen aanvullende kosten in rekening gebracht door Opdrachtnemer.
Eis 7.10.	Geïdentificeerde kwetsbaarheden met een prioriteit 'Hoog' zoals aangegeven door het Nationaal Cyber Security Centrum (NCSC) of een CVSS v4 score van 9 of hoger worden onmiddellijk door de Opdrachtnemer verholpen conform het beveiligingsadvies van het NCSC of de Opdrachtnemer.
	API-beveiliging
Eis 7.11.	Opdrachtnemer past aantoonbaar de preventieve maatregelen zoals beschreven in de meest recente OWASP Top 10 API Security Risks (versie 2023) 'by design' toe tijdens het ontwikkelproces. Indien er gedurende het ontwikkeltraject een recentere versie door OWASP wordt gepubliceerd, borgt de Opdrachtnemer dat te allen tijde de meest recente versie van de OWASP Top 10 API Security Risks aantoonbaar wordt toegepast in haar ontwikkelproces.
Eis 7.12.	Opdrachtnemer beveiligt alle API’s in overeenstemming met de OWASP REST Security Cheat Sheet of de OWASP GraphQL Cheat Sheet.
Eis 7.13.	Opdrachtnemer zorgt dat alle API’s worden voorzien van sterke authenticatie en autorisatie. Het Oauth 2.0 autorisatie framework wordt bij voorkeur ondersteund.
Eis 7.14.	Opdrachtnemer zorgt dat al het API-verkeer wordt voorzien van rate-limiting en zorgt dat API's worden beschermd tegen misbruik (bijvoorbeeld brute-force-aanvallen, enumeratie).
Eis 7.15.	Het gebruik van API-gateways en validatiemechanismen is verplicht om injectieaanvallen te voorkomen en veilige communicatie te waarborgen.

Eis 7.16.	Voor API's die niet op basis van het OAuth 2.0 autorisatie framework worden beschermd en waarbij er sprake is van voorspelbare afnemers (de API is slechts voor een voorspelbare groep systemen of gebruikers bedoeld), dient de toegang tot de API te worden beperkt door middel van IP-whitelisting. Hiermee wordt het aanvalsvlak beperkt door ongeautoriseerde toegang te minimaliseren, ook wanneer een API-sleutel is gecompromitteerd.
Eis 7.17.	Opdrachtnemer zorgt dat API keys op een veilige wijze worden beheerd en opgeslagen.
Eis 7.18.	API keys worden op een veilige manier gegenereerd, bij voorkeur in een passende beveiligde omgeving;
Eis 7.19.	API keys worden versleuteld bewaard;
Eis 7.20.	API keys worden bewaard en beheerd in beveiligde omgeving (zoals Azure Key Vault, AWS Secrets Manager, of vergelijkbaar). API keys worden nooit hard-coded in broncode of configuratiebestanden bewaard;
Eis 7.21.	API keys worden voorzien van een key rotation policy. Alle keys worden voorzien van een vervaldatum om te voorkomen dat deze niet oneindig gebruikt kunnen worden. Nieuwe keys worden gegenereerd zodra de oude keys verlopen;
Eis 7.22.	Er is een mechanisme waarmee API keys onmiddellijk kunnen worden ingetrokken zodra ze gecompromitteerd of niet langer nodig zijn;
Eis 7.23.	Gebruik van API keys wordt gelogd, zodat ongeautoriseerd gebruik of misbruik kan worden gedetecteerd. Automatische waarschuwingen worden ingesteld om misbruik tijdig te detecteren.
	Hardening
Eis 7.24.	Componenten waaruit de Oplossing bestaat (zoals maar niet beperkt tot (Cloud)platforms, hypervisors, containerplatforms, (besturings)systemen, database platforms, (virtuele) servers) dienen door Opdrachtnemer afdoende te zijn gehardened aan de hand van CIS benchmarks of vergelijkbare voorschriften van de fabrikant (aan de hand van het comply or explain principe).
	PatchManagement
Eis 7.25.	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.
	Toegangsbeveiliging
Eis 7.26.	Het informatiesysteem biedt mogelijkheden tot het automatisch uitloggen van Gebruikers wanneer de Gebruiker een bepaalde periode inactief is. Deze periode is configurabel.
Eis 7.27.	Opdrachtnemer zorgt ervoor dat de wachtwoorden die worden toegepast, die niet worden beheerd binnen de Microsoft Entra ID van de KB, minimaal voldoen aan de wachtwoordcriteria die de KB hanteert. Deze criteria zijn configurabel.

Eis 7.28.	Opdrachtnemer zorgt ervoor dat wachtwoorden die ten behoeve van het informatiesysteem worden opgeslagen, welke niet worden beheerd binnen de Microsoft Entra ID van de KB, op adequate en actuele wijze worden versleuteld. De versleutelde opslag maakt uitsluitend gebruik van adequate encryptiestandaarden naar de stand van de techniek.
Eis 7.29.	Opdrachtnemer zorgt voor een sterk proces voor het aanvragen, wijzigen en wegnemen van toegangsrechten voor medewerkers die toegang nodig hebben tot broncode of infrastructuur voor het informatiesysteem. Opdrachtnemer zorgt te allen tijde dat de toegang tot onderdelen van het informatiesysteem wordt weggenomen voor medewerkers die geen toegang meer nodig hebben tot onderdelen van het informatiesysteem.
Eis 7.30.	Het informatiesysteem web interface biedt de mogelijkheid om met behulp van zelf te definiëren autorisatierollen (overeenkomstig het RBAC model) gebruikers toegang te geven tot specifieke functionaliteiten. Een optie/functionaliteit waar de gebruiker niet voor geautoriseerd is, is niet beschikbaar voor de gebruiker.
Eis 7.31.	'Secrets' zoals gebruikt voor authenticatie worden veilig bewaard in een 'key vault' of vergelijkbare toepassing. Secrets worden bij voorkeur automatisch geroteerd om de kans op misbruik te verkleinen.
Eis 7.32.	De Oplossing biedt de mogelijkheid om bij beëindiging van het dienstverband de toegekende autorisaties aan Gebruikers automatisch te laten vervallen.
Eis 7.33.	Opdrachtnemer zorgt dat de 'principle of least privilege', 'segregation of duties' en 'need to know' aantoonbaar worden toegepast in de geïmplementeerde autorisaties, zowel in applicaties als in de infrastructuur en hosting. Accounts krijgen niet meer rechten dan nodig, kunnen alleen informatie inzien die ze nodig hebben en bezitten geen rechten die conflicteren met de beoogde functiescheiding. Deze eis geldt zowel voor alle relevante persoonsgebonden accounts alsook voor alle relevante niet-persoonsgebonden accounts (zoals service-accounts en API-toegang).
	E-mail beveiliging
Eis 7.34.	Waar in de Oplossing gebruik wordt gemaakt van e-mail die namens de KB wordt verstuurd of ingelezen, dan wordt daarvoor bij absolute 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 de KB voor het verzenden of uitlezen van e-mail.
Eis 7.35.	In het geval dat een e-mailvoorziening wordt toegepast die niet verloopt via het e-mailplatform van de KB, dan zorgt Opdrachtnemer ervoor dat de e-mail herkenbaar is, op basis van domeinnaam van de KB, als e-mail van de Opdrachtgever.
Eis 7.36.	Waar de Oplossing gebruik maakt van e-mailverkeer dat namens de KB plaatsvindt (intern dan wel extern) voldoet de implementatie blijvend aan aanvullende beveiligingsmaatregelen als SPF, DKIM, DMARC en DANE (eventueel na implementatie door Microsoft).

	Versleuteling
Eis 7.37.	Opdrachtnemer zorgt dat alle netwerkverbindingen zijn voorzien van adequate versleuteling. Bij voorkeur wordt gebruikgemaakt van HTTPS of vergelijkbare marktconforme versleutelingstechnieken die passen bij het netwerkprotocol. Netwerkverbindingen omvatten zowel verbindingen van en naar de internet-facing interfaces, alsmede de netwerkverbindingen binnen de hosting-infrastructuur.
Eis 7.38.	De Oplossing maakt standaard gebruik van veilige communicatieprotocollen zoals HTTPS, SSH en SFTP. Waar HTTPS wordt toegepast, vindt dit plaats conform de 'Transport Layer Security (TLS) Beveiligingsrichtlijnen' versie 2025-05 van het NCSC, wat onder andere betekent dat minimaal TLS 1.2 en bij voorkeur TLS 1.3 (dan wel nieuwer) wordt toegepast. Voorts wordt HSTS gehanteerd.
Eis 7.39.	Certificaten en encryptiesleutels worden veilig beheerd en bewaard in een daartoe geschikte 'key vault' of vergelijkbare toepassing. Certificaten en encryptiesleutels worden bij voorkeur automatisch geroteerd.
	Logging en monitoring
Eis 7.40.	Opdrachtnemer zorgt voor monitoring van de beschikbaarheid en performance van de Oplossing en zorgt dat de KB onmiddellijk wordt geïnformeerd bij onder andere (niet uitputtend): uitval, performanceproblemen, (Distributed) Denial of Service aanvallen en onverklaarbaar hoog netwerkverkeer.
	Back-up en herstel
Eis 7.41.	Opdrachtnemer heeft een 'Disaster Recovery Plan'. Het Disaster Recovery Plan beschrijft hoe de dienstverlening die aan de KB wordt geleverd wordt hersteld bij een ramp of andersoortig incident. Opdrachtnemer onderhoudt het Disaster Recovery Plan en zorgt dat de inhoud actueel wordt gehouden.
Eis 7.42.	Opdrachtnemer test jaarlijks de werking van het Disaster Recovery Plan. Opdrachtnemer deelt op verzoek van de KB een gedocumenteerde evaluatie van de Disaster Recovery Plan test.
	Incidentafhandeling
Eis 7.43.	Bij het voordoen van een potentieel informatiebeveiligingsincident met een impact op data, systemen of medewerkers van de KB meldt de Opdrachtnemer dit onverwijld aan de KB via het CSIRT-KB.
	Denial of Service bescherming
Eis 7.44.	Opdrachtnemer zorgt dat alle internet-facing endpoints worden beschermd tegen overbelasting door het toepassen van rate limiting en throttling.

8. Facturatie	
Eis 8.1.	Opdrachtnemer verzendt, na volledige verrichting en acceptatie door de KB, onder vermelding van de Raamovereenkomsten het inkoopopdracht-nummer een factuur met betrekking tot de (aanvullende) werkzaamheden.

Eis 8.2.	De KB hanteert een betalingstermijn van dertig dagen na factuurdatum, mits de factuur onbetwist is.
Eis 8.3.	Een factuur bevat minimaal de volgende gegevens: **Gegevens Opdrachtnemer** • Bedrijfsnaam • Adres • Telefoonnummer • KvK-nummer • Btw-nummer • IBAN-rekeningnummer • Debiteurnummer **Gegevens KB** • Organisatienaam • Adres • Contractnummer **Factuur gegevens** • Factuurdatum • Factuurnummer • Inkooporderdernummer • Periode waar de factuur betrekking op heeft • Totaal factuurbedrag exclusief btw • Btw-percentage • 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 de KB en de Opdrachtnemer vastgesteld.
Eis 8.4.	Facturen worden uitsluitend als e-factuur (UBL 2.1). Een leesbare PDF-kopie mag als bijlage worden toegevoegd onder vermelding van het inkooporderdernummer aan facturen@kb.nl verstuurd.
Eis 8.5.	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.
Eis 8.6.	De KB 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 de KB.