Bijlage 7 Programma van Eisen

Vakbekwaamheidsmanagementsysteem (VMS)

De eisen in dit Programma van Eisen zijn uitsluitende (knock-out) criteria. Het niet voldoen aan deze eisen heeft uitsluiting van verdere deelname aan deze aanbestedingsprocedure tot gevolg.

Minimumeisen	
Eis	**Omschrijving van de eis**
1	Een VMS-oplossing waarmee de Veiligheidsregio Amsterdam Amstelland in staat is, om zijn door de Overheid en Gemeenten opgelegde taken rond de thema's; vakbekwaam blijven en vakbekwaam onderhouden te managen en monitoren van het competentie niveau.
2	De VMS-oplossing informeert de organisatie, d.m.v. rapportage link en de professional d.m.v. persoonlijk inzicht, over de vakbekwaamheidsverplichtingen.
3	De VMS-oplossing met zijn toepassingen, is functioneel en operationeel te koppelen met andere applicaties binnen de VrAA.
4	De VMS-oplossing maakt gebruik van personeelsdata, verstrekt uit de datakluis (momenteel applicatie AFAS) wat is aangesteld als basis documentatie en leidend voor het applicatie landschap.
5	De afdeling Vakbekwaamheid moet in de VMS-oplossing alle vakbekwaamheidsverplichtingen voor zowel mono- als multidisplinaire teams kunnen registreren ten dienste van alle gebruikers.
6	De oplossing moet informatie die van buiten de Veiligheidsregio Amsterdam-Amstelland komt, kunnen koppelen, niet uitputtende voorbeelden zijn; de Arbowet, - catalogus, landelijke opgesteld beleid, Vakraden, Branche richtlijnen Duiken.
7	De VMS-oplossing is een bestaande, direct implementeerbare standaardapplicatie. Afwijkingen op de standaard worden uitsluitend via akkoord van de Opdrachtgever doorgevoerd. Maatwerk is alleen toegestaan als het upgrade pad behouden blijft.
8	De VMS-oplossing wordt geleverd als volledig door de Opdrachtnemer beheerde SaaS (Software as a Service) dienst. De Opdrachtnemer is verantwoordelijk voor hosting, patches, monitoring, beveiliging.
9	De beschikbaarheid van de primaire functionaliteiten bedraagt ≥99,9% tijdens werkuren (07:00–18:00) met uitzondering van maximaal 4 geplande onderhoudsmomenten per kalenderjaar. En ≥99,5% daarbuiten, exclusief gepland onderhoud (≥7 dagen, buiten 18:00–07:00).
10	Rapportages volgens vooraf gedefinieerde lay-outs; aanvrager en opmaker worden gelogd. Rapportage en loginformatie wordt minimaal 12 maanden bewaard, of langer in overeenstemming met wetgeving.

11	De VMS-oplossing ondersteunt de volledige lifecycle (test, acceptatie, productie) met representatieve data en identieke configuratie ten opzichte van productie.
12	De VMS-oplossing genereert automatisch vaardigheid certificaten zodra aan vooraf ingestelde criteria is voldaan. Sjablonen voor certificaten kunnen ingesteld worden door de opdrachtgever.
13	De VMS-oplossing voldoet aantoonbaar aan de verplichte open standaarden (Forum Standaardisatie), loopt maximaal één major versie achter en verwerkt wijzigingen binnen 12 maanden; de oude standaard blijft minimaal 12 maanden ondersteund.
14	De web interface is veilig toegankelijk in de laatste twee versies van Microsoft Edge, Google Chrome en Apple Safari, zonder gebruik van plug-ins (zoals Flash, Silverlight of ActiveX).
15	De Opdrachtnemer werkt in overeenstemming met ISO 27017 en ISO 27018 (of gelijkwaardig) en past privacy by design toe. Verwerking en opslag vinden plaats binnen de EER, aantoonbaar via passende Assurance (Bijvoorbeeld een derden verklaring).
16	De VMS-oplossing past 'Single Sign-On' (SSO) toe én biedt Multi-Factor-Authenticatie (MFA) als authenticatiemiddel aan via SSO. De VMS-oplossing ondersteunt authenticatie op basis van SAML 2 of Oauth. Authenticatie verloopt bij de Opdrachtgever via de Azure Active Directory (AAD)/ Microsoft Entra ID van de Opdrachtgever. Multi-Factor-Authenticatie (MFA), wordt afgedwongen door de SSO-inlog via de AAD.
17	De leverancier volgt relevante NCSC-beveiligingsadviezen op; opvolging wordt vastgelegd in releasenotes.
18	Bij het sturen en ontvangen van e-mails wordt gebruik gemaakt van alle hiervoor relevante, voor overheden verplichte, beveiligingsstandaarden. Voor het versturen en ontvangen van e-mails worden SPF, DKIM en DMARC toegepast. Voor het mailen vanuit de VMS-oplossing wordt er gebruik gemaakt van STARTTLS 1.2, waarbij een DKIM-sleutel mogelijk is. Andere standaarden waar de VMS-oplossing aan moet voldoen met een 'secure connections', zijnde: DNSSEC, DANE en IPv4 en IPv6, HTTPS en HSTS-verkeer. Hierop kan getoetst worden via www.internet.nl.
19	Updates en upgrades worden binnen 3 maanden na release kosteloos geleverd. Bij security alerts meldt de leverancier binnen 3 werkdagen aan de opdrachtgever en treft binnen 3 werkdagen maatregelen.
20	De Opdrachtnemer documenteert ondersteunings-, storing/downtime-, release en datalekprocedures met duidelijk eigenaarschap, doorlooptijden en updatefrequentie.
21	Alle data uit de VMS-oplossing is relationeel te exporteren middels een API, met bijbehorend datamodel en documentatie die voldoet aan de open API-specification. Voor aanvullende info, zie: https://www.forumstandaardisatie.nl/open-standaarden/openapi-specification.
22	De REST API voldoet aantoonbaar aan de REST API Design Rules van het Forum Standaardisatie (open standaard) en wordt geleverd inclusief OpenAPI specificatie. De API ondersteunt lees en schrijfacties in overeenstemming met deze standaard. De performance eis bedraagt p95 < 3s per API-call.

23	Indien relevant kan de beheeromgeving gegevens afnemen via webservices/API's van Geo4OOV, PDOK en DSO. Toepasselijkheid wordt vooraf vastgesteld.
24	De VMS-oplossing ondersteunt minimaal de volgende coördinatenstelsels: het Nederlandse stelsel van Rijksdriehoekmetingen (RD), het European Terrestrial Reference System 1989 (ETRS89) en het World Geodetic System 1984 (WGS 84).
25	De VMS-oplossing ondersteunt het metrisch stelsel met meeteenheden zoals mm, cm, m, hm, km et cetera.
26	Autorisaties zijn rol /attribuut gebaseerd (RBAC/ABAC) op persoon, rol en functie. Meerdere rollen per gebruiker zijn mogelijk Rapportage autorisaties zijn per rol/laag configureerbaar. Geautoriseerde beheerders kunnen zelf servicerapporten bouwen binnen hun bevoegdheden.
27	Standaard wachtwoorden moeten direct bij installatie gewijzigd worden bij een lokale login. Fysiek op een eventueel apparaat, maar ook op web interfaces direct bij installatie. Er mag geen gebruik worden gemaakt van een serviceprovider generiek wachtwoord.
28	Als er gewerkt wordt met een certificaat of certificaten, dan worden alleen certificaten toegestaan van vertrouwde certificerings-instanties. De verbindingen tussen de VMS-oplossing en gebruikers dienen met HTTPS (via poort 443) beveiligd te worden.
29	De verbindingen tussen de VMS-oplossing en gebruikers dienen met HTTPS (via poort 443) beveiligd te worden.
30	Functionele beheertaken worden zonder merkbare verstoring uitgevoerd. Impactvolle taken vinden buiten piekuren plaats en worden vooraf aangekondigd.
31	Niet muteerbare logging registreert gebruikersactiviteiten, uitzonderingen, beveiligingsgebeurtenissen, dossier en rolwijzigingen en beheeracties. Bewaartermijn: minimaal 12 maanden of langer in overeenstemming met wet.
32	Updates en aanpassingen worden getest en in afstemming met de Opdrachtgever in de T&A (Test & Acceptatie) omgeving, na goedkeuring op de productieomgeving uitgezet.
33	De Opdrachtnemer borgt back up en herstel met RPO ≤24 uur en RTO ≤8 uur. Restore wordt periodiek getest en gerapporteerd. Back-ups dienen minimaal 3 en maximaal 12 maanden bewaard te worden, of zo lang als nodig is volgens de Archiefwet.
34	Gedurende de contractduur (inclusief de eventuele verlengingen) heeft Opdrachtgever onbeperkt gebruiksrecht binnen de eigen infrastructuur en recht op onderhoud en support inclusief updates en upgrades.
35	Continuïteit is geborgd via escrow of open source beschikbaarstelling van broncode, build scripts en documentatie. Trigger events en third party maintenance zijn geregeld; escrow is in de prijs inbegrepen.
36	Bij calamiteiten buiten invloed van de leverancier wordt de dienstverlening binnen 48 uur hersteld, rekening houdend met ketenafhankelijkheden. Na herstel is de VMS-oplossing direct weer beschikbaar voor eindgebruikers in overeenstemming met de overeenkomst.

37	Minimaal eens per 2 jaar wordt een pentest uitgevoerd; kritieke bevindingen worden binnen afgesproken SLA termijnen verholpen en gerapporteerd.
38	Bij een veiligheidsincident is relevante logging minimaal 1 jaar beschikbaar; logs zijn passend versleuteld en integraal.
39	Doorontwikkeling zonder meerkosten betreft uitsluitend wettelijk verplichte wijzigingen, wijzigingen i.v.m. open standaarden en security updates. Overige wijzigingen verlopen via het changeproces.
40	De VMS-oplossing (zowel gebruik als onderhoud), gebruikers en beheerdocumentatie zijn Nederlandstalig (niveau C1).
41	De applicatie is ook webbased, via intranet en internet toegankelijk en responsive op desktop, laptop, tablet en mobiel (moderne browsers).
42	De UI is gebruiksvriendelijk en Nederlandstalig; kritieke taken zijn met minimale handelingen uit te voeren volgens een consistent navigatiepatroon.
43	Toegang en functionaliteit worden per account bepaald via rol gebaseerde autorisaties, met periodieke re certificatie.
44	Inzage en mutatierechten in het persoonlijke vakbekwaamheidsdossier zijn geregeld voor de medewerker en aangewezen rollen (bijv. leiding/P&O) in overeenstemming met autorisatiebeleid met audittrail.
45	De VMS-oplossing ondersteunt upload van PDF, JPG en MP4 met virusscan, toegestane bestandstypen en instelbare maxima.
46	De VMS-oplossing ondersteunt het gebruik van tablets, smartphones en andere mobiele devices via aangepaste interface (app) of responsive design.
47	Vóór livegang levert de Opdrachtnemer een integraal beheerdocument (functioneel, security, privacy, archivering, beheerprocedures).
48	Elke gebruiker heeft een persoonlijk dashboard met status, planning, jaarvoortgang en openstaande verplichtingen.
49	De applicatie en app verwijzen naar helpdesk en functioneel beheer.
50	P&O (Personeel en Organisatie) en gebruiker kunnen externe diploma's/certificaten toevoegen binnen autorisatiekaders; mutatieherkomst wordt vastgelegd.
51	Gedelegeerde registratie is toegestaan met logging; de medewerker blijft eindverantwoordelijk.
52	Opnemen in de SLA • Updates, upgrades & NCSC beveiligingsadviezen beschrijven in de SLA. • Documenteren en registreren beschrijven in de SLA. • Updates en upgrades definities opnemen in de SLA. • Wijzigingen verlopen via het changeproces, beschrijven in de SLA. • Ketenafhankelijkheden bij calamiteiten beschrijven in de SLA.

	• Pentest criteria opnemen in de SLA. • SCORM-koppeling behoefte beschrijving opnemen in de SLA.

Bijlage: Lijst van afkortingen en begrippen

Microsoft Edge	Webbrowser van Microsoft.
Google Chrome	Webbrowser van Microsoft voor; bezoek websites, video bekijken en apps.
Apple Safari	Webbrowser van Apple.
Flash	Geheugen oplossing zonder stroomgebruik.
Silverlight	Bouwen interactieve wegapplicaties en media content.
ActiveX	Technologie voor herbruikbare softwarecomponenten.
NSCS	Nationaal Cyber Security Center/ Cyber Veiligheid voor Overheidsinstanties.
Pentest	Applicatie veiligheid en kwetsbaarheid toets.
PDF	Om documenten op te slaan, gelijk aan het origineel.
MP4	Multimediacontainerformaat voor video, audio, ondertiteling en afbeeldingen.