Bijlage 4 Programma van Eisen

Dit document bevat de eisen die aan de opdracht worden gesteld. Inschrijver verklaart door in te schrijven bij uitvoering van de opdracht volledig te voldoen aan deze eisen en alle overige eisen die in de Aanbestedingsstukken zijn genoemd.

Indien uit de Inschrijving blijkt dat aan één of meerdere van deze eisen niet wordt voldaan, dan wordt de inschrijving uitgesloten van verdere deelname aan deze aanbestedingsprocedure.

Algemene eisen

Eis 1.	IAM ondersteunt relevante en betreffende bedrijfsvoerings(keten)processen in relatie tot de op te leveren project resultaten. Dit is in lijn met de MORA (https://mora.mbodigitaal.nl).
Eis 2.	IAM sluit aan op de sector architectuur; https://mbodigitaal/mosa.
Eis 3.	IAM sluit aan op vervolgonderwijs (mbo, ho) en digitale sectorvoorzieningen.
Eis 4.	Leverancier levert één geïntegreerde, flexibele en modulair opgebouwde SaaS-voorziening, die gebaseerd is op open standaarden en aansluit bij de uitgangspunten van interoperabiliteit.
Eis 5.	IAM levert bedrijfsvoeringservices inclusief ondersteuning en doorontwikkeling.
Eis 6.	IAM is passend en meebewegend binnen het VISTA college Informatievoorziening (IV) en ICT-landschap (waaronder het blijven voldoen aan (onderwijs) wet- en regelgeving) gedurende de looptijd van de overeenkomst.
Eis 7.	De gebruikersinterface (inclusief online helpteksten) is intuïtief ingesteld en communiceert in de Nederlandse taal en/of Engels. Voorkeur kan ingesteld worden op Nederlands.
Eis 8.	Leverancier draagt zorg voor het meenemen van de gebruikers- en beheerorganisatie VISTA college inclusief relevante externe partners en leveranciers gedurende de contractperiode (training, begeleiding, ondersteuning). De gehele support is Nederlandstalig (woord en geschrift).
Eis 9.	De performance betreft een SaaS-oplossing. De wachttijd voor eindgebruikers bij schermwisselingen is aantoonbaar < 2 seconden per uitgevoerde beeldschermtransactie, bij concurrent gebruik van 20 gebruikers of minder. Dit bij voldoende bandbreedte en netwerkcapaciteit aan de gebruikerskant (buiten de invloedssfeer van Leverancier). Leverancier geeft de minimale bandbreedte vereiste vanuit de client richting de SaaS-toepassing. Ter informatie, op een VISTA college locatie is draadloos de primaire toegang.
Eis 10.	De responsetijd voor online functionaliteit / transacties tijdens kantooruren ligt voor minimaal 95% aantoonbaar op <1 seconden (SaaS-variant). Dit bij voldoende bandbreedte en netwerkcapaciteit aan de gebruikerskant (buiten de invloedssfeer van Leverancier).
Eis 11.	Voor veelgebruikte reguliere rapportages en opvragingen wordt een goede responsetijd gevraagd van < 5 seconden in minimaal 95% van de gevallen. Dit bij voldoende bandbreedte en netwerkcapaciteit van aan de gebruikerskant (buiten de invloedssfeer van leverancier).
Eis 12.	De SaaS-applicatie is webbased en via het internet 24/7 beschikbaar met een service level van minimaal 99,5% en dient ondergebracht te zijn binnen de Europese Economische Ruimte (EER).
Eis 13.	Leverancier draagt zorg dat de applicatie in Nederland via publiek internet beschikbaar is met de hierboven gespecificeerde performance. Leverancier maakt gebruik van DDoS mitigerende maatregelen zodat de SaaS-oplossing conform de hierboven gespecificeerde performance beschikbaar blijft. Toegang tot de SaaS-dienst verloopt ten alle tijden via beveiligde verbinden (standaard, onder andere via https).
Eis 14.	De SaaS-dienstverlening en ondersteuning van de IAM oplossing dient te voldoen aan: 1. ISO/IEC 25010:2023 – productkwaliteitsmodel (meetbaar, robuust en gebruikersgericht), 2. ISO/IEC 25019:2023 – kwaliteit in gebruik (gebruikservaring, effectiviteit en tevredenheid), 3. ISO/IEC 25002:2024 – raamwerk voor structurering en toepassing van kwaliteitmodellen (meting, evaluatie en governance). Deze standaarden ondersteunen VISTA college in het realiseren van hoogwaardige, betrouwbare en gebruiksvriendelijke SaaS-oplossingen die aansluiten bij onze onderwijsbehoeften — zowel bij ingebruikname als gedurende de volledige contractduur.
Eis 15.	De documentatie is Nederlandstalig en bevat een functionele en technische beschrijving. Leverancier levert de (eind)gebruikers- en beheerhandleiding aan en houdt deze up-to-date.
Eis 16.	Gedurende looptijd van de overeenkomst heeft VISTA college de mogelijkheid tot het uitvoeren van audits op de serviceorganisatie en dienstverlening van de aanbieder door eigen of andere (externe) auditors.
Eis 17.	De aangeboden SaaS-dienstverlening is onderverdeeld in meerdere logische lagen (presentatie, logica, data). De aangeboden SaaS-dienstverlening is volledig functioneel op mobiele devices

	(Windows, iOS en Android) via web interface of app en is te gebruiken op verschillende operating systems, waaronder in ieder geval Microsoft Windows, Mac OS en Linux. Het ondersteunt en volgt de (keten)processen zoals beschreven in de MORA in relatie tot de aangeboden SaaS-dienstverlening.
Eis 18.	In de aangeboden SaaS-omgeving kunnen businessrules worden ingesteld. Daarnaast bestaat de mogelijkheid om een centrale businessrule engine aan te roepen waar de aangeboden SaaS-omgeving op acteert.
Eis 19.	Indien Leverancier in de aangeboden dienstverlening en ondersteuning gebruik maakt van kunstmatige intelligentie (AI), gelden de volgende voorwaarden: a. het gebruik van AI wordt expliciet beschreven: waarom, wanneer en hoe AI wordt toegepast; b. AI-toepassingen zijn transparant, uitlegbaar (Explainable AI) en auditeerbaar; c. AI-toepassingen voldoen aan de EU-richtlijnen voor betrouwbare AI en aan de verplichtingen uit de AI Act; d. geconstateerde tekortkomingen worden door Leverancier op eigen kosten hersteld; e. indien AI onderdeel uitmaakt van de dienstverlening, wordt dit opgenomen in het prijzenblad, onderverdeeld in standaarddiensten, periodieke standaarddiensten en optionele diensten Indien kunstmatige intelligentie onderdeel uitmaakt van de aangeboden dienstverlening en ondersteuning functioneert dit nooit als een blackbox en is auditeerbaar. Het herstellen van eventueel geconstateerde tekortkomingen komt voor rekening van Leverancier.

Technische eisen

Eis 20.	De oplossing dient beschikbaar te zijn als SaaS-oplossing en inzetbaar te zijn binnen hybride IT-landschappen.
Eis 21.	*Schaalbaarheid* De oplossing dient schaalbaar te zijn naar minimaal: • 25.000 gebruikers • 100 gekoppelde applicaties • 1 miljoen autorisaties zonder functionele beperkingen.
Eis 22.	*Disaster Recovery* De oplossing dient een Disaster Recovery-voorziening te bevatten.
Eis 23.	*Back-ups* De oplossing dient dagelijkse back-ups uit te voeren en minimaal 45 dagen te bewaren.
Eis 24.	*Encryptie tijdens transport* Alle communicatie dient versleuteld plaats te vinden met TLS 1.2 of hoger.
Eis 25.	*Role Based Administration* Beheerrechten dienen op basis van rollen toegekend te worden.
Eis 26.	De applicatie biedt de mogelijkheid om naast de Productie-omgeving andere (test)omgevingen te onderhouden, waaronder ten minste één omgeving/sandbox voor opleidingsdoeleinden van gebruikers en functionele testen (bv. testen van nieuwe configuratie-settings) die is meegenomen in de prijs.
Eis 27.	Optioneel is het mogelijk een volledige Ontwikkel Test Acceptatie Productie (OTAP) omgeving(en) af te nemen. Afspraken met betrekking tot verversing frequentie en kosten zijn ondergebracht in SLA/DAP en prijzenblad.

Architecturale eisen

Eis 28.	De oplossing ondersteunt een modulaire inrichting waarbij IAM/IGA, integratie en gegevensbeheer logisch van elkaar zijn gescheiden. De oplossing mag niet vereisen dat algemene gegevensuitwisseling of niet-IAM-functionaliteit uitsluitend binnen het IAM/IGA-product wordt ingericht.
Eis 29.	De oplossing kan meerdere door VISTA college aangewezen gezaghebbende bronsystemen gebruiken en respecteert per gegeven welke bron leidend is.
Eis 30.	De oplossing ondersteunt de volledige levenscyclus van identiteiten, relaties en toegangsrechten: aanmaken, wijzigen, tijdelijk opschorten, herstellen en beëindigen.
Eis 31.	De oplossing ondersteunt meerdere gelijktijdige relaties en contexten per persoon of andere entiteit zonder te vereisen dat alle contexten tot één universele identiteit worden samengevoegd.

Eis 32.	De oplossing biedt gedocumenteerde, open en versie-beheerbare koppelvlakken en ondersteunt gangbare open standaarden voor identity en toegang. Minimaal: SAML 2.0, OpenID Connect, OAuth 2.x, SCIM 2.0, OEAPI en SOAP REST/API; event- of webhookintegratie (één technische manier om zo'n gebeurtenis direct door te geven) moet mogelijk zijn.
Eis 33.	De oplossing ondersteunt federatieve toegang en kan aantoonbaar integreren met SURFconext en toekomstige opvolgende/aanvullende SURF-voorzieningen. Ook koppeling met eduID en ECKid moet mogelijk zijn waar VISTA college dat toepast.
Eis 34.	De oplossing ondersteunt snelle en aantoonbare intrekking van identiteiten, relaties, rechten en toegang wanneer de onderliggende relatie of bevoegdheid eindigt of wordt ingetrokken.
Eis 35.	Iedere kritieke mutatie en ieder relevant autorisatiebesluit is herleidbaar tot bron, toegepaste regel, actor, tijdstip, resultaat en waar van toepassing goedkeuring.
Eis 36.	De oplossing ondersteunt identity governance voor niet-menselijke identiteiten, waaronder serviceaccounts, API-identiteiten, workloads en AI-agents. Iedere dergelijke identiteit kan worden gekoppeld aan een verantwoordelijke eigenaar, doel, mandaat/bevoegdheid, rechten, geldigheidsduur en auditinformatie en kan afzonderlijk worden uitgeschakeld.
Eis 37.	De oplossing is configureerbaar zonder onnodige product specifieke maatwerkcode. Uitbreidingen gebruiken door Leverancier ondersteunde extensiemechanismen en mogen reguliere SaaS-upgrades niet blokkeren.
Eis 38.	De architectuur mag toekomstige aansluiting op digitale wallets en verifieerbare digitale bewijzen niet blokkeren. De oplossing mag daarvoor geen verplichte afhankelijkheid introduceren van één specifieke wallet, SSI-, DID-, blockchain- of andere leveranciersspecifieke technologie. DID (Decentralized Identifier): een gestandaardiseerde digitale identifier die niet afhankelijk hoeft te zijn van één centrale beheerder. Blockchain: een vorm van gedistribueerde registertechnologie die in sommige identity-oplossingen wordt gebruikt, maar geen noodzakelijke voorwaarde is voor digitale wallets of verifieerbare bewijzen.
Eis 39.	Leverancier maakt alle in de dienstverlening gebruikte AI-functionaliteit expliciet inzichtelijk. AI-functionaliteit die persoonsgegevens, identiteitsgegevens, toegangsrechten of autorisatiebesluiten verwerkt, moet afzonderlijk configureerbaar en waar functioneel mogelijk uitschakelbaar zijn. Gegevens van VISTA college mogen niet zonder voorafgaande schriftelijke toestemming van VISTA college worden gebruikt voor het trainen of verbeteren van generieke AI-modellen. Kritieke toegangs- en autorisatiebesluiten blijven herleidbaar en onder menselijke verantwoordelijkheid.
Eis 40.	De aangeboden oplossing voldoet aan de vastgestelde architectuurprincipes* VISTA college. * Een architectuurprincipe is een beleidsuitspraak die specifiek betrekking heeft op de inrichting van producten, organisatie, processen en informatievoorziening. Opgenomen in de Project start architectuur (Bijlage 8, PSA).
Eis 41.	Leverancier conformeert zich aan de Project Start Architectuur (PSA) van VISTA college. De PSA waarborgt dat nieuwe ontwikkelingen en veranderingen in samenhang worden gerealiseerd en passen binnen de huidige en toekomstige gewenste situatie. De PSA geeft de context en richting aan van de oplossing, maar niet de (detail)oplossing zelf. De PSA is een formeel onderdeel van de opdracht aan Leverancier. Daarmee geldt de PSA als kader voor scope, samenhang, randvoorwaarden en het projectplan.
Eis 42.	Indien het geheel of onderdelen van de aangeboden dienstverlening gedurende de contractperiode via de coöperatie SURF of het collectief (mbo, ho) overgezet kan worden, dan staat Leverancier dit toe. Hier worden nadere afspraken over gemaakt.
Eis 43.	Leverancier biedt voor de aangeboden applicatie een broncode-ESCROW en/of CloudESCROW regeling, welke is geregeld door Leverancier of een door Leverancier ondersteunde gebruikersgroep. Voor SaaS wordt een SaaS-escrow aangeboden, of vergelijkbaar, waar niet alleen de broncode(s) onder vallen maar ook de data van VISTA college.
Eis 44.	Onder koppelingen tussen voorzieningen wordt in dit Programma van Eisen verstaan: volledig geautomatiseerde, machine-leesbare interoperabiliteit tussen systemen, gebaseerd op open standaarden en gedocumenteerde interfaces (API's), zonder structurele handmatige tussenkomst. De beschreven geautomatiseerde koppelingen dienen uiterlijk gerealiseerd te zijn voordat beheer wordt overgedragen aan Opdrachtgever. Onder een interoperabiliteitsvoorziening wordt verstaan: • een technische voorziening (zoals een adapter, broker, service-laag, event-mechanisme of gestandaardiseerde uitwisselservice); • die werkt op basis van open standaarden en open specificaties; • die herbruikbaar, configureerbaar en gedocumenteerd is; • en die geen structurele handmatige handelingen vereist voor reguliere gegevensuitwisseling.

	Oplossingen waarbij gegevensuitwisseling structureel afhankelijk is van handmatige invoer, bestandsuitwisseling (zoals handmatige CSV-uploads), of gesloten, leveranciers specifieke koppelingen zonder open documentatie, worden niet beschouwd als geautomatiseerde koppelingen.
Eis 45.	Leverancier realiseert geautomatiseerde, machine-leesbare gegevensuitwisseling met de overeengekomen aanleverende en afnemende systemen binnen het VISTA-college-landschap, gebaseerd op open standaarden en gedocumenteerde interfaces (API's), zonder structurele handmatige tussenkomst. Indien voor het realiseren van een koppeling afhankelijkheid bestaat van een derde partij, verplicht Leverancier zich tot: • het actief initiëren en technisch faciliteren van de koppeling; • het tijdig afstemmen met de betreffenLeverancier; • het leveren van de benodigde documentatie, interfaces en ondersteuning. Indien een koppeling aantoonbaar niet gerealiseerd kan worden door beperkingen bij een derde partij, informeert Leverancier Opdrachtgever hierover tijdig en schriftelijk, inclusief: • een toelichting op de belemmering; • de ondernomen acties; • mogelijke alternatieve oplossingsrichtingen.
Eis 46.	VISTA college is een regieorganisatie (VISTA college voert regie over uitbestede diensten). Dit betekent dat: a. Leverancier applicatie- en technisch beheer uitvoert van de door hem geleverde SaaS-oplossing; b. functioneel beheer is belegd bij VISTA college, dat de regie voert richting eindgebruikers en interne processen; c. de SIAM-rol is belegd bij de huidige externe ICT-kennispartner van VISTA college onder verantwoordelijkheid van ICT Technisch Beheer; d. Leverancier zich conformeert aan deze structuur en rolverdeling en hierin actief samenwerkt met de door VISTA college aangewezen partijen.

Functionele eisen

Eis 47.	*Centraal identiteitenbeheer* De oplossing dient een centrale voorziening te bieden voor het beheren van digitale identiteiten van medewerkers, externen, gasten leveranciers, stagiairs en serviceaccounts.
Eis 48.	*Unieke identiteit* De oplossing dient iedere gebruiker te voorzien van een unieke digitale identiteit die gedurende de gehele levenscyclus te volgen is.
Eis 49.	*Ondersteuning hybride landschap* De oplossing dient identiteiten te kunnen beheren voor zowel cloud-, on-premises- als hybride omgevingen.
Eis 50.	*Meerdere bronsystemen* De oplossing dient meerdere gezaghebbende bronnen (HR-systeem, leveranciersportaal, studentenadministratie, etc.) te ondersteunen.
Eis 51.	*Geautomatiseerde instroom* De oplossing dient automatisch gebruikersaccounts aan te maken op basis van mutaties uit een bronsysteem.
Eis 52.	*Geautomatiseerde functiewijzigingen (doorstroom)* De oplossing dient wijzigingen in functies, rollen, organisatie-eenheden en locaties automatisch te verwerken.
Eis 53.	*Geautomatiseerde uitstroom* De oplossing dient accounts en autorisaties automatisch te intrekken bij uitdiensttreding of beëindiging van een contract.
Eis 54.	*Accountprovisioning* De oplossing dient geautomatiseerd accounts te kunnen aanmaken, wijzigen en verwijderen in gekoppelde doelsystemen.
Eis 55.	*Connectoren* De oplossing dient standaardconnectoren beschikbaar te hebben voor gangbare systemen zoals: • Microsoft Entra ID

	• Active Directory • Microsoft 365 • AFAS • Topdesk • Eduarte • Magister • Canvas • Xedule • Cardsonline De oplossing dient tevens ondersteuning te bieden aan in- en export van CSV, XML, JSON.
Eis 56.	*Role Based Access Control (RBAC)* De oplossing dient RBAC-functionaliteit te ondersteunen.
Eis 57.	*Attributen gebaseerde autorisatie* De oplossing dient Attribute Based Access Control (ABAC) te ondersteunen.
Eis 58.	*Rechtenbundeling* De oplossing dient autorisaties te kunnen groeperen in rollen en profielen.
Eis 59.	*Automatische roltoekenning* De oplossing dient rollen automatisch toe te kennen op basis van attributen zoals functie, afdeling, locatie en contracttype.
Eis 60.	*Self-serviceportaal* De oplossing dient een gebruikersportaal te bieden voor aanvragen van accounts en rechten.
Eis 61.	*Delegatie* De oplossing dient gebruikers en managers in staat te stellen bevoegdheden tijdelijk te delegeren.
Eis 62.	*Goedkeuringsworkflows* De oplossing dient configureerbare goedkeuringsworkflows te ondersteunen.
Eis 63.	*Hercertificatie van rechten* De oplossing moet periodieke beoordeling en hercertificering van toegewezen rechten en rollen ondersteunen.

Eisen m.b.t. security en privacy

Certificering, compliance en gegevensverwerking	
Eis 64.	Informatiebeveiligingscertificering – Leverancier moet aantoonbaar te beschikken over een geldig ISO 27001-certificaat of aantoonbaar gelijkwaardige certificering voor de aangeboden dienstverlening.
Eis 65.	Aanvullende assurance-verklaring – Leverancier moet periodiek een onafhankelijke assurance-verklaring (ISAE 3000, ISAE 3402 Type II, SOC 2 Type II of gelijkwaardig) beschikbaar stellen.
Eis 66.	AVG-conformiteit – De oplossing moet volledig te voldoen aan de vereisten van de Algemene Verordening Gegevensbescherming (AVG) en aanpalende Nederlandse wet- en regelgeving.
Eis 67.	Verwerkersovereenkomst – Leverancier moet bereid zijn een verwerkersovereenkomst te sluiten op basis van het model van VISTA college.
Eis 68.	Gegevensverwerking binnen EER – Persoonsgegevens moeten uitsluitend binnen de Europese Economische Ruimte (EER) worden verwerkt en opgeslagen, tenzij VISTA college vooraf schriftelijk toestemming verleent.
Eis 69.	Transparantie gegevenslocaties – Leverancier moet inzichtelijk maken in welke landen persoonsgegevens worden opgeslagen, verwerkt en geback-upt (in de verwerkersovereenkomst).
Logging, audit en monitoring	
Eis 70.	Logging van beveiligingsgebeurtenissen – De oplossing moet beveiligingsrelevante gebeurtenissen vastleggen, waaronder aanmeldingen, mislukte aanmeldingen, privilegewijzigingen, autorisatiemutaties en wijzigingen in configuraties.
Eis 71.	Bewaartermijn auditlogs – Audit- en beveiligingslogs dienen minimaal 12 maanden beschikbaar te blijven voor onderzoek, compliance en forensische doeleinden.
Eis 72.	Export van loggegevens – De oplossing moet loggegevens kunnen exporteren naar externe SIEM- of monitoringsoplossingen via standaardprotocollen of API's.

Authenticatie en toegangsbeveiliging	
Eis 73.	Multi-Factor Authenticatie – De oplossing moet MFA ondersteunen voor beheerders en eindgebruikers, inclusief integratie met Microsoft Entra ID.
Eis 74.	Voorwaardelijke toegang – De oplossing moet integratie met Conditional Access-voorzieningen van Microsoft Entra ID ondersteunen.
Eis 75.	Privileged Access Management – De oplossing moet onderscheid te maken tussen reguliere accounts en beheeraccounts en aanvullende beveiligingsmaatregelen voor beheeraccounts ondersteunen.
Eis 76.	Least Privilege-principe – De oplossing dient het least privilege-principe te ondersteunen, waarbij gebruikers uitsluitend de minimaal noodzakelijke rechten ontvangen.
Eis 77.	Segregation of Duties – De oplossing moet functiescheiding (Segregation of Duties) ondersteunen en conflicterende autorisaties inzichtelijk kunnen maken.
Eis 78.	Sterke authenticatieprotocollen – De oplossing moet moderne authenticatiemechanismen zoals FIDO2, passkeys en passwordless authenticatie ondersteunen.
Eis 79.	Wachtwoordbeleid – Als wachtwoorden worden gebruikt moet de oplossing configureerbare wachtwoordvereisten volgens actuele beveiligingsrichtlijnen ondersteunen.
Security incidenten en kwetsbaarhedenbeheer	
Eis 80.	Monitoring en detectie – De oplossing moet verdachte activiteiten kunnen detecteren en hierover signaleringen of notificaties genereren.
Eis 81.	Security Incident Management – Leverancier moet een formeel proces voor security-incidentmanagement hanteren en VISTA college onverwijld informeren over relevante beveiligingsincidenten.
Eis 82.	Meldplicht datalekken – Leverancier moet vermoede of daadwerkelijke datalekken zonder onredelijke vertraging en uiterlijk binnen 24 uur na constatering aan VISTA college melden.
Eis 83.	Kwetsbaarhedenbeheer – Leverancier moet een formeel vulnerability management-proces hanteren voor het identificeren, classificeren en verhelpen van kwetsbaarheden.
Eis 84.	Penetratietesten – Leverancier dient minimaal jaarlijks onafhankelijke penetratietesten uit te laten voeren en een managementsamenvatting van de resultaten beschikbaar stellen.
Security & Privacy by Design	
Eis 85.	Security by Design – De oplossing moet ontwikkeld zijn en beheerd worden volgens de principes van Security by Design en Secure Development Lifecycle.
Eis 86.	Privacy by Design en Privacy by Default – De oplossing dient Privacy by Design en Privacy by Default aantoonbaar te ondersteunen.
Eis 87.	Dataminimalisatie – De oplossing dient uitsluitend persoonsgegevens te verwerken die noodzakelijk zijn voor het uitvoeren van identiteits- en toegangsbeheerprocessen.
Eis 88.	Gegevensclassificatie – De oplossing dient ondersteuning te bieden voor classificatie en afscherming van gevoelige persoonsgegevens.
Eis 89.	Recht op inzage en verwijdering – De oplossing dient VISTA college te ondersteunen bij het uitvoeren van AVG-verzoeken, waaronder inzage-, correctie- en verwijderverzoeken.
Eis 90.	Bewaar- en verwijderbeleid – De oplossing dient configureerbare bewaartermijnen en geautomatiseerde verwijderprocessen voor persoonsgegevens te ondersteunen.
Eis 91.	Gegevensportabiliteit – Persoonsgegevens, configuraties, rollen, auditgegevens en koppelingen dienen bij beëindiging van de overeenkomst volledig exporteerbaar te zijn in een gangbaar formaat.
Technische beveiliging	
Eis 92.	Encryptiesleutelbeheer – Leverancier dient aantoonbaar veilige processen te hanteren voor beheer, opslag, rotatie en bescherming van cryptografische sleutels.
Eis 93.	Beveiliging van API's – Alle API's dienen beveiligd te zijn door middel van sterke authenticatie, autorisatie en versleutelde communicatie.
Eis 94.	Tenantisolatie – Bij een multi-tenant SaaS-oplossing dient logische scheiding van klantgegevens aantoonbaar gewaarborgd te zijn.
Eis 95.	Bescherming tegen brute-force-aanvallen – De oplossing dient bescherming te bieden tegen brute-force-, password spraying- en credential stuffing-aanvallen.
Continuïteit en encryptie	
Eis 96.	Ondersteuning onderwijscontinuïteit – De oplossing dient zodanig te zijn ingericht dat verstoringen in identiteits- en toegangsbeheer geen onevenredige impact hebben op onderwijs-, examen- en bedrijfsvoeringsprocessen van VISTA college.
Eis 97.	Encryptie van data in rust – De oplossing dient alle opgeslagen gegevens (data at rest), waaronder persoonsgegevens, identiteitsgegevens, autorisatiegegevens, auditlogs, configuratiegegevens en

	back-ups, versleuteld op te slaan met minimaal AES-256 of een aantoonbaar gelijkwaardig en industrieel geaccepteerd encryptiemechanisme. De encryptie dient standaard ingeschakeld te zijn en Leverancier dient aantoonbaar passende maatregelen te treffen voor het beheer, de bescherming en de periodieke rotatie van de gebruikte cryptografische sleutels.

Projectmatige eisen

Eis 98.	Opleverdatum en eindresultaat: Leverancier voert de implementatie zodanig uit dat de nieuwe IAM-voorziening uiterlijk 17 december 2027 volledig is ingericht, technisch gerealiseerd, getest, door VISTA college is geaccepteerd en operationeel in gebruik is. De voor de initiële vervanging benodigde processen, functionaliteiten, autorisaties en koppelingen functioneren op dat moment aantoonbaar conform de overeengekomen eisen. De werkzaamheden worden zodanig uitgevoerd dat T4E uitgefaseerd kan worden.
Eis 99.	Verantwoordelijkheid implementatie: Leverancier is verantwoordelijk voor de projectmatige regie, coördinatie en uitvoering van de implementatie van de aangeboden IAM-voorziening voor zover deze werkzaamheden onderdeel zijn van de opdracht. Hieronder vallen in ieder geval de projectleiding aan leverancierszijde, voorbereiding en informatieverzameling, functioneel en technisch ontwerp, inrichting en configuratie, realisatie van de IAM-zijde van koppelingen, het bepalen, overnemen, converteren en/of opnieuw inrichten van relevante gegevens, mappings, configuraties en technische instellingen die noodzakelijk zijn voor de werking van de nieuwe IAM-voorziening, testen en ketentesten, productieovergang, kennisoverdracht, overdracht naar de beheerorganisatie en ondersteuning tijdens de overeengekomen nazorgfase. Leverancier draagt zorg voor de onderlinge samenhang van deze werkzaamheden en maakt tijdig inzichtelijk welke informatie, expertise, capaciteit, werkzaamheden en besluitvorming vanuit VISTA college en betrokken derde partijen noodzakelijk zijn. Leverancier bepaalt vanuit zijn IAM- en productexpertise een passende implementatieaanpak en fasering waarmee het overeengekomen resultaat en de uiterste opleverdatum worden gerealiseerd.
Eis 100.	Technische regie: Leverancier voert de technische regie over de implementatie van de door hem aangeboden IAM-voorziening, waaronder de configuratie, technische inrichting, integraties en koppelingen. Leverancier maakt tijdig inzichtelijk welke technische activiteiten, afhankelijkheden, randvoorwaarden, informatie en besluiten noodzakelijk zijn om de voorziening werkend en beheersbaar op te leveren. VISTA college is niet verantwoordelijk voor het bepalen van de technische implementatieroute van de aangeboden oplossing.
Eis 101.	Implementatie- en veranderplan: Leverancier werkt het bij inschrijving in het kader van K2 ingediende en beoordeelde implementatie- en veranderplan, in overleg met VISTA college, uit tot een definitief implementatie- en veranderplan. Dit definitieve plan is uiterlijk drie (3) weken na definitieve gunning afgerond en vormt de basis voor de uitvoering van de initiële vervanging. Het plan bevat minimaal de projectopdracht en doelstelling; implementatieaanpak, projectactiviteiten, fasering en integrale planning inclusief mijlpalen en afhankelijkheden; projectgrenzen en randvoorwaarden; projectorganisatie met rollen, verantwoordelijkheden en taakverdeling tussen Leverancier, VISTA college en betrokken derde partijen; de benodigde inzet van VISTA college en Leverancier, gespecificeerd naar rol, expertise en verwachte inspanning; producten en diensten; kwaliteitsborging; communicatie-, overleg- en escalatiestructuur; risico- en issuemanagement inclusief beheersmaatregelen; de aanpak en planning voor de uitwerking, beoordeling en goedkeuring van het functioneel en technisch ontwerp; realisatie en testen van integraties en koppelingen; test- en acceptatieaanpak; productieovergang en terugval; uitfasering van T4E; opleidings-, trainings- en kennisoverdrachtsactiviteiten voor de relevante gebruikers- en beheerorganisatie; overdracht naar beheer en lijnorganisatie; en de inrichting van de nazorgfase. Als onderdeel van het plan wordt een oplever- en acceptatiematrix opgenomen waarin per belangrijk resultaat of product is vastgelegd wat wordt opgeleverd, welke acceptatiecriteria gelden, wie verantwoordelijk is voor beoordeling en op welk moment formele goedkeuring of acceptatie plaatsvindt. Voor zover van toepassing op de reguliere dienstverlening wordt tevens vastgelegd hoe de in K2 beschreven uitgangspunten voor exit en doorontwikkeling gedurende de contractperiode worden geborgd. Uit het definitieve plan blijkt aantoonbaar op welke wijze de IAM-voorziening uiterlijk 17 december 2027 volledig is ingericht en technisch gerealiseerd, getest, door VISTA college geaccepteerd, operationeel in gebruik is genomen en is overgedragen aan de beheerorganisatie, zodat T4E gecontroleerd kan worden uitgefaseerd.
Eis 102.	Integrale planning: Leverancier stelt als onderdeel van het project- en implementatieplan een integrale planning op en houdt deze gedurende de implementatie actueel. De planning bevat minimaal de door Leverancier gekozen fasering, activiteiten, resultaten, mijlpalen, afhankelijkheden,

	besluit- en acceptatiemomenten, realisatie en testen van koppelingen, productieovergang en het kritieke pad. Afwijkingen die gevolgen kunnen hebben voor de opleverdatum worden direct gemeld, inclusief impact en herstelmaatregelen.
Eis 103.	Projectorganisatie: Leverancier richt een projectorganisatie in met voldoende projectmatige, functionele en technische IAM-kennis en capaciteit. Binnen het implementatieteam is aantoonbare expertise aanwezig op het gebied van de aangeboden IAM-oplossing, provisioning en deprovisioning, autorisaties, integraties, gegevensverwerking, testen en productieovergangen. Leverancier benoemt één (1) projectleider die verantwoordelijk is voor de projectmatige aansturing en coördinatie van de implementatie aan leverancierszijde en die fungeert als centraal aanspreekpunt voor de projectleider van VISTA college. Leveranciersprojectleider draagt zorg voor voorbereiding en vastlegging van voortgang, besluiten, acties en escalaties aan leverancierszijde.
Eis 104.	Capaciteit en continuïteit: Leverancier waarborgt gedurende de volledige implementatie voldoende gekwalificeerde capaciteit. Kritieke werkzaamheden mogen niet zodanig afhankelijk zijn van één sleutelfunctionaris dat diens uitval de voortgang of kwaliteit van de implementatie in gevaar brengt. Vervangende medewerkers beschikken over aantoonbaar gelijkwaardige kennis en ervaring.
Eis 105.	Rollen en verantwoordelijkheden: Leverancier stelt in afstemming met VISTA college een RACI-matrix op waarin de verantwoordelijkheden voor minimaal ontwerp, inrichting, configuratie, koppelingen, testen, acceptatie, productieovergang, terugval, documentatie, kennisoverdracht en overdracht naar beheer worden vastgelegd. De RACI-matrix concretiseert de uitvoering, maar kan de verantwoordelijkheden zoals vastgelegd in de aanbestedingsstukken en overeenkomst niet wijzigen.
Eis 106.	Benodigde inzet VISTA college: Leverancier maakt tijdig inzichtelijk welke inzet van VISTA college en betrokken derde partijen noodzakelijk is voor de uitvoering van de implementatie. Hierbij wordt aangegeven welke rol of expertise, informatie, werkzaamheden of besluitvorming nodig is, wanneer deze nodig is en wat de verwachte inspanning is. De verwachte inzet wordt per fase of relevante periode zoveel mogelijk gekwantificeerd in uren of dagdelen per rol of expertise. De benodigde inzet wordt zodanig tijdig gemeld dat VISTA college deze redelijkerwijs kan organiseren.
Eis 107.	Validatie huidige IAM-situatie: VISTA college stelt de beschikbare informatie over de huidige IAM-situatie aan Leverancier beschikbaar. Leverancier valideert deze informatie voor zover noodzakelijk voor een correcte inrichting van de nieuwe voorziening en maakt tijdig inzichtelijk wanneer informatie ontbreekt, inconsistent is of nadere verduidelijking vereist. Leverancier geeft daarbij concreet aan welke aanvullende informatie of besluitvorming noodzakelijk is.
Eis 108.	Functioneel en technisch ontwerp: Leverancier stelt het functioneel en technisch ontwerp van de IAM-voorziening op en houdt deze gedurende de implementatie actueel. In het functioneel ontwerp wordt uitgewerkt hoe de overeengekomen IAM-processen, functionaliteiten, autorisaties en uitzonderingen worden gerealiseerd in de aangeboden voorziening. In het technisch ontwerp worden minimaal de technische architectuur, configuratie, gegevensverwerking, mappings, provisioning- en deprovisioninglogica, koppelingen en interfaces, foutafhandeling, logging en monitoring uitgewerkt. VISTA college levert de beschikbare functionele uitgangspunten, eisen en architectuurkaders en is verantwoordelijk voor de VISTA-specifieke besluitvorming. Het functioneel en technisch ontwerp worden voorafgaand aan de betreffende realisatie ter goedkeuring aan VISTA college voorgelegd. Goedkeuring door VISTA college laat de verantwoordelijkheid van Leverancier voor de juistheid en werking van het ontwerp en de gerealiseerde oplossing onverlet.
Eis 109.	Inrichtingsvraagstukken en besluitvorming: Leverancier identificeert tijdig de functionele en technische inrichtingsvraagstukken waarvoor besluitvorming van VISTA college noodzakelijk is. Leverancier beschrijft het vraagstuk, relevante oplossingsrichtingen en de consequenties voor werking, beheerbaarheid, koppelingen, continuïteit, planning en waar relevant kosten. Waar redelijkerwijs mogelijk geeft Leverancier vanuit zijn IAM- en productexpertise een onderbouwd advies. De uiteindelijke VISTA-specifieke besluitvorming blijft bij VISTA college.
Eis 110.	Initiële inrichting en configuratie: Leverancier is verantwoordelijk voor de correcte initiële configuratie en inrichting van de aangeboden IAM-voorziening voor zover deze onderdeel is van de opdracht. VISTA-beheerders kunnen hierbij actief worden betrokken voor validatie, kennisoverdracht en voorbereiding op het toekomstig beheer. Deze betrokkenheid wijzigt de verantwoordelijkheid van Leverancier voor een correcte initiële inrichting niet.
Eis 111.	Afhankelijkheden: Leverancier identificeert en beheert actief de technische en organisatorische afhankelijkheden die van invloed zijn op de implementatie. Hieronder vallen in ieder geval afhankelijkheden met VISTA college, infrastructuur, bron- en doelsystemen en derLeveranciers. Leverancier maakt tijdig inzichtelijk welke acties van andere partijen noodzakelijk zijn en welke gevolgen vertraging daarvan kan hebben voor planning, kwaliteit, continuïteit of kosten.
Eis 112.	Koppelingen en derde partijen: Leverancier is verantwoordelijk voor de werkzaamheden aan de IAM-zijde van de koppelingen die onderdeel zijn van de opdracht. Indien medewerking van VISTA college of derLeveranciers noodzakelijk is, levert Leverancier tijdig de benodigde technische specificaties, mappings, configuratie-informatie en testvoorwaarden en werkt actief samen met de betrokken partijen. Leverancier toont aantoonbaar aan dat de gerealiseerde IAM-koppelingen correct functioneren in samenhang met de betreffende bron- en doelsystemen.

Eis 113.	Risico- en issuemanagement: Leverancier houdt gedurende de implementatie een actueel risico- en issueregister bij. Per materieel risico of issue worden minimaal impact, eigenaar, beheers- of herstelmaatregel en status vastgelegd. Risico's en issues die invloed kunnen hebben op planning, technische werking, continuïteit, informatiebeveiliging, privacy, kwaliteit of kosten worden tijdig gemeld en waar nodig geëscaleerd.
Eis 114.	Voortgangsrapportage: Leverancier rapporteert minimaal tweewekelijks over de voortgang van de implementatie. De rapportage bevat minimaal de status van planning en mijlpalen, voortgang van inrichting en koppelingen, risico's en issues, afhankelijkheden, benodigde besluiten en afwijkingen ten opzichte van gemaakte afspraken. Materiële afwijkingen worden niet uitgesteld tot de eerstvolgende reguliere rapportage maar direct gemeld.
Eis 115.	Wijzigingsbeheer: Wijzigingen die gevolgen kunnen hebben voor scope, planning, kosten, kwaliteit, architectuur, informatiebeveiliging, privacy, technische werking, beheerbaarheid of continuïteit worden vooraf voorzien van een schriftelijke impactanalyse. Uitvoering vindt uitsluitend plaats nadat de wijziging via de overeengekomen besluitvormingsprocedure is goedgekeurd.
Eis 116.	Continuïteit tijdens implementatie: Leverancier voert de implementatie en overgang zodanig uit dat de continuïteit van het identiteits- en toegangsbeheer en de daarvan afhankelijke processen en systemen wordt geborgd. De huidige IAM-functionaliteit blijft beschikbaar totdat de betreffende functionaliteit aantoonbaar door de nieuwe voorziening kan worden overgenomen. Eventuele noodzakelijke onderbrekingen worden vooraf afgestemd en tot een minimum beperkt.
Eis 117.	Overgang en terugval: Leverancier stelt voorafgaand aan de productieovergang een overgangs- en terugvalplan op. Hierin worden minimaal de overgangsactiviteiten, technische volgorde, verantwoordelijkheden, afhankelijkheden, controles voor en na de overgang, go/no-go-criteria en objectieve criteria voor terugval beschreven. Tevens wordt vastgelegd hoe de continuïteit wordt geborgd wanneer de overgang niet succesvol verloopt.
Eis 118.	Gegevens-, configuratie- en inrichtingsovergang: Leverancier bepaalt in afstemming met VISTA college welke gegevens, mappings, configuraties, technische instellingen en overige relevante inrichting uit de huidige situatie moeten worden overgenomen, geconverteerd of opnieuw ingericht. Uitgangspunt is functionele continuïteit; een volledige één-op-één technische migratie van T4E is geen zelfstandig doel. Leverancier werkt hiervoor een passende aanpak uit en voert de werkzaamheden uit die tot zijn verantwoordelijkheid behoren.
Eis 119.	Testaanpak: Leverancier stelt een integraal testplan op dat aansluit bij het technische karakter en de ketenafhankelijkheden van de IAM-voorziening. Het testplan omvat voor zover relevant technische, functionele, koppeling-, provisioning-, autorisatie-, regressie- en ketentesten, inclusief testdata, testomgevingen, bevindingenprocedure en hertesten. Leverancier voert de testen uit die binnen zijn verantwoordelijkheid vallen en stelt de testresultaten en bewijsvoering beschikbaar aan VISTA college.
Eis 120.	Ketentesten: Leverancier werkt actief mee aan het end-to-end testen van de IAM-ketens en voert de werkzaamheden uit die binnen zijn verantwoordelijkheid vallen. Hierbij wordt aantoonbaar vastgesteld dat identiteit-, account-, rollen- en autorisatiegegevens vanaf de relevante bronsystemen via de IAM-voorziening correct worden verwerkt richting de aangesloten doelsystemen, inclusief relevante mutatie-, uitstroom- en uitzonderingssituaties.
Eis 121.	Acceptatie: VISTA college is verantwoordelijk voor de formele acceptatie van de IAM-voorziening. Leverancier ondersteunt de voorbereiding en uitvoering van de acceptatie en stelt hiervoor alle noodzakelijke testresultaten, technische bewijsvoering en documentatie beschikbaar. De voorziening wordt pas als geaccepteerd beschouwd nadat VISTA college dit formeel heeft bevestigd.
Eis 122.	Bevindingen en restpunten: Bevindingen uit de uitgevoerde testen worden geregistreerd, geclassificeerd, opgelost en waar nodig opnieuw getest. Op 17 december 2027 mogen geen openstaande bevindingen aanwezig zijn die de continuïteit, veiligheid, noodzakelijke functionaliteit, werking van kritieke koppelingen, formele acceptatie of beheerbaarheid van de voorziening belemmeren. Overige restpunten zijn alleen toegestaan na expliciete goedkeuring van VISTA college en worden voorzien van eigenaar, risico en afhandeldatum.
Eis 123.	Documentatie en kennisoverdracht: Leverancier levert actuele en volledige documentatie op die noodzakelijk is voor functioneel en technisch beheer en voor de continuïteit van de IAM-voorziening. Hieronder vallen voor zover relevant het functioneel en technisch ontwerp, configuraties, koppelingen, gegevensstromen en mappings, autorisaties, logging, monitoring, beheerprocedures en testdocumentatie. Leverancier verzorgt tevens de benodigde kennisoverdracht aan de door VISTA college aangewezen beheerders. Leverancier maakt tijdig inzichtelijk welke beheer-, service- of overige relevante rollen vóór ingebruikname moeten worden geïnstrueerd of opgeleid en verzorgt de hiervoor binnen de opdracht benodigde training en begeleiding.
Eis 124.	Overdracht naar beheer: Leverancier ondersteunt de formele overdracht van de IAM-voorziening naar de beheerorganisatie van VISTA college. Overdracht vindt plaats nadat de overeengekomen inrichting en testen zijn afgerond, de benodigde documentatie beschikbaar is, kennisoverdracht heeft plaatsgevonden en aan de overeengekomen acceptatiecriteria is voldaan. Eventuele geaccepteerde restpunten worden vóór overdracht vastgelegd.

Eis 125.	Projectafsluiting en decharge: Leverancier levert na acceptatie en overdracht een afsluitend opleverdossier op. Dit bevat minimaal een overzicht van de gerealiseerde resultaten, formele acceptaties, definitieve documentatie, geaccepteerde restpunten inclusief eigenaar en afhandeldatum, uitgevoerde kennisoverdracht en eventuele nog openstaande acties. Op basis hiervan kan VISTA college de implementatie formeel afsluiten en decharge verlenen.
Eis 126.	Uitfasering T4E: VISTA college is verantwoordelijk voor het formele besluit tot uitfasering van T4E. Leverancier voert alle tot zijn verantwoordelijkheid behorende werkzaamheden tijdig uit en verleent de noodzakelijke technische ondersteuning zodat T4E uiterlijk 17 december 2027 gecontroleerd kan worden uitgefaseerd. De nieuwe IAM-voorziening en de voor de initiële vervanging noodzakelijke koppelingen zijn daarom uiterlijk 17 december 2027 geaccepteerd en operationeel.
Eis 127.	Reguliere dienstverlening: Vanaf de operationele ingebruikname van de nieuwe IAM-voorziening is de overeengekomen SaaS-dienstverlening, inclusief de van toepassing zijnde SLA- en DAP-afspraken, volledig van toepassing. Fouten of tekortkomingen die aantoonbaar voortkomen uit de door Leverancier uitgevoerde implementatie, configuratie of gerealiseerde koppelingen en aan Leverancier zijn toe te rekenen, worden zonder aanvullende kosten hersteld.

Eisen m.b.t. service en dienstverlening

Eis 128.	Er dienen adequate overlegmomenten en escalatieniveaus te worden afgestemd en ingericht aangaande de beschikbaarheid, performance en ondersteuning van de SaaS-toepassing.
Eis 129.	*Service Level Agreement (SLA)* Leverancier levert en onderhoudt gedurende de contractperiode een Service Level Agreement (SLA), waarin de overeengekomen IAM/IGA-SaaS-dienstverlening, ondersteuning, prestaties, verantwoordelijkheden en kwaliteitsafspraken concreet, meetbaar en toetsbaar zijn vastgelegd. De SLA heeft betrekking op de zeven samenhangende onderdelen van de IAM/IGA-dienstverlening zoals beschreven in § 1.3.2 – Gewenste situatie en scope van Deel A – Beschrijvend document. De afspraken richten zich zowel op de beschikbaarheid en ondersteuning van de voorziening als op de aantoonbare werking van de overeengekomen dienstverlening binnen de IAM/IGA-keten. De SLA bevat minimaal de volgende onderdelen: 1. Documentbeheer: versiebeheer, documentstatus, eigenaarschap, vaststelling en wijzigingsbeheer. 2. Begrippen: eenduidige definities van dienstverlening, prestaties, servicevensters en relevante IAM/IGA-begrippen. 3. Doelstelling: borging van betrouwbare, veilige, beschikbare, beheerbare en toekomstbestendige IAM/IGA-dienstverlening. 4. Onderwerp van de overeenkomst: beschrijving en afbakening van de overeengekomen SaaS-dienstverlening, applicatieservices, applicatiecomponenten, koppelingen, beheer en ondersteuning. 5. Partijen, verklaring en ondertekening: contractpartijen, bevoegdheden, verantwoordelijkheden en formele vaststelling. 6. Aanvang en looptijd: ingangsdatum, dienstverlening vanaf ingebruikname, looptijd, wijzigingen en beëindiging. 7. Servicebeschrijving: beschrijving van de overeengekomen dienstverlening voor de zeven samenhangende IAM/IGA-onderdelen, inclusief de verantwoordelijkheidsverdeling binnen de keten. 8. Prestatieafspraken: afspraken over beschikbaarheid, monitoring, service- en onderhoudsvensters, ondersteuning, incidenten, prioritering, reactie- en hersteltijden, continuïteit, wijzigingen, releases, beveiliging, risicobeheersing en continue verbetering. 9. Prestatie-indicatoren en prestatienormen: meetbare afspraken, aansluitend op de zeven KPI-onderwerpen uit Bijlage 8 – PSA IAM-vervanging. Per indicator worden minimaal norm, meetwijze, meetperiode, verantwoordelijke, bewijsvoering en opvolging bij afwijkingen vastgelegd. 10. Rapportage, overleg en afstemming: periodieke rapportage over prestaties, ketenwerking, incidenten, beveiliging, risico's, wijzigingen en verbetermaatregelen, inclusief operationele, tactische en strategische afstemming. 11. Verantwoording en controle: aantoonbare naleving van afspraken, periodieke controles op toegangsrechten, logging, audits, architectuurtoetsing, continuïteitsbeproeving en opvolging van bevindingen.

	Borging: De SLA maakt onderscheid tussen beschikbaarheid van de SaaS-voorziening, beschikbaarheid van ondersteuning en calamiteitenafhandeling. De overeengekomen tijdvensters en prestaties sluiten aan op de continuïteitsbehoefte van onderwijs en bedrijfsvoering. De afspraken omvatten tevens de aantoonbare verwerking van wijzigingen in identiteiten en toegangsrechten, inclusief foutafhandeling en intrekking van rechten in aangesloten systemen, binnen de overeengekomen verantwoordelijkheden. De SLA wordt vóór ingebruikname van de betreffende dienstverlening door VISTA college beoordeeld en vastgesteld en blijft gedurende de contractperiode actueel. De aangeboden dienstverlening en ondersteuning sluiten aan op de eisen uit het PvE, de relevante architectuurkaders uit Bijlage 8 – PSA IAM-vervanging en de onder K1 – Dienstverlening en ondersteuning aangeboden en geaccepteerde kwaliteit.
Eis 130.	*Dossier Afspraken en Procedures (DAP)* Leverancier levert en onderhoudt gedurende de contractperiode een Dossier Afspraken en Procedures (DAP), waarin de operationele uitvoering van de overeengekomen IAM/IGA-SaaS-dienstverlening en ondersteuning is vastgelegd. Het DAP beschrijft hoe de afspraken uit de SLA worden uitgevoerd, bewaakt, gecontroleerd en verbeterd. Daarbij wordt rekening gehouden met de zeven samenhangende onderdelen van de IAM/IGA-dienstverlening, de verantwoordelijkheden van VISTA college en de afhankelijkheden van betrokken ketenpartners. Het DAP mag niet strijdig zijn met de SLA en mag de daarin overeengekomen verplichtingen en prestatienormen niet beperken. Het DAP bevat minimaal de volgende onderdelen: 1. Documentbeheer: versiebeheer, eigenaarschap, vaststelling, actualisatie en samenhang met de SLA. 2. Procesafspraken: afspraken over incidentmanagement, problem management, monitoring, IAM/IGA-verwerking, autorisatiebeheer, periodieke rechtencontrole, beveiliging, wijzigingen, continuïteit, ketenregie en continue verbetering. 3. Procedureafspraken: concrete werkwijzen voor meldingen, prioritering, escalatie, herstel, wijzigingen, foutafhandeling, beveiligingsincidenten, controles, attestatie waar van toepassing en overdracht. 4. Communicatielijnen: afspraken over meldpunten, bereikbaarheid, communicatie, terugkoppeling, escalatie en afstemming tussen leverancier, VISTA college en betrokken ketenpartners. 5. Taken, verantwoordelijkheden en bevoegdheden: concrete rol- en taakverdeling, inclusief mandaten, verantwoordelijkheden bij ketenverstoringen, de service delivery manager en de relevante beheer- en eigenaarsrollen. 6. Contactpersonen: actuele contactgegevens, escalatielijnen, bereikbaarheid en vervanging bij afwezigheid. 7. Rapportages: praktische uitvoering van SLA-rapportages, inclusief gegevensbronnen, registratie, meetmethoden, bewijsvoering, actiepunten en opvolging van afwijkingen. Borging: Het DAP beschrijft hoe Leverancier de overeengekomen dienstverlening en ondersteuning in samenhang met de IAM/IGA-keten organiseert, inclusief samenwerking met de beheerorganisatie van VISTA college en overige betrokken leveranciers. De proces- en procedureafspraken zijn concreet, uitvoerbaar en controleerbaar. Daarbij wordt vastgelegd hoe afwijkingen worden gesignaleerd, opgevolgd en aantoonbaar opgelost, binnen de overeengekomen taak- en verantwoordelijkheidsverdeling. Het DAP wordt vóór ingebruikname van de betreffende dienstverlening door VISTA college beoordeeld en vastgesteld en blijft gedurende de contractperiode actueel. De operationele inrichting sluit aan op de SLA, de eisen uit het PvE, de relevante architectuurkaders uit Bijlage 8 – PSA IAM-vervanging en de onder K1 – Dienstverlening en ondersteuning aangeboden en geaccepteerde kwaliteit.
Eis 131.	De SLA en DAP vormt een onlosmakelijk onderdeel van de definitieve overeenkomst.
Eis 132.	Na gunning zal zo spoedig mogelijk, uiterlijk 4 weken na gunning een DAP worden opgesteld.

Financiële eisen

Eis 133.	De GIBIT 2025 Inkoopvoorwaarden zijn van toepassing.
Eis 134.	De door Opdrachtgever te betalen facturen t.b.v. deze Overeenkomst zullen door Leverancier vooralsnog digitaal, zowel in PDF als .XML (PEPPOL), per mail worden verzonden aan crediteur@vistacollege.nl.
Eis 135.	Leverancier stelt de benodigde softwarelicenties gedurende de implementatie-, test- en acceptatiefase beschikbaar zonder aanvullende licentiekosten. De reguliere licentievergoeding gaat pas in na succesvolle acceptatie en schriftelijke goedkeuring van de productieve ingebruikname door VISTA college.
Eis 136.	Indien het aantal af te nemen licenties gedurende de looptijd van de Overeenkomst toeneemt of afneemt, wordt het gewijzigde aantal licenties afgerekend tegen hetzelfde stukstarief zoals opgenomen in het bij de Overeenkomst behorende Prijzenblad, met inachtneming van eventueel overeengekomen prijsindexeringen.
Eis 137.	Leverancier hanteert een betalingstermijn van dertig (30) dagen na de ontvangst van de factuur, tenzij anders overeengekomen in de Overeenkomst.
Eis 138.	Betaling door Opdrachtgever houdt op geen enkele wijze afstand van recht in.
Eis 139.	De factuur van Leverancier dient minimaal de volgende gegevens bevatten: • Crediteurnummer; • Inkooporderdernummer (indien bekend); • Contractnummer; • Factuurnummer; • Contactpersoon nadere opdracht; • KVK-nummer; • IBAN-nummer; • btw-nummer; • btw percentage; • btw bedrag; • Specificatie van de geleverde producten en diensten.
Eis 140.	Leverancier dient een transparante prijsstructuur te hanteren, zodat de maximale kosten voor licenties, beheer, onderhoud en eventuele groei van het aantal gebruikers vooraf zijn vastgesteld en beheersbaar blijven. Alleen per actieve gebruiker (licenties) worden geteld (betaald), 1e van de maand welke van toepassing is op de laatste kalendermaand. Er worden geen kosten in rekening gebracht m.b.t. inactieve gebruikers (geblokkeerd, beëindigd).
Eis 141.	De prijs van de standaard aangeboden functionaliteit dan wel door Leverancier getoond en/of toegezegd in de demonstratie of interview zijn verwerkt in het prijzenblad. Dit is inclusief de (beheer)kosten van eventueel minimaal maatwerk. De additionele opties die de aanbieder kan leveren richting het VISTA college en welke niet vallen onder de standaard ICT-dienstverlening worden benoemd in het prijzenblad.