Bijlage A2 – Programma van eisen Technische vereisten v2.0

Begrippenlijst (gehele PVE):

In dit document en de overige aanbestedingsstukken hebben de navolgende begrippen de volgende betekenis:

Begrip	**Betekenis**
Change managementproces	Gestructureerde aanpak om veranderingen binnen een organisatie, project of systeem effectief te beheren en implementeren.
DDOS-beveiliging	Maatregelen en technologieën die worden ingezet om het systeem te beschermen tegen cyberaanvallen.
Hosting	Provider beheert de technische aspecten zoals opslag, netwerkverbindingen en beveiliging, zodat gebruikers zonder eigen serverbeheer hun content kunnen publiceren.
Identify Access Management (IAM)	Framework van beleid, processen en technologieën die ervoor zorgen dat de juiste personen en systemen de juiste toegang hebben.
Inschrijver	Een geïnteresseerde die een inschrijving heeft ingediend.
LAS	Leerling administratiesysteem.
Opdrachtnemer	De inschrijver met wie de opdrachtgever de overeenkomst afsluit.
Logging	Verzameling van gebeurtenissen, activiteiten of berichten die binnen een systeem plaatsvinden.
LVS	Leerlingvolgsysteem.
Opdrachtgever	De opdrachtgever, in dit geval Stichting Lucas Onderwijs, die de overeenkomst aangaat met de opdrachtnemer.
Overeenkomst	De overeenkomst tussen de opdrachtgever en de opdrachtnemer voor het leveren van (een) product(en), de te verrichten werkzaamheden en/of het verlenen van een dienst, zoals beschreven in de aanbestedingsstukken.
Roadmap	Strategisch plan dat de stappen en mijlpalen beschrijft die nodig zijn om een doel te bereiken.
SaaS-applicatie	Cloud gebaseerde softwareoplossing die via het internet wordt geleverd en beheerd door een externe provider. Gebruikers hebben toegang tot de applicatie via een webbrowser, zonder dat ze software lokaal hoeven te installeren of infrastructuur hoeven te beheren.
Service Level Agreement (SLA)	Afspraken vanuit de opdrachtgever en Opdrachtnemer.
Systeem	Product van de Opdrachtnemer dat voldoet aan de eisen van las en las.

Minimumeis	
Eis nr.	**Categorie**
	Architectuur & Inrichting
1	De Opdrachtnemer voert het volledig technisch beheer uit op het aangeboden systeem.
2	Alle technische vereisten worden door de Opdrachtnemer gefaciliteerd (waaronder hosting).
3	Het LAS/LVS is een SaaS- applicatie. Voor optimaal gebruik van het LAS/LVS hoeven geen aparte add-ons of andere extra software geïnstalleerd te worden.
4	Het LAS/LVS dient als bronsysteem voor leerling en leerkracht identiteiten. Deze identiteiten moeten opgehaald worden door een externe IAM (Identify Access Management) zodat Opdrachtgever de leerlingen en leerkrachten kan voorzien van een ICT-account. Dit account wordt bijvoorbeeld gebruikt voor de toegang tot Microsoft 365 en Wifi netwerk van de vestiging.
5	Opdrachtnemer stelt jaarlijks in oktober de 'roadmap' voor het daaropvolgende jaar beschikbaar. Op deze manier krijgt de Opdrachtgever inzage in de ontwikkelingen die voor dat jaar op de agenda staan.
6	Het LAS/LVS is voor elke gebruiker device-onafhankelijk optimaal te gebruiken, zonder dat aparte add-ons of andere extra software geïnstalleerd hoeft te worden.
7	Het LAS/LVS is volledig web-based en browseronafhankelijk te gebruiken op devices draaiend op Windows 11 en hoger, OSX, iOS, Chrome OS en Android. De laatste twee versies van Edge, Firefox, Safari en Chrome dienen ondersteund te worden.
8	Alle data van opdrachtgever en of haar leerlingen die worden gegenereerd bij het gebruik van het LAS/LVS van Opdrachtnemer zijn eigendom van opdrachtgever en dienen derhalve te allen tijde ter beschikking te staan aan opdrachtgever. Opdrachtgever dient te allen tijde te beschikken over deze eigen data, ook in noodsituaties. Indien Opdrachtgever geen toegang meer heeft tot de eigen data in het LAS/LVS van Opdrachtnemer (bijvoorbeeld bij een cyberaanval) dient Opdrachtnemer op eerste verzoek van opdrachtgever de data aan te leveren.
9	Het systeem kan gebruik maken van de lokaal geïnstalleerde randapparatuur (waaronder printers en scanners) en vergt beperkte aanpassingen aan inrichting en configuratie.
	Security
10	De Opdrachtnemer voldoet aan ISO 27001.
11	Er wordt gewerkt met een DDOS-beveiliging, die wordt toegelicht in het SLA.
12	Er worden periodiek, op een secundaire locatie, back-ups gemaakt om de Opdrachtgever (in samenwerking met Opdrachtnemer in staat te stellen om data en systemen terug te zetten als hier aanleiding voor is.

13	Opdrachtnemer beschikt over een Business Continuity Plan (BCP), een escrow-overeenkomst of soortgelijke regeling om de impact van een grote verstoring te beperken. Dit plan wordt jaarlijks gecontroleerd door de opdrachtgever of het nog toereikend is.
14	Wachtwoorden worden one-way versleuteld opgeslagen.
15	Gebruikers kunnen inloggen met single sign-on waarmee toegang wordt verschaft tot de verschillende functionaliteiten en/of applicaties. Dit is onderworpen aan de IAM-oplossing van de Opdrachtgever.
16	Data wordt versleuteld opgeslagen.
17	Dataverkeer tussen (sub) Opdrachtnemers is versleuteld.
18	Opdrachtnemer overlegt jaarlijks een onafhankelijke assurance verklaring (ISAE type 2 of gelijkwaardig) over de werking van de overeengekomen beveiligingsmaatregelen. Non-compliance issues worden geïdentificeerd en gecommuniceerd, verbeteracties worden gedefinieerd en gemonitord. Inschrijver moet blijven voldoen aan de ISO27001 norm. Dit doet de inschrijver door a) na gunning een verklaring van toepasselijkheid te verstrekken en b) jaarlijks kosteloos een TPM af te geven.
19	Logbestanden dienen te worden beschermd tegen modificatie, inzien door onbevoegden en verwijdering. (Pogingen tot) Oneigenlijk wijzigen of verwijderen hiervan dient te worden gemeld als beveiligingsincident.
20	Logging moet op aanvraag beschikbaar worden gesteld ten behoeve van audits en onderzoek aan daartoe geautoriseerde personen.
21	Opdrachtnemer ziet 24/7 toe op mogelijke cyberaanvallen (bijvoorbeeld via SIEM/SOC).
22	Informatie over technische kwetsbaarheden (vulnerabilities) van informatiesystemen behoort tijdig te worden verkregen of gemeld. Zodat passende maatregelen kunnen worden genomen om het risico te verminderen.
23	Opdrachtnemer heeft een procedure met betrekking tot het melden van beveiligingsincidenten (in lijn met de Meldplicht datalekken).
24	Security updates van gebruikte systemen en applicaties dienen periodiek te worden geïnstalleerd. Daarbij moet worden voldaan aan de eisen van het Change Management proces.
Privacy	
25	Testactiviteiten worden uitsluitend uitgevoerd met geanonimiseerde testdata.
26	De Algemene Verordening Gegevensbescherming (AVG) is het uitgangspunt voor elke vorm van gegevensregistratie, -verwerking en –uitwisseling.

27	Opdrachtnemer dient met Opdrachtgever de verwerkersovereenkomst, die als offerte is bijgevoegd, te tekenen. Deze offerte heeft drie bijlagen.
28	Bij uitwisseling van gegevens wordt gegevensminimalisatie toegepast. Alleen gegevens die nodig zijn worden geleverd, proportioneel aan het doel van de uitwisseling.
29	Opdrachtnemer maakt alleen gebruik van in de EER gevestigde sub-verwerkers of van goedgekeurde verwerkers die voldoen aan de AVG of General Data Protection Regulation.
30	Het systeem maakt het mogelijk te voldoen aan uitvoering van de rechten van betrokkenen zoals inzage, recht op rectificatie en vergetelheid.
31	Wettelijke bewaartermijnen zijn per datagroep instelbaar. Verder moet het mogelijk zijn dat er verwijder-opdrachten worden gegeven om individuele gegevens of groepsgewijs te verwijderen.
32	Afspraken omtrent de verwerking van persoonsgegevens tussen opdrachtgever (verwerkingsverantwoordelijke) en Opdrachtnemer (verwerker) worden vastgelegd in een verwerkersovereenkomst conform de meest recente versie van het privacy convenant onderwijs.