

Bijlage D1

Programma van Eisen Sophia Scholen Europese Aanbesteding *ICT Beheer*

Sophia
Scholen
Duin- & Bollenstreek



Opdrachtgever:
Publicatiedatum:
Besteknummer:
Procedure:

Sophia Scholen
2024-ICTB-303786
Europees Openbaar

1. Huidige organisatie

De aanbestedende dienst probeert zoveel als mogelijk informatie te verstrekken op basis van de huidige en toekomstige situatie. Het is algemeen bekend dat dit bij ICT een flinke uitdaging is. De aanbestedende dienst heeft dan ook haar uiterste best gedaan om een goed beeld te geven van de werkelijkheid, maar de verstrekte informatie kan in de praktijk of ingehaald door de tijd, afwijken.

1.1 Huidige ICT Organisatie

De huidige ICT-organisatie bestaat uit diverse rollen met daarin de taken, verantwoordelijkheden en bevoegdheden. Hiervoor zijn de bestaande processen het uitgangspunt. Hoewel de verschillende rollen en processen beperkt beschreven zijn, kunnen we op hoofdlijnen de volgende rollen beschrijven:

Functie	Verantwoordelijke
College van Bestuur	Bestuurlijk verantwoordelijk voor de gehele organisatie.
Directeur centraal bureau	Belast met de dagelijkse aansturing van de gehele bedrijfsvoering van Sophia Scholen.
Bovenschoolse ICT coördinator	Belast met operationeel/tactisch advies, beleidsuitvoerende en coördinerende taken voor de ICT.
ICT-coördinatoren op scholen	Belast met beleidsmatige/operationele taken gericht op het onderwijsbeleid in combinatie met ICT.

Huidige leverancier

In de huidige situatie wordt er gebruik gemaakt van een Google omgeving en werken met G-Suite voor de leerlingen, de medewerkers werken met M365. De huidige ICT dienstverlener voor het beheer is Heutink ICT. Heutink ICT functioneert als SPOC (Single Point of Contact). De ICT hardware wordt geleverd door Heutink ICT via een separaat contract. De ICT Hardware wordt volledig werkend opgeleverd, hieronder wordt verstaan dat na levering geen aanvullende installaties nodig zijn om bestelde apparatuur werkend te krijgen en dat deze volledig en geautoriseerd toegang heeft tot de ICT-omgeving van Opdrachtgever en de ICT Beheerder. Het beheer van de hardware valt binnen de scope van deze aanbesteding.

De reden van de aanbesteding is een aflopend contract met de huidige leverancier. Sophia Scholen wil stabiliteit in haar ICT omgeving en een snelle oplossing als er problemen zijn. Samen met een externe leverancier wil Sophia Scholen de juiste voorwaarden creëren. Dit document geeft een weergave van de huidige en gewenste situatie.

Locatielijst

School	Adres	Postcode	Plaats
Basisschool De Avonturier	Jacoba van Beierenweg 53d	2215 KV	Voorhout
Basisschool De Buitenplaats	De Krogt 6	2361 GT	Warmond
Chr. Basisschool De Fontein	Willem de Rijkelaan 13	2181 TA	Hillegom
Chr. Basisschool De Lisbloem	Orion 2	2163 AJ	Lisse
Chr. Basisschool De Regenboog	Distelweg 60	2215 DZ	Voorhout
Chr. Basisschool Hoffenne	Invaltij 17	2201 WM	Noordwijk
De Nieuwe School	Geversstraat 1a	2211 HK	Noordwijkerhout
IKC Vossepark	Weerlaan 22	2181 HH	Hillegom
KC op Zee	Hoogwakersbosstraat 22	2202 SP	Noordwijk
Kindcentrum Andreas	Rembrandtlaan 14	2215 CK	Voorhout
Kindcentrum Het Sterrenwerk	Sint Anthoniuslaan 15	2171 EL	Sassenheim
Kindercampus Joseph	Achterweg 7-7a	2161 GA	Lisse
Montessorischool Noordwijk	Jan de Ridderstraat 6	2201 DN	Noordwijk
Nieuwe Boekhorst (toek. basisschool)	Bollendreef		Voorhout
Nieuwkomersschool De Wereld	Duin en Dal 1a	2211 JP	Noordwijkerhout
R.K. Basisschool De Bronckhorst	Bronckhorststraat 32	2201 KW	Noordwijk
R.K. Basisschool De Giraf	Guido Gezellelaan 3	2182 WB	Hillegom
R.K. Basisschool De Horizon	Mgr Bekkersstraat 1b	2223 AP	Katwijk
R.K. Basisschool De Klarinet	Handelsstraat 34-36	2162 AG	Lisse
R.K. Basisschool De Overplaats	Willibrorduslaan 71	2171 VB	Sassenheim
R.K. Basisschool De Prinsenhof	Langevelderweg 2	2211 AH	Noordwijkerhout
R.K. Basisschool De Schapendel	Stakman Bossestraat 73	2203 GH	Noordwijk
R.K. Basisschool De Springplank	Kagerplein 30	2172 EA	Sassenheim
R.K. Basisschool De Startbaan	Smirnovffstraat 15	2171 NZ	Sassenheim
R.K. Basisschool Emmaüs	Bonekruidstraat 11	2215 BG	Voorhout
R.K. Basisschool Johannes	Mariastraat 30	2181 CT	Hillegom
R.K. Basisschool St. Victor	Pilarenlaan 33	2211 LH	Noordwijkerhout
R.K. Basisschool St. Willibrord	Oranjelaan 96	2161 KH	Lisse
R.K. Brede School De Egelantier	Hafkenscheidtlaan 2	2191 BP	De Zilk
Bestuurskantoor	Leidsevaart 2	2215 RE	Voorhout

1.2 Processen

Voor de ondersteuning aan het onderwijs wordt er vanuit de Opdrachtgever gebruik gemaakt van de volgende processen:

Incidenten/meldingen

Incidenten/meldingen

Incidenten/meldingen worden op verschillende manier gemeld:

- Beheer: incidenten/meldingen op het gebied van beheer worden gemeld door de ICT coördinator van de desbetreffende locatie. Indien er sprake is van escalatie, verloopt dit via de bovenschoolse ICT coördinator.
- Hardware: incidenten/meldingen op het gebied van ICT Hardware worden gemeld door de ICT coördinator van de desbetreffende locatie bij de leverancier waar de hardware is aangekocht.
- Wifi: incidenten/meldingen aan het wifi netwerk worden gemeld door de ICT coördinator van de desbetreffende locatie. Indien er sprake is van escalatie, verloopt dit via de bovenschoolse ICT coördinator.
- Internet: incidenten/meldingen aan het internet worden gemeld door de ICT coördinator van de desbetreffende locatie. Indien er sprake is van escalatie, verloopt dit via de bovenschoolse ICT coördinator. Mocht de storing niet bij de ICT beheerder liggen dan wordt deze gemeld bij de internetprovider.
- Digiborden/touchscreens: incidenten/meldingen aan de digiborden/touchscreens worden gemeld bij de leverancier waar de digiborden/touchscreens zijn aangekocht.
- Printers (MFC): incidenten/meldingen aan de printers (MFC) worden gemeld bij de leverancier van de printers (MFC).
- Telefonie: incidenten/meldingen worden gemeld bij de leverancier van telefonie.

Beheer werkplekken

Beheer werkplekken

- Google:
De Google omgeving wordt beheerd door de huidige ICT beheerder. Deze wordt beheerd in Google omgeving (G-Suite).
Indien er nieuwe apparatuur wordt aangeschaft zorgt de ICT beheerder ervoor dat deze wordt opgeleverd in G-Suite. De Google licenties worden aangeschaft bij de aanschaf van een device.
De Google omgeving wordt technisch en functioneel beheerd door de huidige ICT-beheerder via Google G-Suite. Indien er nieuwe apparatuur wordt aangekocht, zorgt de ICT beheerder ervoor dat deze werkend wordt opgeleverd in G-Suite. Bij de aanschaf van nieuwe apparatuur zorgt de ICT-beheerder ervoor dat deze correct wordt geïntegreerd en werkend wordt opgeleverd binnen de Google G-Suite omgeving.
- Office 365:
Het volledige beheer van Office 365 licenties in combinatie met Apparaatbeheer valt onder de opdracht. Alle diensten worden beheerd via één centrale tenant. One Drive en Teams zijn in gebruik binnen de organisatie.

1.3 Infrastructuur

Netwerk

In de huidige situatie zijn er geen lokale servers aanwezig op de schoollocaties. Er wordt gewerkt vanuit de Cloud.

Applicaties Onderwijs

Er wordt in de huidige situatie zoveel mogelijk gebruik gemaakt van webbased applicaties. In de toekomst is ook de verwachting dat dit zo blijft.

Huidige verbindingen

Momenteel werkt Sophia Scholen als volgt qua verbinding:

- Firewall, 29 stuks.
- Switches 60 stuks, 30 POE switches en 100 Access Points.
- Het Wifi netwerk wordt beheerd door Heutink ICT, er wordt gewerkt met Ruckus wifi omgeving.

MFA en ATP (Defender) is ingericht en operationeel binnen de scholen van Sophia.

1.4 Omvang

Om u een inschatting te geven van de omvang van de ICT omgeving treft u in onderstaande overzichten de aantallen aan. De aantallen wijzigen voortdurend en u kunt hier geen rechten aan ontleen. De teldatum is 1 februari 2024

Aantal FTE en leerlingen:

	Aantal locaties	Aantal leerlingen	Aantal medewerkers
Sophia Scholen	28	6.700	800

Inschatting ten aanzien van aantal devices, teldatum 01-12-2024:

	Chromebooks	Windows devices	Apple (niet via Beheer)
Sophia Scholen	5.000	1.350	< 50

2. Gewenste situatie

Sophia Scholen heeft vijf kernwaarden, te weten; verwondering, vertrouwen, verbinding, duurzaamheid, eigenaarschap. Een stabiele, veilige en goed werkende ICT omgeving is onmisbaar om deze kernwaarden toe te passen.

Doelstellingen

Het uitgangspunt voor de gewenste situatie is het verder inrichten van onze ICT omgeving waarbij een stabiel en betrouwbaar ICT Beheer de primaire doelen van Sophia Scholen ondersteunt. Sophia Scholen heeft als primaire doelen om uitdagend en toekomstgericht onderwijs te verzorgen, dat inspeelt op individuele mogelijkheden en leerbehoeften. Sophia Scholen staat voor een veilige leer- en werkomgeving waar leerlingen en medewerkers zich optimaal kunnen ontplooiën.

- ✓ Het kunnen vertrouwen op een betrouwbare ICT omgeving

De leverancier zorgt voor een betrouwbare ICT omgeving waarbij de continuïteit en kwaliteit van het onderwijs geborgd is. Graag stelt Sophia Scholen vast wat zij van de leverancier mag verwachten gedurende het gehele proces van advies, opdracht, leveringen en service gedurende de gehele contractduur. De afspraken worden vastgelegd in een SLA.

- ✓ Het gebruik maken van expertise van de leverancier.

Sophia Scholen maakt graag gebruik van de expertise van de leverancier. Eerlijk en transparant advies op basis van kundigheid en met onderwijskundig inzicht. Continuïteit moet ook hier worden geborgd door een vaste contactpersoon met back-up.

- ✓ Het kunnen vertrouwen op een deskundige service/helpdesk.

Bij problemen bij het gebruik van de ICT omgeving dienen de medewerkers van Sophia Scholen te kunnen rekenen op snelle en duidelijke ondersteuning vanuit de leverancier. Wanneer er zich problemen voordoen welke niet eenvoudig op te lossen zijn, dient de leverancier een passende service te bieden. Sophia Scholen wenst in alle gevallen ontlast te worden en verwacht dat een verstoring van het onderwijsproces zich niet, of tenminste zo kort mogelijk, voordoet.

In de gewenste situatie is Sophia Scholen op zoek naar een Opdrachtnemer die bekend is binnen het onderwijs. Sophia Scholen wil het volledige beheer van haar ICT omgeving uitbesteden om zich zodoende te kunnen focussen op het onderwijs. Er wordt van de Opdrachtnemer gedurende het contract een proactieve en adviserende rol verwacht op het gebied van de ICT omgeving.

Scope van de aanbesteding

Om de inschrijvers een beeld te geven van de aanbesteding treft u in onderstaande opsomming de scope van de aanbesteding:

- Het bieden en beheren van een ICT totaaloplossing (zoals omschreven staat in de gewenste situatie) voor de onderwijs- en kantoorwerkplekken;
- Het beheren en onderhouden van de huidige en toekomstige infrastructuur (alle aangesloten apparatuur);
- Opdrachtgever hanteert een vervangingscyclus van al haar hardware. Huidige apparatuur varieert in leeftijd. De apparatuur die vervangen wordt door Opdrachtgever, wordt door de

Opdrachtnemer geconfigureerd en werkend opgeleverd in de omgeving van Opdrachtgever;

- Beheer, onderhoud en monitoring van de WAAS omgeving, rekening houdende met de huidige afschrijvingstermijnen;
- Het beheren en aanmaken van alle gebruikersaccounts;
- Het beheren, updaten en installeren van alle software;
- Het beheren van alle ICT hardware binnen de organisatie;
- Het beheren en onderhouden van de security en beveiliging;
- Het volledig en aantoonbaar voldoen aan de wettelijke eisen, te denken aan onder andere de AVG en het Normenkader;
- Het bieden van support en ondersteuning voor alle eindgebruikers van de Opdrachtgever;
- Het verhelpen van alle problemen en storingen, inclusief het beschikbaar stellen van een webbased helpdesk, logboek en een managementrapportage. Meldingen kunnen zowel telefonisch als via de e-mail gemeld worden. Bovendien is er een mogelijkheid dat leverancier een pc op afstand overneemt om werkzaamheden op afstand te verrichten;
- Het gevraagd en ongevraagd adviseren op alle onderdelen binnen de scope teneinde Opdrachtgever inzicht te geven in innovaties en mogelijke verbeteringen zodat de doelstellingen bereikt kunnen worden.

Buiten de scope:

- Aanschaf Telefonie;
- Printers (MFC)
- Beheer van Sharepoint;
- Aanschaf ICT Hardware;
- Aanschaf Touchscreens;
- Het uitvoeren en beheren van back up.

2.1 Professionele regie-organisatie

Om toekomstbestendig en slagvaardig aan de slag te kunnen met ICT voor Sophia Scholen is een stabiele ICT-organisatie noodzakelijk. Er worden drie niveaus van aansturing onderscheiden:

- Strategisch/richten
- Tactisch/inrichten
- Operationeel/verrichten

We gaan uit van outsourcing/tasking van ICT-diensten. Een ontwikkeling die meer focus vraagt op de beschikbaarheid van die diensten dan op het operationeel beheer ervan en daarmee op zowel vraag- als aanbodmanagement. De kern hiervan is de optimale aansluiting van de ICT-ondersteuning op de strategische, tactische en operationele behoeften van Sophia Scholen.

De ICT-regie is voor de afstemming van vraag en aanbod binnen de kaders van beleid en strategie van onze organisatie. Hierbij gaat het enerzijds om bundelen van vraag naar ICT-diensten vanuit de organisatie, anderzijds controleren van het daarop afgestemde aanbod van ICT-diensten.

2.2 Beheer- en ontwikkelprocessen volgens standaards

ICT is geen doel op zich. De primaire processen, zoals het verzorgen van onderwijs, van Sophia Scholen zijn leidend voor de wijze waarop we de ICT-processen vormgeven. Gebruikers gaan er tegenwoordig vanuit dat de ICT gewoon werkt en dat de ICT toegevoegde waarde levert. We willen voorkomen dat we met zware processen de ICT-organisatie onnodig belasten, maar we onderkennen dat we hiervoor een set aan beheer- en ontwikkelprocessen moeten inrichten. Aangezien de voorgestelde strategie is om op basis van regie extern ICT-diensten in te kopen, zullen de interne processen beperkt zijn.

Moderne infrastructuur vormt de basis

Onze ambities op het gebied van ICT kunnen we alleen realiseren als we onze infrastructuur moderniseren. Dit vormt de technische basis. Deze doelstelling kan worden gerealiseerd door het totale beheer en onderhoud van de ICT-omgeving onder te brengen bij een externe partij. Deze zal het eerste aanspreekpunt zijn voor Sophia Scholen en deze ontzorgen op ICT gebied. Voor de oplossingen die zij zelf niet kunnen leveren mag de leverancier oplossingen bij andere partijen inkopen waarbij Opdrachtnemer primair verantwoordelijk blijft.

Digitale Leer-en werkomgeving (DLWO)

Sophia Scholen maakt gebruik van een Digitale Leer-en Werkomgeving. Er moet voor de gebruiker één systeem zijn waar, door middel van inlog, bepaald wordt welke functionaliteiten aangeboden worden. Indien een gebruiker meerdere rollen heeft binnen de organisatie worden, op basis van één account, alle benodigde functionaliteiten integraal geboden. De aangeboden DLWO dient binnen de prijs te zijn inbegrepen.

Servicedesk

Opdrachtnemer maakt gebruik van gestandaardiseerde procedures voor het afhandelen van incidenten, problemen en wijzigingen zoals bijvoorbeeld ASL en ITIL. Sophia Scholen wil kunnen vertrouwen op een deskundige servicedesk. De Opdrachtnemer is bekend met het onderwijs en is dan ook bereikbaar vanaf 7:30 tot 17:00 uur, zodra de scholen opstarten. Er moet middels een ticket systeem of telefonisch een melding kunnen worden gemaakt bij de Opdrachtnemer. Alle meldingen worden geregistreerd in een ticketsysteem. De bovenschoolse ICT coördinator kan real-time inzicht krijgen in het aantal service meldingen.

On site support en ondersteuning

Voor de dagelijkse servicemeldingen wordt geen on site support verwacht.

ICT hardware

Sophia Scholen faciliteert de hardware en is eigenaar van de hardware. De ICT hardware wordt opnieuw aanbesteed. Indien er behoefte is aan ICT Hardware wordt deze afgenomen binnen deze nieuw te sluiten overeenkomst.

De ICT Hardware dient door de Opdrachtnemer van het ICT beheer volledig werkend en gebruiksklaar te worden opgeleverd. Onder gebruiksklaar wordt het volgende verstaan: operationeel gebruiksklaar geleverd, in de ICT school omgeving, inzetbaar/bruikbaar voor het doel waar het voor bedoeld is. Volledig werkend en gebruiksklaar geleverd, impliceert ook dat er geen aanvullende installaties nodig zijn om bestelde apparatuur werkend te krijgen en dat deze volledig en geautoriseerd toegang heeft tot de ICT omgeving van de Opdrachtgever en de ICT beheerder. In het prijzenblad Bijlage D kan er per device een prijs opgegeven worden voor deze dienstverlening.

Wifi netwerk

Het beheer van het huidige Wifi netwerk dient te worden uitgevoerd door de Opdrachtnemer. Bij de inschrijving dient de Opdrachtnemer rekening te houden met de niet overdraagbaarheid van de licenties op de Wifi apparatuur.

Security en beveiliging

Sophia Scholen wenst een ervaren en betrouwbare leverancier te selecteren voor het leveren van ICT-beheer met betrekking tot de inrichting van beveiliging en security. Het doel is om een robuust en effectief beveiligingssysteem te implementeren dat de vertrouwelijkheid, integriteit en beschikbaarheid van de ICT-infrastructuur en gegevens van de onderwijsinstelling waarborgt. Het is aan de inschrijver om passende, toekomstgerichte oplossingen aan te blijven bieden conform de geldende wet- en regelgeving.

Samengevat

Van de Opdrachtnemer (externe partij) wordt verwacht dat hij het ICT beheer voor de aanbestedende dienst uitvoert, voor nu en in de toekomst. Onder ICT beheer wordt hier verstaan alle activiteiten die vallen onder systeembeheer, configuratiebeheer, asset management en netwerkbeheer. Het beheer omvat de volledige installed base van de aanbestedende dienst, dus onder andere alle (huidige en toekomstige) hardware componenten zijnde werkstations (desktops en laptops) en devices, alle aanwezige switches, touchscreens, routers, printers (MFC), Wifi-stations e.d. en te gebruiken software zijnde besturingssystemen, kantoorapplicaties, onderwijsapplicaties e.d. inclusief de door Opdrachtnemer te leveren en te beheren beveiligingssoftware o.a. (anti-virus).

2.3 Software

De functionaliteit om processen te ondersteunen wordt voornamelijk door middel van software geleverd. Hiervoor zijn softwarepakketten (applicaties) nodig.

Educatieve software

De educatieve software is waar mogelijk webbased en gekoppeld met het leerlingvolgsysteem, zodat er zo min mogelijk tijd verloren gaat aan het beheer van gebruikers. Single sign on functionaliteit moet, waar mogelijk, het gebruiksgemak vergroten voor de eindgebruiker bij het benaderen van de diverse soorten applicaties en diensten via de verschillende gebruikte besturingssystemen. Er dient een koppeling te komen met basispoort. Een koppelingsmogelijkheid met G Suite + Office 365 is een basisvereiste.

Scholen geven zelf aan welke educatieve software ze in combinatie met de gebruikte methode nodig hebben. Indien wenselijk worden de softwarelicenties breed ingekocht door Sophia Scholen.

Licenties

De licenties die noodzakelijk zijn voor rechtmatig gebruik van besturings- en kantoorapplicaties worden centraal geregeld. Hiervoor zijn via APS-diensten contracten afgesloten voor Microsoft desktop- server en Office 365 pakket. Er worden Microsoft Education licenties afgenomen. Leverancier is verantwoordelijk voor het leveren en beheren, up-to-date houden van beveiligingssoftware, waaronder antivirus en back-up. De leverancier is tevens verantwoordelijk voor het (pro)actief monitoren van de netwerken. Dit alles volgens de wettelijke eisen, te denken aan onder andere de AVG en het Normenkader.



Bijlage D1: Programma van eisen ICT Beheer

1	Algemene eisen
1.1	Opdrachtnemer draagt zorg voor één centraal contactpersoon voor Opdrachtgever + back up.
1.2	Indien medewerkers in contact komen met leerlingen op de scholen geldt: De medewerkers van de Opdrachtnemer dienen in het bezit te zijn van een Verklaring Omtrent Gedrag (VOG). Op verzoek van de Opdrachtgever dient de Opdrachtnemer deze aan te vragen, waarbij de kosten voor rekening van de Opdrachtnemer komen. Op aanvraag kan de Opdrachtgever inzage krijgen in de VOG. Indien dergelijke verklaringen niet kunnen worden overlegd, wordt de betreffende medewerker direct de toegang tot de locatie van de Opdrachtgever onttrokken.
1.3	De Opdrachtnemer zal, op zowel gevraagd als ongevraagd verzoek, advies verstrekken met betrekking tot alle aspecten binnen de scope. Dit met als doel de Opdrachtgever inzicht te verschaffen in innovaties en mogelijke verbeteringen, waardoor de gestelde doelstellingen op een efficiëntere wijze kunnen worden behaald.
1.4	De gegevens in zowel de huidige als de gewenste omgeving blijven eigendom van de Opdrachtgever. De toegepaste instellingen dienen transparant te zijn en eenvoudig overdraagbaar naar een andere beheerder.
1.5	Opdrachtnemer voorziet in een gebruikersinterface in de Nederlandse taal.
1.6	Gedurende het gehele eerste jaar van deze overeenkomst zullen géén prijswijzigingen worden doorgevoerd. Na het eerste jaar van de overeenkomst zal er per 1 juni 2026 een prijswijziging kunnen worden doorgevoerd voor dat komende jaar. Een prijswijziging zal nimmer met terugwerkende kracht gebeuren.
1.7	Prijswijzigingen dienen uiterlijk twee maanden voor het verstrijken van het kalenderjaar te worden aangedragen door Opdrachtnemer ter acceptatie op basis van maximaal het CBS-prijsindexcijfer CAO lonen per uur inclusief bijzondere beloningen, categorie zakelijke dienstverlening, waarbij het prijsniveau staat voor 2024 en gelijk is aan 100. Opdrachtnemer stelt de prijswijziging vast op basis van het prijsindexcijfer en meldt dit schriftelijk bij Opdrachtgever.
2	Infrastructuur/netwerk
2.1	Opdrachtnemer is belast met de volledige uitvoering en verantwoordelijkheid van het IT-beheer, waarbij alle activiteiten die onder systeembeheer en configuratiebeheer vallen, inbegrepen zijn.
2.2	Opdrachtnemer draagt de verantwoordelijkheid voor het beheren van de volledige huidige en toekomstige installed base van Opdrachtgever, zoals beschreven in eis 3.1 tot en met 3.8. Hieronder vallen onder andere, maar niet beperkt tot: printers (MFC), inclusief onderhoud van adresboeken), werkstations (desktops en laptops), devices, switches, touchscreens, routers, software (besturingssystemen, kantoor- en onderwijsapplicaties) en beveiligingssoftware (anti-virus).
2.3	Opdrachtnemer neemt het beheer van alle bestaande systemen over.
2.4	Opdrachtnemer installeert geen servers (data- print of mailservers) op de locaties van Opdrachtgever.
2.5	Opdrachtnemer garandeert dat de aangeboden oplossing kan samenwerken met de huidige en toekomstige software.
3	Beheer
3.1	Asset management: Opdrachtnemer is verantwoordelijk voor het complete proces van aanschaf tot afschrijving van IT-middelen van Opdrachtgever. Opdrachtnemer voert activiteiten uit die leiden tot een adequaat administratief beheersproces van IT-



	middelen. Opdrachtnemer registreert alle aanwezige devices (inclusief kenmerken) van de Opdrachtgever en maakt dit inzichtelijk voor Opdrachtgever. Opdrachtgever kan te allen tijde periodiek (nader af te stemmen) een rapportage opvragen zonder bijkomende kosten.
3.2	Configuratie management: Het beheren van programmastuursystemen (software) en apparatuur door middel van een speciaal informatiesysteem als gereedschap (tool) om wijzigingen (change) te controleren en beheersen en de integriteit van het systeem te waarborgen.
3.3	Change management: Opdrachtnemer maakt gebruik van gestandaardiseerde methoden en procedures om wijzigingen (changes) te kunnen afhandelen, waarbij het onderwijsproces zo min mogelijk wordt onderbroken.
3.4	Incident management: Opdrachtnemer hanteert incident management als proces, waarbij het doel is om een incident terug te brengen naar het normale en overeengekomen kwaliteitsniveau.
3.5	Probleem management: Opdrachtnemer is verantwoordelijk voor het volledige proces van het afhandelen van problemen, met als doel storingen en incidenten proactief te verminderen. Hierbij neemt Opdrachtnemer ook de verantwoordelijkheid voor het proactief monitoren van de gehele IT-omgeving.
3.6	Release management: Opdrachtnemer is verantwoordelijk voor het plannen en toezicht houden op de uitrol van nieuwe releases voor hard- en software. De planning wordt te allen tijde voorgelegd aan de Opdrachtgever.
3.7	Capaciteitsmanagement: Opdrachtnemer is verantwoordelijk voor het waarborgen van de juiste capaciteit voor alle IT-middelen om te kunnen voldoen aan de huidige en toekomstige behoeften van Opdrachtgever.
3.8	Actieve monitoring wifi-omgeving en firewalls zijn onderdeel van de beheer opdracht.
4	Toegang en beveiliging
4.1	Opdrachtnemer beheert alle accounts van medewerkers en leerlingen.
4.2	Opdrachtgever doet een verzoek tot het aanmaken van een nieuwe gebruikersaccount. Opdrachtnemer maakt nieuwe accounts aan en koppelt de gewenste rollen en rechten in de Microsoft-omgeving, Basispoort en Leerlingdashboard.
4.3	Opdrachtnemer beschikt over een automatische koppeling met Basispoort dat is gekoppeld aan het leerlingvolgsysteem (LVS) van Opdrachtgever om automatisch (leerling) accounts aan te maken en te blokkeren.
4.4	De Opdrachtnemer zorgt ervoor dat haar eigen producten en diensten voldoen aan het Normenkader (IBP) voor informatiebeveiliging en privacy. Opdrachtnemer zal, gevraagd en ongevraagd, adviseren op alle onderdelen binnen het Normenkader (IBP).
4.5	Opdrachtnemer is verantwoordelijk voor het leveren, installeren, configureren, beheren en up-to-date houden van beveiligingssoftware, waaronder, maar niet beperkt tot: anti-virus. Het doel van de Aanbestedende Dienst is ervoor te zorgen dat zij beschikt over een veilige IT-omgeving. Opdrachtnemer biedt hier een passende oplossing voor, conform de geldende wet- en regelgeving.
4.6	Opdrachtnemer is verantwoordelijk voor het correct en consequent volgen van de Algemene Verordening Gegevensbescherming (AVG) en toekomstige wettelijke opvolgers. Hierbij wordt voldaan aan alle wettelijke IT-beveiligings- en regelgeving.
4.7	Opdrachtnemer beschikt over een ISO 27001 informatiebeveiligingscertificering of vergelijkbaar.
4.8	Opdrachtnemer is verantwoordelijk voor het firewall beheer.
4.9	Opdrachtnemer mag bemiddelen in de levering van licenties (hardware en software). In dat geval draagt Opdrachtnemer zorg voor een correcte tenaamstelling van de



	software, waarbij de software altijd wordt tenaamgesteld op naam van Opdrachtgever.
4.10	Opdrachtnemer realiseert en beheert een storingsvrije toegang naar alle software gedurende alle lesdagen van de Opdrachtgever.
4.11	Opdrachtnemer is verantwoordelijk voor het installeren, configureren, beheren en up-to-date houden van alle software en besturingssoftware.
4.12	De Opdrachtnemer dient expertise te hebben op het gebied van beveiliging en security van ICT-systemen, met aantoonbare ervaring in het werken met onderwijsinstellingen.
4.13	Het beveiligingssysteem dient te voldoen aan internationale best practices en relevante wet- en regelgeving met betrekking tot informatiebeveiliging.
4.14	De aangeboden ICT-omgeving dient maximale bescherming te bieden tegen bekende en opkomende bedreigingen, zoals malware, ransomware, phishing en DDoS-aanvallen. Hierbij is het essentieel dat de Opdrachtnemer expertise kan aantonen in het implementeren van effectieve beveiligingsmaatregelen.
4.15	Er dient een geïntegreerd authenticatie- en autorisatiesysteem te zijn om de toegang tot systemen en gegevens te beheren. Dit systeem moet sterke wachtwoordbeleidsregels omvatten en de mogelijkheid bieden voor tweefactorauthenticatie.
4.16	Er moet continue, 24/7 monitoring zijn van de beveiligingssystemen en het netwerk, met inbegrip van logboekregistratie en analyse. In geval van verstoring wordt de Opdrachtgever direct geïnformeerd.
5	Servicedesk beschikbaarheid en bereikbaarheid
5.1	De Opdrachtnemer vervult de SPOC-rol en moet snel, efficiënt en proactief reageren op alle vragen, incidenten en verzoeken van Opdrachtgever met betrekking tot de ICT. Indien nodig wordt er met derden geschakeld. De Opdrachtnemer fungeert als probleemhouder en neemt verantwoordelijkheid voor het oplossen van de gemelde problemen, waarbij heldere communicatie en een minimale impact op het onderwijsproces centraal staan.
5.2	Opdrachtnemer voorziet in een webbased platform waarop Opdrachtgever incidenten, problemen en wijzigingen kan melden. Op elk moment heeft de Opdrachtgever zicht op de status, doorlooptijd en genomen acties met betrekking tot het oplossen van gemelde incidenten, problemen of wijzigingen. Afmelding van deze gemelde zaken gebeurt te allen tijde door de Opdrachtgever/melder.
5.3	Opdrachtnemer hanteert gestandaardiseerde procedures, zoals ASL en ITIL, voor de afhandeling van incidenten, problemen en wijzigingen.
5.4	De servicedesk ondersteuning is beschikbaar in de Nederlandse taal.
5.5	De servicedesk van de Opdrachtnemer is beschikbaar voor Opdrachtgever op werkdagen (maandag t/m vrijdag) van 07:30 uur tot 17:00 uur.
5.6	Opdrachtnemer dient voorafgaand aan elk kalenderjaar een planning van preventieve onderhoudswerkzaamheden te overleggen en te leveren aan Opdrachtgever.
5.7	Opdrachtnemer plant in overleg met Opdrachtgever correctieve onderhoudswerkzaamheden zo spoedig mogelijk in.
5.8	Indien een storing/melding niet onder de verantwoording valt van Opdrachtnemer dan dient dit vooraf gecommuniceerd te worden met Opdrachtgever.
5.9	Opdrachtnemer overlegt een volledige SLA en DAP nadat de voorlopige gunning is ontvangen. In de SLA worden verschillende onderwerpen beschreven, waaronder maar niet beperkt tot: responstijden, escalatieafhandeling, overlegstructuur, beveiligingsbeheer, callintake, changemanagement, configuratiemanagement, releasemanagement, capaciteits- en performancemanagement, en back-up en recovery. Deze SLA en DAP maken integraal deel uit van de overeenkomst en bevatten



	de minimale eisen zoals vermeld in de conceptovereenkomst en de KPI's (Key Performance Indicators) zoals gesteld in de inschrijving.
5.10	Opdrachtnemer biedt, indien de storing niet op afstand (remote) opgelost kan worden, on site support aan.
6	Migratie
6.1	Opdrachtnemer is verantwoordelijk voor de gehele migratiefase inclusief een voorbereidende training voor alle medewerkers waarbij ze leren hoe de omgeving werkt.
6.2	Opdrachtnemer stelt altijd in overleg met Opdrachtgever een migratie/overgangsdatum vast. Opdrachtgever geeft hier een schriftelijk akkoord voor.
6.3	De migratie wordt uitgevoerd en gepland in overleg met de Opdrachtgever.
6.4	Bij iedere (deel) migratie geeft Opdrachtgever een Go/No Go. In het geval van een No Go beslissing worden de extra kosten niet vergoed door Opdrachtgever. Indien een no go beslissing door een derde partij wordt veroorzaakt is Opdrachtnemer niet verantwoordelijk.
6.5	Nazorg is onderdeel van de migratie en wordt niet apart doorbelast aan Opdrachtgever. In de nazorg fase wordt er ook een evaluatiegesprek met Opdrachtgever gehouden. Een basis training is onderdeel van de nazorg fase en dient binnen de migratiekosten zijn inbegrepen.
7	Rapportage en communicatie
7.1	Opdrachtnemer en Opdrachtgever evalueren half jaarlijks de IT-dienstverlening. Opdrachtnemer is verantwoordelijk voor het organiseren van dit half jaarlijkse overleg, waarbij Opdrachtgever wordt ondersteund door Alpha Adviesbureau.
7.2	Opdrachtnemer rapporteert periodiek (minimaal 1 keer per kwartaal) over de resultaten van de servicedesk, conform de SLA. Op verzoek van Opdrachtgever overlegt Opdrachtnemer te allen tijde.
7.3	Op verzoek van Opdrachtgever overlegt Opdrachtnemer te allen tijde informatie/rapportages zoals in eis 7.2 is omschreven.
8	Exit plan
8.1	Op verzoek van Opdrachtgever zullen Partijen binnen 3 maanden of, indien dit op kortere termijn is, voor het einde van de Overeenkomst, gezamenlijk een Exit Plan opstellen. Opdrachtnemer zal alle medewerking verlenen die nodig is bij het invullen van dit Exit Plan. Het exit plan is minimaal 1 maand voor de einddatum gereed.
8.2	Het Exit Plan bewerkstelligt de volledige migratie en/of overstap van de Diensten naar een nieuwe door Opdrachtgever gekozen dienstverlener. Alle werkzaamheden in verband met de migratie en/of overstap zullen geschieden tegen de standaardtarieven van Opdrachtnemer. Partijen zullen ieder de eigen kosten dragen voor het opstellen en bijhouden van het Exit Plan.
8.3	Het Exit Plan bevat in elk geval een volledige omschrijving van: (i) de taken die Opdrachtnemer op zich zal nemen in verband met de overdracht van de Diensten en overige informatie; (ii) de samenwerking tussen Opdrachtnemer enerzijds en Opdrachtgever of een door Opdrachtgever aangestelde derde anderzijds; (iii) het elektronische formaat waarin de relevante informatie ter beschikking zal worden gesteld (waaronder configuraties, Documentatie en codes).
8.4	Tot aan de einddatum voor de Diensten, zoals bepaald in de Overeenkomst, door welke vorm van beëindiging dan ook, blijft Opdrachtnemer volledig verantwoordelijk voor een volledige, tijdige en juiste uitvoering van de Diensten.
9	Digitale Leerweg Omgeving (DLWO)
9.1	De Opdrachtnemer biedt een DLWO aan. Deze maakt onderdeel uit van de inschrijving en zit binnen de prijs per medewerker/leerling inbegrepen.

9.2	De DLWO moet intuïtief en gebruiksvriendelijk zijn voor zowel docenten als leerlingen.
9.3	De DLWO moet toegankelijk zijn op verschillende apparaten i.c.m. een Office365, Apple of Google account.
9.4	De Digitale Leerweg omgeving op school biedt een veilige omgeving voor alle leerlingen.
9.5	De Digitale Leerweg omgeving bevat een aanpasbare contentfilter
9.6	Door middel van bijvoorbeeld adresboekscheiding kunnen de contacten van leerlingen worden beperkt
9.7	Het leerkrachtportaal biedt een centrale plek waar alle benodigde informatie beschikbaar is, waaronder onderwijs gerelateerde gegevens, apparaat beheer (via Intune), en toegang tot de helpdesk.
9.8	De DLWO moet ontworpen zijn met een onderwijsgerichte benadering, waarbij bijvoorbeeld de instelling van wachtwoorden mogelijk is op verschillende strengheidsniveaus.
9.9	De DLWO moet de leerkracht de regie geven over de leerlingomgeving en het beheer van apparaten, waaronder de mogelijkheid om Chromebooks en Windows devices zelf in CITO FACET te plaatsen.
9.10	Het moet mogelijk zijn om via het leerkrachtportaal mee te kijken op de leerling device, over te nemen of de activiteiten van de leerling te beheren, bijvoorbeeld door de Toetsmodus in te schakelen.
9.11	De leerkracht moet in staat zijn om zowel zijn eigen portaal als dat van de leerling handig in te delen in categorieën, zodat het overzichtelijker is om specifieke items te vinden.
9.12	Het beheer van alle apparaten (Chromebooks en Windows devices) moet eenvoudig zijn voor de scholen.
9.13	Jonge leerlingen moeten op een eenvoudige manier kunnen inloggen, bijvoorbeeld met een plaatjeslogin, terwijl oudere leerlingen gebruik kunnen maken van een gebruikersnaam en wachtwoord.