



Bijlage H - Programma van Eisen

Bijlage bij	Offerteaanvraag EU – NL openbaar – Security diensten
Datum	21-12-2022
Status	Definitief

Thema 1: Beoordelen van securityhuishouding en opvolging	Eisen
Technische en organisatorische beoordeling van securityhuishouding	
Het beheren en beveiligen van alle (digitale) middelen heeft VfPf uitbesteed bij dienstverleners. Zij zijn verantwoordelijk voor het verzorgen en beveiligen van alle (informatie)componenten waar VfPf gebruik van maakt bij het uitvoeren van kerntaken, namelijk het bedienen van schoolbesturen en uitkeringsgerechtigden in het basisonderwijs.	
Dienstverleners zijn verantwoordelijk voor de beveiliging van het gehele securityhuis zoals bedoeld in 1.3 van de offerteaanvraag waar dit Programma van Eisen onderdeel van is. Om waarborgen dat dienstverleners voldoende zorg dragen bij het beveiligen van de securityhuishouding van VfPf heeft VfPf zich als regie organisatie opgesteld. Hierbij is het de taak van VfPf om zorg te dragen dat dienstverleners zich houden aan de gemaakte afspraken op het gebied van informatiebeveiliging. Om zorg te dragen dat beoordeling van de securityhuishouding doeltreffend is, worden kennis en vaardigheden op dit gebied uitgevraagd middels deze aanbesteding.	
De rol van de opdrachtnemer	
Zoals is beschreven in 1.3 van de offerteaanvraag de beveiliging van het securityhuis te beoordelen. Dit dient gedaan te worden voor het gehele securityhuis van VfPf, op zowel technisch als organisatorisch niveau.	
Technische beoordeling	
De technische beoordeling betreft beoordeling van beveiliging van apparaten, applicaties, code, infrastructuur, data en informatie en huidig geïmplementeerde maatregelen. Er dient te worden onderzocht voor welke kwetsbaarheden de complete technische securityhuishouding van VfPf vatbaar is en welke risico's deze kwetsbaarheden met zich mee brengen.	
Organisatorische beoordeling	
De organisatorische beoordeling betreft het reviewen van door VfPf en dienstverleners aangehouden kaderstelling, geldend beleid en richtlijnen op het gebied van informatiebeveiliging.	
Aantoonbare kennis en vaardigheden	
Eis 1 De teamlead	De medewerker die regie voert op het proces van de technische en organisatorische beoordeling van de securityhuishouding behoort te beschikken over een erkende certificering die aansluit bij de gevraagde kennis en vaardigheden zoals bedoeld in de rol van de opdrachtnemer hierboven.
Eis 2 Medewerkers	Medewerkers die betrokken zijn bij het beoordelen van de technische en organisatorische securityhuishouding dienen te beschikken over erkende certificering. Dit behoort aan te sluiten bij de gevraagde kennis en vaardigheden zoals bedoeld in de rol van de opdrachtnemer hierboven.

Plan van aanpak	
Eis 3 Plan van Aanpak	De opdrachtnemer bereidt een plan van aanpak voor op basis waarvan de technische en organisatorische beoordeling uitgevoerd worden. In dit plan van aanpak dient aandacht besteed te worden aan de handelingen die verricht zullen worden om de securityhuishouding van VfPf te toetsen en te beoordelen, de hiervoor gebruikte werkwijze en de hiervoor gebruikte middelen. Denk hierbij aan middelen zoals tijdsinzet, inzet van personeel en gebruikte (software)tools
Frequentie van dienstverlening	
Eis 4 Planning van beoordeling	De opdrachtgever verwacht dat de opdrachtnemer een planning voorbereid voor de technische en organisatorische beoordeling van de VfPf securityhuishouding. Hierbij dient rekening gehouden te worden met het cyclische karakter van het toetsen van informatiebeveiliging, zoals bedoeld in 1.2 van de offerteaanvraag.
Eis 5 Beoordeling bij incidenten, nieuwe kwetsbaarheden of wijzigingen	Wanneer er sprake is van wijzigingen aan VfPf securityhuishouding, er sprake is van incidenten die de kritieke product- en dienstlevering van VfPf (kunnen) raken of kwetsbaarheden die door een derde partij zijn geïdentificeerd, dient de opdrachtnemer een nieuwe beoordeling uit te voeren.
Rapportage	
Eis 6 Planning rapportage	De opdrachtnemer plant de rapportage over bevindingen en resultaten van beoordelingen in een planning. Hierbij dient rekening gehouden te worden met het cyclische karakter van het toetsen van informatiebeveiliging (zoals bedoeld in 1.2 van de offerteaanvraag), om te zorgen dat VfPf voortdurend 'in control' is op het gebied van informatiebeveiliging.
Eis 7 Uitgevoerde werkzaamheden	De opdrachtnemer legt de werkzaamheden die ten behoeve van het beoordelen van securityhuishouding uitgevoerd worden vast in rapportage, met inbegrip van de uitgevoerde activiteiten, beschrijving van de doelstelling van de beoordeling en de hierbij eventueel gebruikte software/tools.
Eis 8 Resultaten en bevindingen	De opdrachtnemer legt de resultaten van securitytests/reviews en de beoordeling van securityhuishouding vast in rapportage.
Eis 9 Rapportage bij ingrijpende ontwikkelingen risicolandschap	Wanneer bij tests, beoordeling of evaluaties aanwijzingen zijn gevonden dat VfPf staat blootgesteld aan voorheen onbekende risico's dient de opdrachtnemer deze aanwijzingen en risico's vast te leggen in rapportage.
Eis 10 Communicatie van regelmatige rapportage	De opdrachtnemer verzorgt frequente communicatie van rapportage richting de opdrachtgever met inachtneming van de gevraagde planning zoals bedoeld in eis 4 van dit thema.

Eis 11 Communicatie bij ontdekking kritieke kwetsbaarheden	De opdrachtnemer draagt zorg dat gevonden kwetsbaarheden die een mogelijk gevaar vormen voor de kritieke dienst- en productlevering van VfPf binnen 24 uur gemeld worden bij VfPf.
Opvolging	
Eis 12 Behandelstrategie	De opdrachtnemer brengt schriftelijk advies uit voor het oplossen van geïdentificeerde kwetsbaarheden. Hierbij ondersteunt de opdrachtnemer is het formuleren van een behandelstrategie als basis voor het selecteren van maatregelen om de kwetsbaarheden te op te lossen, dan wel te verminderen.
Eis 13 Selecteren van maatregelen	De opdrachtnemer brengt schriftelijk advies uit om VfPf te ondersteunen in het selecteren en implementeren van geschikte maatregelen om gevonden kwetsbaarheden te verhelpen.
Eis 14 Opvolging	De opdrachtnemer behoort middels ondersteuning en schriftelijk advies (zoals bedoeld in thema 2 van dit PvE) opvolging te geven aan de bevindingen van beoordeling en review door advies uit te brengen over het oplossen van kwetsbaarheden die bij technische beoordeling geïdentificeerd zijn.
Privacy	
Eis 15 Verwerkersovereenkomst	Wanneer er bij het beoordelen en testen van infrastructuur en maatregelen gebruik gemaakt wordt van persoonsgegevens en de opdracht (in de zin van AVG) is gericht op het verwerken van persoonsgegevens, wordt de opdrachtnemer hierbij aangemerkt als verwerker en zal er een verwerkersovereenkomst afgesloten worden.
Eis 15a Maatregelen ten behoeve van de beschikbaarheid van persoonsgegevens	De gevraagde dienst behoort bij de verwerking van persoonsgegevens zoals bedoeld in eis 15 hierboven te beschikken over volledig redundant uitgevoerde architectuur.
Eis 15b Maatregelen ten behoeve van de integriteit van persoonsgegevens	Bij de verwerking en bescherming van persoonsgegevens zoals bedoeld in eis 15 hierboven houdt de opdrachtnemer zich aan de onderstaande richtlijnen: • Alle gebruik, starten en stoppen van audit logs wordt gelogged • Creatie en verwijdering van system-level objects wordt gelogged • Alle mutaties van audit trails, configuratiebestanden en parameter files wordt gelogged • Audit trails worden minimaal 3 maanden online en 1 jaar offline, opvraagbaar 48 uur bewaard • Logs worden beschermd door file-integrity monitoring of wijzigingsdetectiesystemen • Integriteitscontroles zijn aanwezig om de integriteit van systeem en configuratiebestanden te monitoren.

Eis 15c Maatregelen ten behoeve van de vertrouwelijkheid van persoonsgegevens	Bij de bescherming van de vertrouwelijkheid van verwerkte persoonsgegevens zoals bedoeld in eis 15 hierboven houdt de opdrachtnemer zich aan de onderstaande richtlijnen: • 2-factor authenticatie moet worden toegepast. • Deblokkeren van geblokkeerde account dient handmatig plaats te vinden. • Alle data worden versleuteld opgeslagen. • Alle gebruik van authenticatiemiddelen wordt gelogged. • Gedetecteerde extreme aantallen verkeerde inlogpogingen worden direct aan Security Management gemeld. • Host based ISD dient geactiveerd te zijn. • Interne IT beheerder maken gebruik van een Stepping Stone om toegang te krijgen tot de omgeving.

Thema 2 Voorziening van kennis en inzicht	Eisen
De rol van de opdrachtnemer VfPf zoekt de samenwerking met een kennishoudende partij op het gebied van informatiebeveiliging. Binnen de scope van de opdracht verwacht VfPf dat de opdrachtnemer kennis en inzicht levert op het gebied van: ▪ Het formuleren van vervolgstappen om bevindingen uit audits, beoordelingen en reviews (zoals bedoeld in thema 1 van dit document) op te lossen. ▪ Het aanbesteden van nieuwe diensten en/of producten op het gebied van informatiebeveiliging. (zoals bedoeld in thema 4 van dit document) ▪ Het ontwikkelen, onderhouden en verbeteren van de interne kaderstelling ten opzichte van informatiebeveiliging als ondersteuning van de tweede lijn (P&S). ▪ Marktontwikkelingen op het gebied van producten, diensten en (informatie)beveiligingstechnieken.	
Aantoonbare kennis en vaardigheden	
Eis 16 Vergelijkbare opdracht	De opdrachtnemer dient aan te kunnen tonen een vergelijkbare opdracht te hebben uitgevoerd waarbij de opdrachtnemer verantwoordelijk was voor het leveren van kennis en advies op het gebied van informatiebeveiliging.
Eis 17 Aantoonbare kennis Teamlead	Werknemers van de opdrachtnemer dienen te beschikken over de juiste kennis en vaardigheden. De Teamlead behoort over erkende certificering te beschikken die aansluit bij de gevraagde kennis en vaardigheden van een persoon die regie voert over de activiteiten zoals beschreven in de rol van de opdrachtnemer hierboven
Eis 18 Aantoonbare kennis teamleden	Werknemers van de opdrachtnemer dienen te beschikken over de juiste kennis en vaardigheden. De medewerkers die betrokken zijn bij het voorzien van kennis en inzicht behoort over erkende certificering te beschikken die aansluit bij de gevraagde kennis en vaardigheden zoals bedoeld in de rol van de opdrachtnemer hierboven
Levering van kennis en inzicht op het gebied van informatiebeveiliging	
Eis 19 Inzicht over informatiebeveiliging	De opdrachtnemer is op aanvraag beschikbaar voor het beantwoorden van vragen op het gebied van de ontwikkeling van de algehele informatiebeveiliging bij VfPf.
Eis 20 Second opinion	De opdrachtnemer is beschikbaar om een 'second opinion' te formuleren wanneer een van de andere dienstverleners die voor VfPf werkzaam is een advies op het gebied van informatiebeveiliging uitbrengt waarbij VfPf twijfels heeft over de doeltreffendheid.

	Hierbij dient de opdrachtnemer een oordeel te formuleren over het door een andere dienstverlener geleverde advies. VfPf verwacht ondersteuning bij het maken van de juiste keuzes op het gebied van informatiebeveiliging, ook in het geval van incidenten en calamiteiten.
Eis 21 Ondersteuning bij kaderstelling	De opdrachtgever verlangt ondersteuning bij het (blijvend) ontwikkelen van de interne kaderstelling zoals bedoeld . De kaderstelling wordt ontwikkeld op basis van relevante, huidig geldende en nieuw ontwikkelde normen en standaarden op het gebied van informatiebeveiliging. Hierbij wordt de opdrachtnemer verwacht te ondersteunen in het opstellen en verbeteren van interne kaderstelling op basis van erkende normen en standaarden.
Beschikbaarheid	
Eis 22 Beschikbaarheid binnen werktijden	De opdrachtnemer dient altijd beschikbaar te zijn voor vragen en het leveren van inzicht en informatie ten opzichte van informatiebeveiliging binnen VfPf werktijden.
Eis 23 Beschikbaarheid buiten werktijden	De opdrachtnemer dient bij spoed bereikbaar te zijn voor het beantwoorden van vragen en het leveren van inzicht en informatie ten opzichte van informatiebeveiliging buiten werktijden van VfPf.
Eis 24 Overleg op locatie	Binnen kantooruren of bij calamiteiten kan VfPf de opdrachtnemer vragen om op locatie van VfPf aanwezig te zijn voor overleg.
Communicatie	
Eis 25 Communicatie over onbeschikbaarheid / verzuim	Wanneer de opdrachtnemer niet in staat is om de gevraagde diensten te leveren dient de opdrachtgever hiervan zo snel mogelijk, maar niet langer dan 24 uur op de hoogte gesteld te worden. De opdrachtgever houdt zich bij situaties waarin de gevraagde diensten niet geleverd kunnen worden altijd het recht voor de gevraagde dienstverlening bij een derde partij af te nemen.

Thema 3: Beoordeling van naleving	Eisen
VfPf zoekt een partij die de eerste lijn ondersteunt in het beoordelen van de mate waarin dienstverleners zich houden aan de gemaakt afspraken uit overeenkomsten op het gebied van informatiebeveiliging. De rol van de opdrachtnemer De opdrachtnemer wordt verwacht ondersteuning te bieden bij de werkzaamheden van de eerste lijn, namelijk het beoordelen van de mate waarin dienstverleners voldoen aan de door VfPf vastgelegde eisen en geldende principes op het gebied van informatiebeveiliging. Dit gebeurt met inachtneming van de door VfPf vastgelegde eisen en geldende principes zoals bedoeld in thema 3 (hoofdstuk 1.3 van de offerteaanvraag)	
Eis 26 Toetsen van naleving	De opdrachtnemer ondersteunt bij het beoordelen van naleving aan kaderstelling, afspraken en overeenkomsten tussen VfPf en dienstverleners. Dit houdt in de opdrachtnemer de afdeling service management ondersteunt bij het nagaan of dienstverleners zich houden aan de gemaakte afspraken op het gebied van informatiebeveiliging en de daaraan verwante overeenkomsten.
Eis 27 Wijze van ondersteuning	De opdrachtnemer wordt verwacht als kennishouder te ondersteunen bij het beoordelen van de door dienstverleners uitgevoerde taken. Dit dient gedaan te worden met inachtneming van hoofdstuk18 uit ISO 27001/2 (Versie 2017) en andere van toepassing verklaarde normenkaders.
Eis 28 Planning van dienstverlening	De opdrachtgever verwacht dat de opdrachtnemer een planning opgesteld waarlangs de gevraagde dienstverlening uitgevoerd wordt.

Thema 4: Advisering en ondersteuning bij aanbestedingen	Eisen
Wanneer er vanuit de organisatie behoefte bestaat voor het aanbrengen van wijzigingen in de IT-infrastructuur van VfPf, of het aannemen van nieuwe dienstverleners kan het zijn dat VfPf een nieuwe aanbesteding in gaat op het gebied van informatiebeveiliging. VfPf heeft behoefte aan een partij die ondersteunt in het maken van de juiste keuze voor nieuwe dienstverleners bij aanbestedingen.	
Formuleren van behoeftes	
Eis 29	VfPf verlangt ondersteuning bij het identificeren en formuleren van behoeftes voor informatiebeveiliging. Deze behoeftes vormen de basis voor het opstellen van selectiecriteria die gelden voor aanbestedingen op het gebied van informatiebeveiliging.
Opstellen van selectie eisen en vragen	
Eis 30	De opdrachtgever vraagt de opdrachtnemer om de eerste lijn op verzoek te ondersteunen in het formuleren van eisen en vragen op het gebied van informatiebeveiliging voor het selecteren van opdrachtnemers op verdere aanbestedingen op het gebied van informatiebeveiliging.
Beoordelen van aanbieders	
Eis 31 Beoordelen van aanbieders	De opdrachtnemer ondersteunt VfPf in het beoordelen van de geschiktheid van (mogelijke) aanbieders voor aanbestedingen op het gebied van informatiebeveiliging. De beoordeling van aanbieders gebeurt met inachtneming van de door VfPf vastgelegde selectiecriteria.
Eis 32 Beoordeling van aanbod	De opdrachtnemer dient te ondersteunen in het beoordelen van de reacties van opdrachtnemers op door VfPf uitgevraagde aanbestedingen op het gebied van informatiebeveiliging.