

**Europese aanbesteding Kantoorautomatisering en systeembeheer  
voor het  
Commissariaat voor de Media  
Bijlage 6: Programma van Eisen**

Datum	4 maart 2022
Versie	1.1
Status	Definitief
Disclaimer	© Gehele of gedeeltelijke overneming, reproductie of openbaarmaking van de stukken, op welke wijze dan ook, zonder voorafgaande schriftelijke toestemming van het Commissariaat voor de Media is verboden, behoudens de beperkingen bij de wet gesteld. Het verbod betreft ook gehele of gedeeltelijke bewerking.



# Inhoud

Definiëren opdracht.....	3
Vertrekpunt .....	3
Doelstellingen opdracht .....	3
Omschrijving opdracht .....	3
Huidige en gewenste situatie .....	4
Huidige situatie .....	4
Gewenste toekomstige situatie .....	4
Leveringen en diensten .....	4
Leveringen: .....	4
Diensten .....	5
Buiten de scope van de inkoopopdracht .....	5
Onsite systeembeheerder .....	6
Servicedesk .....	6
Inrichten, beheren, onderhouden, support leveren van IT werkplekken .....	7
Werkplek inrichting : .....	7
Werkplekbeheer : .....	7
Werkplek onderhoud:.....	7
Werkplek support: .....	7
Inrichten, beheren en onderhouden van de server omgeving / Azure .....	9
Inrichten, beheren en onderhouden van de netwerk infrastructuur .....	9
Het (proactief) adviseren van de IT-adviseur.....	9
Capacity Management .....	10
Availability Management .....	11
Beveiliging.....	11
Change Management.....	12
Service Asset & Configuration Management .....	12
Incident Management.....	13
Problem management .....	13
Continual Service Improvement .....	13
IT service continuity management .....	13
Eisen met betrekking tot de performance van IT Service Continuity Management .....	13
Aansturing leverancier inclusief overlegstructuur .....	14
Eisen aan de transitie .....	15
Bijlage 1 : Overzicht software en SaaS diensten .....	16
Bijlage 2: Schematische beschrijving huidige IT-omgeving .....	18

## **Definiëren opdracht**

### Vertrekpunt

Het Commissariaat voor de Media is voornemens om de IT-werkplekken van medewerkers, de daarbij behorende netwerkinfrastructuur, het onderhoud van het virtuele serverpark en de gebruikersondersteuning te gaan aanbesteden. De directe aanleiding voor aanbesteding is het aflopen van de contracttermijn met de huidige leverancier.

## **Doelstellingen opdracht**

Het inkooptraject is gericht op het contracteren van één leverancier voor het beheren en onderhouden van de gehele kantoorautomatisering en het ondersteunen van de medewerkers van het Commissariaat voor de Media bij IT problemen en vraagstukken. Ondersteuning dient zowel remote/telefonisch bereikbaar te zijn maar ook drie dagen per week op locatie in Hilversum.

## **Omschrijving opdracht**

Voor de duur van 24 maanden, met de mogelijkheid om deze overeenkomst te kunnen verlengen met 2 x 12 maanden, een organisatie contracteren die de totale kantoorautomatisering verzorgt met daarbij een systeembeheerder die 3 dagen in de week (ma, di, do) werkzaam is op locatie in Hilversum. De andere 2 dagen (wo, vr) of bij afwezigheid van de systeembeheerder worden door een back-up organisatie "op afstand" geserviced. De systeembeheerder op locatie zal primair aanspreekpunt zijn voor de medewerkers van het Commissariaat voor de Media bij IT problemen en vraagstukken.

Met betrekking tot IT heeft het Commissariaat voor de Media een aantal belangrijke uitgangspunten:

- Het Commissariaat voor de Media werkt alleen met 'proven technology';
- Eén leverancier is het eerste aanspreekpunt voor netwerk-, server- en werkplekproblemen;
- De interne functioneel beheerder is het eerste aanspreekpunt voor de specifieke primaire applicaties;
- De leverancier verzorgt een webportal voor incident management (zowel voor de IT-infrastructuur als de applicaties).
- Bij afwezigheid van de interne systeembeheer is er een Servicedesk bereikbaar die door alle medewerkers van het Commissariaat voor de Media kan worden benaderd.

## **Huidige en gewenste situatie**

### **Huidige situatie**

De ongeveer 70 medewerkers van het Commissariaat voor de Media hebben allen een laptop (HP Elitebook X360) tot hun beschikking met Windows 10 Pro en Office 365 E3 licentie (CSP). Alle gegevens op de laptops zijn door middel van Bitlocker versleuteld en door het gebruik van Always On VPN kunnen alle medewerkers plaats onafhankelijk veilig werken.

De laptops worden via Autopilot geïnstalleerd en vanuit MS Intune beheerd en van de juiste software packages voorzien. Enkel devices die in Intune bekend zijn kunnen inloggen op het domein.

Het Commissariaat voor de Media heeft gekozen voor de strategie om zoveel mogelijk SaaS applicaties te gebruiken, hierdoor zijn er maar een beperkt aantal losse softwarepakketten nodig. Inloggen op de cloudapplicaties gaat nagenoeg allemaal door middel van SSO (Azure AD) en is beveiligd door Multi-Factor Authenticatie (MFA) in combinatie met Conditional Access.

Het Commissariaat voor de Media gebruikt Windows servers, deze staan in een Azure omgeving. Op dit moment fungeert één van deze servers als fileserver, medewerkers krijgen via een fileshare toegang tot de gegevens op deze fileserver.

Op kantoor zijn alle (flex)werkplekken voorzien van twee beeldschermen en een dockingstation, de onsite systeembeheerder verzorgt de aansluitingen en kabelmanagement van deze (flex)werkplekken. De (flex)werkplekken zijn allemaal voorzien van een bekabelde aansluiting op 1 van de 6 Aruba switches, een WatchGuard firewall ontsluit de internetlijn (KNP ÉÉN (1Gb). Daarnaast is er een losse backup internetlijn van Ziggo die ingezet kan worden bij storing op de KPN-aansluiting.

### **Gewenste toekomstige situatie**

Hybride werken is de nieuwe norm binnen het Commissariaat voor de Media, het blijft dus belangrijk om veilig plaats onafhankelijk te kunnen werken. Het Commissariaat voor de Media heeft groeiplannen waardoor het de verwachting is dat er voor juni 2023 80 medewerkers zullen zijn.

Het is de wens om de huidige fileshare-omgeving om te zetten naar een SharePoint omgeving. Deze SharePoint omgeving dient zo laagdrempelig mogelijk benaderd te kunnen worden en er loopt een project om te inventariseren welke data er naar SharePoint verhuisd zou kunnen worden. Ook wordt er momenteel gebouwd aan een nieuw (SharePoint) Intranet, zodat er gemakkelijk vanuit het Intranet verwezen kan worden naar SharePoint bestanden.

De verwachting is dat de komende tijd meer gebruik gemaakt worden van de mogelijkheden van MS Office 365; de overgang naar het nieuwe Intranet en de bestanden naar SharePoint geeft mogelijkheden om door middel van PowerBI betere rapportage mogelijkheden te gaan bieden. Ook voorzien wij een verhoogd gebruik van het werken met Teams, de eerste Teams-pilots lopen momenteel en wekken enthousiaste reacties van de medewerkers op.

### **Leveringen en diensten**

De aanbesteding heeft betrekking op de inkoop van de volgende leveringen en diensten:

#### **Leveringen**

- Hardware voor de netwerkinfrastructuur onderhouden, leveren en adviseren bij eventuele benodigde vernieuwing.

- Leveren en licentiebeheer van Microsoft Office 365 E3 licenties en Adobe Acrobat Pro.
- Leveren en beheren PKI SSL certificaten.
- Registreren en verlengen van domeinnamen.

### **Diensten**

- Het leveren van een vaste systeembeheerder op locatie.
- Inrichten, beheren en onderhouden van IT-werkplekken.
- Inrichten, beheren en onderhouden van de server omgeving.
- Inrichten, beheren en onderhouden van de netwerk infrastructuur.
- Het leveren van een vloeiend Nederlandstalig sprekende Servicedesk die door alle medewerkers van het Commissariaat voor de Media kunnen worden benaderd bij vragen of problemen.
- Het proactief adviseren van de IT-adviseur en het uitvoeren van service aanvragen.

Buiten de scope van de inkoopopdracht vallen in ieder geval de navolgende zaken:

- Aanschaf van hardware. Het Commissariaat voor de Media wil de vrijheid behouden om hiervoor zelf een leverancier te selecteren.
- Telefonie platform. Het Commissariaat voor de Media heeft de mobiele en vaste telefonie belegd bij een derde partij.
- Printers. Het Commissariaat voor de Media heeft de lease en het onderhoud van de kantoorprinters belegd bij een derde partij.
- Wifi netwerk. Het Commissariaat voor de Media heeft het Wifi netwerk belegd bij een derde partij.

De leveringen en diensten zijn op de volgende pagina's nader geconcretiseerd:

## Onsite systeembeheerder

Op maandag, dinsdag en donderdag zal er een systeembeheerder aanwezig zijn in het kantoorpand van het Commissariaat voor de Media in Hilversum. Het Commissariaat voor de Media hecht er grote waarde aan dat er één persoon vanuit de leverancier als onsite systeembeheerder wordt ingezet bij het Commissariaat voor de Media en dat er niet met een pool-constructie wordt gewerkt. Bij ziekte of afwezigheid van de onsite systeembeheerder zal de leverancier op eigen initiatief zorg dragen voor een -zo goed als mogelijke- vervanger. De onsite systeembeheerder fungeert als primair contactpersoon bij alle IT problemen en vraagstukken en wordt aangestuurd door de IT-adviseur van het Commissariaat voor de Media. Van de onsite systeembeheerder wordt verwacht dat hij zich verdiept en proactief meedenkt in de IT vraagstukken die zich kunnen voordoen bij het Commissariaat voor de Media. Tevens zal de onsite systeembeheerder participeren in werkzaamheden die niet specifiek worden uitgevraagd in deze aanbesteding zoals het inrichten van werkplekken, het verzorgen van de on- / off boardingswerkzaamheden, het assisteren bij organisatie specifieke oplossingen zoals het zaakstelsel, het uren registratiesysteem, het toegangscontrole systeem etc.

De taken van de onsite systeembeheerder zullen voornamelijk gericht zijn op het ondersteunen van de interne organisatie en niet op serverbeheer, backup controle en het verzorgen van updates.

## Servicedesk

De onsite systeembeheerder zal op de dagen dat hij aanwezig is het primaire aanspreekpunt zijn voor alle medewerkers van het Commissariaat voor de Media. Op de dagen dat de onsite systeembeheerder niet op locatie is zal zijn telefoon en mail worden doorgeschakeld naar een servicedesk zodat de medewerkers van het Commissariaat voor de Media ten allen tijden ondersteuning kunnen krijgen vanuit de leverancier.

## Met betrekking op de servicedesk

Van de servicedesk wordt verwacht dat er snel wordt opgenomen (80% binnen 20 seconden) en dat de servicedesk medewerker over voldoende kennis en kunde beschikt om eenvoudige vragen en kleine verstoringen direct op te kunnen lossen (oplossingsgerichtheid en klantgerichtheid).

Onderstaande hersteltijden gelden als minimum serviceniveaus:

Prioriteit	Beschrijving	Max. reactietijd	Hersteltijd na melding
1 (top)	Functionaliteit voor 5 of meer gebruikers niet beschikbaar	15 min	< 4 uur
2 (hoog)	Functionaliteit voor minder dan 5 gebruikers niet beschikbaar en hinderlijk voor 5 of meer gebruikers	30 min	< 8 uur
3 (normaal)	Hinderlijke verstoring voor enkele gebruikers	30 min	< 16 uur
4 (laag)	Verstoring, maar geen hinderlijke situatie	4 uur	< 40 uur

5	Afhandeling standaard service verzoeken	1 uur	conform opgegeven termijnen bij standaard changes
6	Beantwoording niet standaard serviceverzoeken en complexe vragen niet vallen onder bovenstaande categorieën 1 t/m 5	24 uur	In overleg doch uiterlijk binnen 1 maand

De servicedesk medewerkers spreken de Nederlandse taal vloeiend, hebben inzicht hebben in de werkzaamheden van de onsite systeembeheerder en het werk- en denkniveau is hoog genoeg is om het groot deel van de vragen gelijk worden opgelost zonder te hoeven escaleren naar een hogere helpdesklijn.

### **Inrichten, beheren, onderhouden, support leveren van IT werkplekken**

Overzicht werkzaamheden **werkplekken**:

Werkplek inrichting :

- (her)installeren van bestaande of nieuwe laptops door middel van een automatisch systeem zoals AutoPilot.
- Het installeren van software op de laptops.
- Het installeren van een mobiele telefoon / iPad.
- Het uitgeven van nieuwe apparatuur aan medewerkers van het Commissariaat voor de Media.
- Het beheren en uitgeven van tijdelijke apparatuur.

Werkplekbeheer :

- Het monitoren van de laptops op virussen/ malware / ransomware en hierop acteren.
- Het monitoren van de laptops op stabiliteit en abnormale processen en hier op acteren.
- Het packagen van veel gebruikte softwarepakketten zodat deze eenvoudig op verzoek bij medewerkers van het Commissariaat voor de Media kunnen worden geïnstalleerd.
- Het remote kunnen overnemen van het werkstation van de CvdM medewerker om efficiënt te kunnen ondersteunen.

Werkplek onderhoud:

- Het tijdig bijwerken van software updates voor Windows, Office en algemeen voorkomende applicaties zoals Adobe Reader en VLC-mediaplayer.
- Het updaten van specifieke software oplossingen die door het Commissariaat voor de Media in gebruik zijn.
- Het tijdig bijwerken van firmware van laptops, dockingstations en andere apparatuur waarbij dit nodig is.
- Bij defecte apparatuur contact opnemen met de leverancier en de garantie afhandeling afwickelen of reparatie verzorgen.
- Het bijhouden van het assetmanagement systeem.

Werkplek support:

- Medewerkers van het Commissariaat voor de Media begeleiden en instructies geven over gebruik van de tot hun beschikking gesteld hard- en software.

- Aanspreekpunt voor eerste, tweede en derdelijns IT problemen en indien nodig deze problemen voorleggen aan de IT-adviseur.
- Schakelen met leveranciers van IT oplossingen die door het Commissariaat voor de Media worden gebruikt om problemen op te lossen of hier in te assisteren.
- Azure AD Accountbeheer.
- Permissie wijzigingen maken in mailboxen, SharePoint sites, netwerkschijven etc.

## **Inrichten, beheren en onderhouden van de server omgeving / Azure**

Overzicht werkzaamheden:

- Het tijdig updaten/vervangen van de huidige virtuele Windows servers.
- Het verzorgen van een backup van de servers inclusief een periodieke controle.
- Monitoren van de servers op onregelmatigheden / virussen / performance en beveiligings issues en daar op acteren.
- Het bijhouden van een deugdelijke documentatie van de servers en de Azure omgeving.

## **Inrichten, beheren en onderhouden van de netwerk infrastructuur**

Overzicht werkzaamheden:

- Het beheren van de switches, firewall en internetverbindingen.
- Het tijdig bijwerken van firmware updates van de switches, firewall en routers.
- Het monitoren op beveiligingsproblemen en ongewone activiteiten (en hier op acteren).
- Het bijhouden van een deugdelijke documentatie waarin minimaal terug te vinden is welk poorten afwijkend geconfigureerd zijn (en met welke reden).
- Het bijhouden van een backup van de configuraties van de apparatuur waar mogelijk.
- Het op verzoek van de IT-adviseur wijzigingen maken op poort-niveau.

## **Het (proactief) adviseren van de IT-adviseur**

Van de leverancier wordt het volgende verwacht:

- Inzicht hebben/geven in incident-statussen en prioriteringen, problemen, serviceverzoeken en standaard changes.
- Tussentijds opvragen door het Commissariaat voor de Media van prioritering en status van requests dient telefonische, per e-mail en via een webportaal mogelijk te zijn.
- Opstellen maand SLA-rapportages (binnen maximaal 5 werkdagen na afloop van kalendermaand) en versturen aan IT-adviseur met daarin:
  - o aantal, prioriteit, soort melding (tenminste incidenten, service requests en wijzigingen);
  - o prestatieoverzichten van afhandeling meldingen (duur openstaande melding, responstijd, hersteltijd, per categorie);
  - o aantal, soort en beschrijving beveiligingsincidenten (inclusief rapportages uit antivirus programma, firewall en/of intrusion detection systemen);
  - o aantal, soort en beschrijving integriteitsincidenten;
  - o technische gegevens m.b.t. capaciteit en beschikbaarheid (CPU gebruik, geheugengebruik etc.);
  - o oordeel en/of advies naar aanleiding van de SLA-rapportage;
  - o maatregelen ter verbetering van service levels indien deze beneden het vereiste niveau zijn of dreigen te raken;
  - o lopende en afgeronde niet-standaard changes.
- Periodiek overleg met IT-adviseur:
  - o Bespreking SLA-rapportages en opvolging voorgestelde maatregelen;
  - o Problem Management;
  - o Continual Service Improvement;
  - o Actueel houden van technische en beheerdocumentatie.

## Capacity Management

- Het garanderen van de (in de inventarisatie bepaalde) performance (nu en in de toekomst) van de werkplekinrichting en aanvullende diensten die aan het Commissariaat voor de Media ter beschikking worden gesteld. Leverancier dient bij dit proces het voortouw te nemen en tools/methodieken aan te dragen, af te stemmen en in te zetten;
- Het maandelijks meten van de performance van de werkplekinrichting aan de hand van de in de inventarisatie gezamenlijk vastgestelde performance baseline;
- Het maandelijks meten van de capaciteit van de (virtuele) hardware en infrastructuur die nodig is voor het leveren van zijn diensten;
- Het proactief adviseren over de aanvulling of verbetering van de infrastructuur (inclusief werkplekken), zodat de performance gegarandeerd blijft;
- De kwaliteit van de hardware en infrastructuur op dusdanig niveau houden, zodat service levels te allen tijde gehaald kunnen blijven worden;
- Het op basis van de gestelde eisen, ten aanzien van de performance en capacity van de dienstverlening, opstellen van voorstellen voor vervanging van onderdelen uit de infrastructuur inclusief werkplekken (refreshments) en het, na schriftelijke accordering door het Commissariaat voor de Media, uitvoeren hiervan conform de gestelde eisen met betrekking tot availability management;
- Voor de performance van de centrale infrastructuur verwacht Commissariaat voor de Media een adequate performance voor haar kantoorapplicaties. Om dit te kwantificeren hanteert het Commissariaat voor de Media de volgende performance parameters op basis van normaal gebruik (uitgezonderd van fouten in maatwerk, gebruikersfouten, lopende batchjobs, abnormaal netwerkverbruik en bugs in standaardapplicaties) met maximaal de volgende verwerkingstijden:
  - De ingezette hard- en software dient 95% van de dagelijkse veel gebruikte 'ICT-activiteiten' van de medewerkers geheel uit te voeren binnen één seconde. Het vaststellen van deze 'dagelijks veel uitgevoerde activiteiten' gebeurt in overleg met het Commissariaat voor de Media.
  - De overige minder vaak uitgevoerde ICT-activiteiten (zoals ook inloggen, rapportages, etc.) worden binnen drie seconden afgerond of tonen de eerste resultaten (eventueel plus tijd nodig voor het verzenden van bestanden). Het vaststellen van deze minder uitgevoerde activiteiten gebeurt in overleg met het Commissariaat voor de Media.
  - De door de opdrachtgever gebruikte applicaties ondervinden geen vertragingen door de opzet van de door leverancier geleverde onderliggende systemen en diensten.
  - Leverancier garandeert dat de aan het Commissariaat voor de Media aangeboden oplossing (bv. netwerk, reken capaciteit, opslagcapaciteit) niet wordt beïnvloed (performance beschikbaarheid) door gedrag of activiteiten van andere gebruikers van de infrastructuur van leverancier.

Bovenstaande performancecriteria gelden als minimale performancecriteria. Indien de performance lager dreigt te worden dient de leverancier in ieder geval maatregelen voor te stellen en te nemen (inspanningsverplichting).

## **Availability Management**

- Het garanderen van de beschikbaarheid van de werkplekinrichting voor gebruikers van het Commissariaat voor de Media, inclusief thuiswerkers;
- Het maken van afspraken op het operationele vlak (DAP) om de beschikbaarheidsniveaus te halen;
- Het garanderen dat preventief en adaptief onderhoud en andere systeem belastende werkzaamheden tussen 19:00 en 07:00 uur, dus buiten kantooruren, worden ingepland, zodat de gevraagde beschikbaarheid gehaald kan worden. De aangegeven periode is de periode waarin preventief en adaptief onderhoud kan plaatsvinden;
- Leverancier kondigt onderhoud aan de werkplekinrichting en aanvullende diensten minimaal 14 dagen van tevoren aan middels een nog vast te stellen procedures in het DAP;
- Leverancier is tevens verantwoordelijk voor patches en updates die vanuit leveranciers van de door hem gebruikte werkplekapparatuur komt. Deze worden door leverancier getest doorgevoerd op een moment waardoor het Commissariaat voor de Media hier geen last van heeft;
- Leverancier garandeert dat de beschikbaarheid van de werkplekinrichting en aanvullende diensten minimaal 99,8% bedraagt, exclusief gepland onderhoud, per maand gemeten tijdens het service window 07:00-19:00 uur.

De beschikbaarheid op centraal niveau (servers, storage) dient gemeten te worden door de leverancier:

- op basis van zowel automatische voorzieningen die aangeven dat bepaalde functies in het geheel niet beschikbaar zijn voor alle gebruikers of een deel van de gebruikers;
- op basis van door de gebruikers gemelde verstoringen dat de functionaliteit van een werkplek geheel of voor een belangrijk deel niet beschikbaar is.

## **Beveiliging**

- Leverancier garandeert dat minimaal 1x per jaar een penetratietest wordt uitgevoerd, de eerste keer tijdens de transitiefase, en legt de uitkomsten voor aan het Commissariaat voor de Media. Deze penetratietest wordt uitgevoerd door een onafhankelijke derde partij. Indien uit deze test aandachtspunten naar voren komen zal leverancier maatregelen treffen om deze aandachtspunten op te lossen;
- Firewall: 100% adequate bescherming tegen ongeautoriseerde toegang vanaf externe netwerken en het internet (zowel centraal als op de werkplek);
- Virusbeveiliging: 100% adequate bescherming tegen virussen die per email, via de browser of via andere opslagmedia (USB-keys, etc.) verspreid kunnen worden (zowel centraal als op de werkplek), waaronder dus ook up-to-date houden van de virusbeveiligingssoftware;
- Spamfiltering: bij 98% van de gebruikers geen enkele spammail per dag in hun persoonlijke e-mail. Bij de resterende 2% van de gebruikers wordt dit beperkt tot maximaal 1 spammail per dag;
- Leverancier garandeert dat informatie en/of gegevens van andere klanten niet vermengd kunnen raken met de informatie en/of gegevens van het Commissariaat voor de Media;
- Leverancier garandeert dat alle door hem geleverde diensten voldoen en blijvend zullen voldoen aan het gestelde in de Algemene Verordening Gegevensbescherming (AVG);
- Leverancier garandeert dat bewaartermijnen van gegevens instelbaar zijn.

## **Change Management**

- Analyseren van gewenste wijzigingen in de werkplekinrichting en/of infrastructuur en vervolgens op geautoriseerd verzoek van het Commissariaat voor de Media doorvoeren en aanbieden van de wijzigingen;
- Het uitvoeren van standaard wijzigingsverzoeken (de genoemde tijden gelden binnen het service window van 7:00 tot 19:00 uur). Leverancier beoordeelt en behandelt minimaal de volgende verzoeken als standaardverzoeken:
  - Installeren of verhuizen van een nieuwe werkplek (binnen 4 uur)
  - Blokkeren van gebruikerstoegang (account) (binnen 1 uur)
  - Aanmaken nieuw gebruikersaccount (binnen 4 uur)
  - Afvoeren gebruikersaccounts (binnen 4 uur)
  - Wijzigen autorisatie van gebruikers (4 uur)
  - (Her)installeren nieuwe werkplek (2 uur)
  - Wachtwoord reset (binnen 1 uur)
  - Het geautoriseerd installeren en toekennen van nieuwe software aan een gebruiker (binnen 4 uur)
  - Wijzigingen in individuele instellingen email, agenda, filesettings (binnen 4 uur)
  - Restore verzoek van individuele gebruikers (binnen 4 uur)
  - Verwerken aan/af melding domein op spamlist (binnen 4 uur);
- Leverancier dient bij niet-standaard wijzigingen een Plan van Aanpak voor de niet-standaard wijziging in, waarin in ieder geval de planning, voorziene impact en de verwachte kosten zijn beschreven;
- Het op niveau houden van kennis bij eindgebruikers van het gebruik van de centrale infrastructuur nadat nieuwe gebruikers worden aangemaakt en wijzigingen met impact op het gebruik zijn doorgevoerd;
- Testen, installeren en doorvoeren van nieuwe release en versies om de infrastructuur en werkplekken “state-of-the-art” te houden.

## **Service Asset & Configuration Management**

- Het vastleggen en actueel houden van de configuratiegegevens ten behoeve van het verkrijgen van inzicht in de status en inrichting van de systemen in een configuration management database (CMDB) (naast hardware componenten, ook de patch levels, firmware versies etc.);
- Het documenteren van de configuratie van deze componenten op een dermate manier dat kennis raadpleegbaar en overdraagbaar is;
- Het verschaffen van inzicht aan het Commissariaat voor de Media c.q. toegang verlen en aan het Commissariaat voor de Media tot deze CMDB;
- Het onderhouden van de configuratiegegevens en documentatie met behulp van een CMDB in de reeds gebruikte portal binnen het CVDM;
- Het uitvoeren van een jaarlijkse check op de volledigheid van de CMDB en hierover rapporteren.

### **Incident Management**

- Het vastleggen, volgen en beantwoorden van alle incidenten van gebruikers van Commissariaat voor de Media;
- Het doorgeven van incidenten aan het aanspreekpunt bij de verantwoordelijke third party of verantwoordelijke voor functioneel applicatiebeheer binnen het Commissariaat voor de Media;
- Het oplossen en testen van de oplossing van het incident, indien noodzakelijk met behulp van andere betrokken partijen en eventueel on-site;
- Indien noodzakelijk het escaleren van het incident volgens de afspraken in de DAP;
- Het afsluiten, melden en rapporteren over de oplossing of workaround.

### **Problem management**

- Signaleren van trends, vaak voorkomende incidenten, onderliggende oorzaken en verbanden. Deze trends worden periodiek besproken met de ICT-adviseur binnen het Commissariaat voor de Media;
- Het doen van voorstellen op basis van bovenstaande analyse, ter voorkoming van incidenten;
- Analyseren van gemelde incidenten in de betreffende periode (maandelijks) en van de IT-infrastructuur op mogelijke zwakke punten en oorzaken van terugkomende incidenten;
- Resultaten van de analyse communiceren naar en bespreken met leverancier (maandelijks) en wanneer nodig opdracht geven voor onderzoek en probleemoplossing;
- Rapporteren over openstaande en afgesloten problemen.

### **Continual Service Improvement**

Per kwartaal zal leverancier op basis van ontwikkelingen in de markt en binnen het Commissariaat voor de Media adviezen uitbrengen op het gebied van innovatie om hiermee kosten te besparen en/of de dienstverlening te verbeteren. Tevens wordt in de bespreking van dit advies stilgestaan bij mogelijkheden om de nieuwe functies en functionaliteiten beschikbaar te stellen.

### **IT service continuity management**

Eisen met betrekking tot IT Service Continuity Management :

- Back-up, restore en testen van restore functionaliteit:
  - Leverancier voorziet in het maken van een backup;
  - Leverancier voorziet in het testen van de backup;
  - Leverancier voorziet in het terugzetten van backup.
- Leverancier voorziet in disaster recovery;
- Onderhoud (naast correctief ook preventief en adaptief) ten behoeve van alle in beheer zijnde functionaliteiten en in beheer zijnde fysieke componenten, waaronder garantieafhandeling/contractmanagement (inclusief verlengen van contracten) bij leveranciers van de in beheer genomen componenten voor:
  - technisch onderhoud voor hardware;
  - reparatie;
  - eventueel courante vervanging werkplekken wanneer fysieke componenten niet meer bruikbaar zijn, d.w.z. niet meer voldoen aan de vigerende standaard of extra nodig zijn.

### **Eisen met betrekking tot de performance van IT Service Continuity Management**

- De periode van dataverlies van de gegevens die beschikbaar zijn op een werkplek is maximaal 24 klokuren. Daardoor gaat nooit meer dan 1 werkdag werk verloren;

- De back-ups worden incrementeel in het datacentrum van leverancier of beveiligd in de cloud opgeslagen;
- Dagelijks wordt een back-up gemaakt van de gegevens (bestanden en Exchange). De minimale bewaartermijn van de dagelijkse back-ups is 4 weken;
- Maandelijks wordt een back-up gemaakt van de gegevens (incl. file- en mailservers). De minimale bewaartermijn van de dagelijkse back-ups is 1 jaar;
- Jaarlijks wordt een back-up gemaakt van de gegevens (incl. file- en mailservers). De minimale bewaartermijn van de dagelijkse back-ups is 7 jaar;
- Opdrachtnemer garandeert dat gegevens die opgeslagen liggen in de back-up op een passende wijze worden beveiligd tegen inzage van derde partijen, bijvoorbeeld door middel van encryptie;
- Er dient voor e-mail minimaal één back-up systematiek te worden verzorgd waarmee dagelijks aan individuele restore verzoeken kan worden voldaan;
- Back-ups dienen dagelijks te worden gecontroleerd door leverancier en bij foutmeldingen dient door leverancier direct actie te worden ondernomen;
- Leverancier is verantwoordelijk voor het leveren van exceptie-rapportage op basis van failed back-ups (per geval);
- Jaarlijks worden minimaal 2 restore testen uitgevoerd door leverancier;
- Leverancier test jaarlijks de disaster recovery procedure.

#### **Aansturing leverancier inclusief overlegstructuur**

De basis voor de aansturing en samenwerking daarvoor wordt in de overeenkomst en SLA vastgelegd, maar in de dagelijkse operatie zal de regie vanuit het Commissariaat voor de Media worden uitgevoerd door de IT-adviseur.

De demand- en regieorganisatie zijn bij het Commissariaat voor de Media gelegen binnen de subafdeling ICT van de afdeling Bestuurs- en Organiszakzen. Binnen de organisatie wordt voorzien in het aansturen van demand en supply op de volgende niveaus:

- Strategisch, door de IT-adviseur in afstemming met de directeur Bestuurs- en organisatiezakzen middels:
  - het vormgeven van ICT-beleid;
  - het initiëren van projecten;
  - ICT-inkoop- en leveranciersmanagement.
- Tactisch, door de IT adviseur middels:
  - het bewaken en sturen op key performance indicatoren (KPI's);
  - programmamanagement bij meerdere ICT-verander- en vernieuwingsprojecten;
  - contractmanagement;
- Operationeel, door de IT-adviseur middels:
  - het behandelen van, door outsourcepartner verstrekte, servicerapportages;
  - en het bewaken van bedrijfskritische incidenten.

## **Eisen aan de transitie**

- Voor zover mogelijk worden zaken, gezien vanuit de gebruikers, binnen het Commissariaat voor de Media gehandhaafd, minimaal zijn/haar opgeslagen bestanden, contacten, mails, Outlook mappen en Outlook geschiedenis, etc.;
- De gegevens in de huidige back-ups moeten worden overgenomen;
- Voor het project dient de Opdrachtnemer een projectmanager aan te stellen die zorgdraagt voor alle benodigde werkzaamheden, contacten tussen partijen coördineert en aanwezig is op de benodigde periodieke overleggen op locatie van de Opdrachtgever. De projectbegeleiding dient te bestaan uit een verantwoordelijke deskundige die de Nederlandse taal goed machtig is en in staat is om in voldoende mate te communiceren met derdelijns specialisten;
- Direct na ondertekening van de overeenkomst zal de leverancier aanvangen met de werkzaamheden in het kader van deze opdracht;
- Tijdens de transitie dienen maatregelen genomen te worden om de gevolgen van calamiteiten te mitigeren;
- Risico's met betrekking tot een verlaagde beschikbaarheid of kansen van uitval dienen zoveel mogelijk te worden beperkt;
- Leverancier dient aan te geven aan welke eisen van beheer voor of tijdens de transitiefase eventueel niet of niet geheel kan worden voldaan en na welke periode volledig wordt voldaan aan alle in dit document genoemde eisen met betrekking tot het beheer;
- De live gang na transitie zal als geheel (alles in één keer) plaatsvinden. Na live gang wordt de leverancier verantwoordelijk voor het beheer van de gevraagde dienstverlening;
- Na live gang dient de leverancier te voldoen aan de gestelde eisen, wensen en servicelevels zoals gesteld in deze offerteaanvraag;
- Leverancier dient te voorzien in een fallback scenario, waarbij het mogelijk is om wijzigingen in de transitie ongedaan te maken.

## **Bijlage 1 : Overzicht software en SaaS diensten**

### **Azure Servers:**

1 x Windows AD domain controller, NPS, CA, File Server  
1 x Windows AD domain controller, NDES  
1 x AlwaysOn VPN Server  
1 x SQL database server SafeQ, ADFS  
Djuma Synchronisatie Services  
1 x ADFS voor Legal Intelligence (evt. ook AFAS, Djuma)  
1 x Printserver

### **Netwerk:**

Watchguard firewall  
6 Aruba switches  
Internetverbinding via KPN EEN MKB Excellence fiber (1Gb) + backuplijn via Ziggo  
Diverse domeinregistraties en SSL certificaten

### **Werkplek:**

Plusminus 65 werkplekken  
HP Elitebook X360  
HP Thunderbolt G2 docking station  
Beheer via AutoPilot / Intune  
Conditional Access / Always on VPN  
Office 365 (Exchange, OneDrive, Teams, SharePoint)  
FSecure Antivirus

### **Licenties:**

Licenties zijn eigendom van het Commissariaat voor de Media (aanschaf gaat via leverancier)  
Office 365 E3 en Enterprise Mobility Suite + Security E3 (CSP)  
Windows 10 Pro

### **Software**

*Alle laptops zijn voorzien van:*

Adobe Acrobat Reader  
F-secure  
MS New Edge  
MS Office 365 Proplus (x64)  
HP Tool & Thunderbolt Docking drivers  
Google Chrome  
Citrix receiver  
VLC Media player  
7-Zip

*Enkele laptops zijn voorzien van :*

IBM SPSS  
Docscorp Cleandocs  
Adobe Standard Edition  
Hunchly Auditing  
NCH Debut

### **SaaS-diensten die worden afgenomen :**

TimeTell

Djuma zaaksysteem  
AFAS Insights  
Exact Online  
Filecloud  
iBabs  
Legal Intelligence  
Elvy  
Waar mogelijk wordt er gebruik gemaakt van SSO via Azure AD

### **Printers**

De lease van de printers is bij een derde partij ondergebracht. Het onderhoud van de printers valt buiten de scope van de opdracht. Het onderhoud van de printerserver en de uitrol van de juiste software en de installatie van de printers op de werkplekken behoren wel bij de werkzaamheden van de leverancier evenals het communiceren met de derde partij in geval van problemen.

### **(Mobiele) telefonie**

De vaste en mobiele telefonie zijn ondergebracht bij een derde partij en valt buiten de scope van de opdracht. Het inrichten van mobiele telefoons wordt echter niet door deze derde partij gedaan en zal door de leverancier worden uitgevoerd.

### **Wifi**

Het Wifi netwerk is ook uitbesteed aan een derde partij en valt buiten de scope van de opdracht. Van leverancier wordt wel de volledige medewerking verwacht in geval van storingen met het Wifi netwerk als er indicaties zijn die duiden op problemen met de onderliggende infrastructuur.

## Bijlage 2: Schematische beschrijving huidige IT-omgeving

