

Bijlage: Programma van Eisen



Inhoudsopgave

1	Inleiding	4
2	Algemene eisen	4
3	Technische uitgangspunten en eisen i.r.t. capaciteit en prestaties.....	4
3.1	Infrastructuur Architectuur.....	4
3.2	Werkplekken en mobiele devices	5
3.3	Serverlaag.....	5
3.4	Lokale server binnen Lopik	5
3.5	Test- en acceptatieomgeving	6
3.6	Proeftuinomgeving.....	6
3.7	Storagelaag binnen het datacentrum van de leverancier	6
3.8	Internet verbinding & firewall binnen het datacentrum van de leverancier	6
3.9	Security en informatiebeveiliging	7
4	Ontwerp, installatie, configuratie, migratie, testen en implementatie back- en frontend	9
4.1	Algemeen	9
4.2	Virtuele werkplek via desktop- en applicatievirtualisatie op basis van SBC.....	9
4.3	Applicaties.....	10
4.4	WAN	10
4.5	LAN	11
4.6	Beheervoorzieningen	11
4.7	Opslagvoorzieningen.....	11
4.8	Back-up en restore voorzieningen	11
4.9	Remote access voorzieningen/thuiswerken	12
4.10	E-mail-, contactpersonen- en agendasyndronisatie	12
4.11	Beveiliging	12
4.12	Multifunctionals	13
4.13	SaaS-leveranciers/hosting door derden.....	13
4.14	Koppelingen	13
5	Documentatie.....	13
6	Software en licenties (gebruikersrecht)	13
7	Technisch beheer.....	14
8	Service, support & onderhoud	14
8.1	Algemene eisen.....	14
8.2	Helpdesk.....	15

8.3	Servicelevelmanagement inclusief rapportage.....	15
8.4	Self Service Portal	16
9	Onsite support.....	16

1 Inleiding

De in dit document opgenomen eisen zijn bedoeld als nadere aanvulling en/of invulling op de minimale vereiste functionaliteit en kwaliteit van de leveringen en dienstverlening zoals omschreven in het Aanbestedingsdocument. Het streven van gemeente Lopik is om zoveel mogelijk standaarddiensten af te nemen c.q. aan te sluiten op de standaard van de leverancier.

2 Algemene eisen

1. Alle voor de dienstverlening benodigde backend hardware (servers, netwerkcomponenten, opslagvoorzieningen, etc.) die de leverancier voor het leveren van de diensten inzet, dienen onderdeel uit te maken van deze geleverde dienstverlening.
 - a. Uitzondering hierop is de (additionele) routing/firewall netwerkapparatuur benodigd ten behoeve van de redundante WAN-koppeling tussen het datacentrum en de gebouwlocatie aan het Raadhuisplein te Lopik.
 - b. De reeds in gebruik zijnde netwerkcomponenten op de gebouwlocaties van gemeente Lopik voor het LAN zijn nog niet economisch en technisch gezien afgeschreven. De leverancier is niet verantwoordelijk voor de levering van nieuwe switches/access points.
2. De te leveren software is in de praktijk bewezen programmatuur.
3. Alle te leveren voorzieningen dienen te voldoen aan de Arbowetgeving.
4. Gemeente Lopik is en blijft te allen tijde eigenaar van haar data.
5. De verantwoordelijkheid voor een correcte opslag conform wet- en regelgeving alsmede in technische zin van data van applicaties die geïnstalleerd zijn in de nieuwe ICT-omgeving, ligt bij de leverancier.
6. Alle data in de nieuwe ICT-omgeving dient ongeacht de wijze van hosting in Europese lidstaat opgeslagen te worden conform Europese wetgeving.
7. Er dient voldaan te worden aan relevante wet- en regelgeving (onder andere Archiefwet en de AVG).

3 Technische uitgangspunten en eisen i.r.t. capaciteit en prestaties

3.1 Infrastructuur Architectuur

8. De leverancier dient een overall Infrastructuur Architectuur voor gemeente Lopik uit te werken.
9. De leverancier dient de Infrastructuur Architectuur in detail te beschrijven door het opleveren van Technische Ontwerpen. De leverancier is vrij in de keuze van het aantal Technische Ontwerpen en het onderwerp van een Technisch Ontwerp, zolang de optelsom van de Technische Ontwerpen de volledige Infrastructuur Architectuur beschrijft.
10. De technische ontwerpen dienen geschreven te worden op zodanig een detail niveau dat een gespecialiseerde partij de ontwerpen kan begrijpen en toetsen.
11. In elk van de Technische Ontwerpen dient de leverancier onder meer de volgende onderwerpen te beschrijven:
 - a. De plaats van het Technisch Ontwerp in de Infrastructuur Architectuur
 - b. De relatie tussen het specifieke Technisch Ontwerp en andere Technische Ontwerpen
 - c. De functionele eisen en requirements van gemeente Lopik die door het betreffende Technisch Ontwerp gerealiseerd worden
 - d. De principes en ontwerpregels die zijn gehanteerd bij het ontwerp en evt. verwijzingen naar de ontwerpregels van een fabrikant
 - e. De overwegingen, keuzes en aannamen waarop het ontwerp gebaseerd is

- f. De specificatie van gebruikte hard- en/of software inclusief aangeboden type, sizing en versie aanduidingen
- 12. Daarnaast dient de leverancier in elk van de Technische Ontwerpen in detail in te gaan op de volgende infrastructurele kwaliteitsaspecten:
 - a. Beschikbaarheid (onder meer redundancy options & SPOF's)
 - b. Performance (onder meer verwerkingscapaciteit en potentiële performance bottlenecks)
 - c. Schaalbaarheid (op basis van licentie, additionele hardware of vervanging van hardware)
 - d. Beheerbaarheid (eenvoud van administratie, monitoring van de goed werking)
 - e. Beveiliging (toegang, permissies en logging)
- 13. Alle ontwerpen zullen vooraf getoetst en goedgekeurd worden door gemeente Lopik, of een door gemeente Lopik in te schakelen derde partij.
- 14. De implementatie zal niet aanvangen voordat het betreffende technisch ontwerp goedgekeurd is.
- 15. De infrastructuur kent een minimum aan "single point of failures" (SPOF). De resterende SPOF's zijn benoemd en hiervoor is een herstelplan opgesteld en op eerste verzoek ter inzage beschikbaar voor gemeente Lopik.

3.2 Werkplekken en mobiele devices

- 16. De virtuele werkplek functioneert op de werkplekken hardware (desktops, workstations, laptops en thin clients) van de gemeente Lopik.
- 17. Onbekende en daarmee onvertrouwde end-points, zoals niet door gemeente Lopik beheerde end-points, die gebruik moeten kunnen maken van de virtuele werkplek mogen geen beveiligingsrisico's te vormen.

3.3 Serverlaag

- 18. Uitgangspunt voor de backend servers is Windows Server 2019, tenzij het technisch niet anders mogelijk is. Afwijking van dit uitgangspunt vereist voorafgaande toestemming van de gemeente Lopik.
- 19. Er wordt zoveel mogelijk gebruik gemaakt van server virtualisatie.
- 20. De capaciteit van de omgeving dient dermate geschaald te zijn, dat bij calamiteiten (zoals uitval van hardware) de impact naar de gebruikers minimaal is. De baseline betreft 150 gebruikers.
- 21. De infrastructuur voorziet in de mogelijkheid om wijzigingen, zonder impact op de productieomgeving, te testen en selectief te verstrekken aan een groep gebruikers.
- 22. Werkplekken en applicaties worden primair door middel van applicatievirtualisatie (server-based hosted apps) ontsloten. Daar waar virtualisatie technisch niet mogelijk of zinvol is, worden applicaties na uitdrukkelijke toestemming van gemeente Lopik geschikt gemaakt voor andersoortige automatische distributie/installatie op het endpoint. Gemeente Lopik heeft circa 10 fat clients/desktops in gebruik ten behoeve van zwaardere applicaties zoals AutoCAD en InfraCAD.

3.4 Lokale server binnen Lopik

- 23. Leverancier levert, installeert, configureert, beheert en onderhoud één lokale server op locatie voor gemeente Lopik ten behoeve van de volgende functies:
 - HP/Dell/overig Device Manager t.b.v. beheer van de thin clients
 - WSUS of ander gelijksoortig systeem voor het op centraal niveau en op afstand kunnen uitrollen van updates/upgrades van het lokale Windows OS.
 - DHCP
 - Print server
 - Netwerkshare – Dis4all\$

3.5 Test- en acceptatieomgeving

24. De leverancier levert, onderhoudt en beheert een permanente TA-omgeving gedurende de looptijd van de Overeenkomst. Het dient een representatieve en geactualiseerde kopie te zijn van de productieomgeving met dien verstande dat er geen performance-eisen gelden.

3.6 Proeftuinomgeving

25. De leverancier levert, onderhoudt en beheert een permanente proeftuin-omgeving gedurende de looptijd van de Overeenkomst. Het dient een kleine representatieve en geactualiseerde kopie te zijn van de productieomgeving met dien verstande dat er geen performance-eisen gelden.

3.7 Storagelaag binnen het datacentrum van de leverancier

26. De storage is in termen van capaciteit op en af schaalbaar
27. De storage is afgestemd op de toepassing. Voor de virtuele werkplek is bijvoorbeeld voldoende IOPS en een beperkte latency van cruciaal belang voor een goede gebruikerservaring.
28. Voor storage waar geen hoge eisen aan gesteld worden (bijvoorbeeld voor archivering), is een alternatieve, meer kosteneffectieve opslagmogelijkheid beschikbaar.
29. De storage is dusdanig gekozen en ontworpen dat de performance ook in de toekomst, met tussentijdse op- en afschalen tot een maximum van 50% ten opzichte van de uitgangssituatie bij acceptatie, gewaarborgd blijft.

3.8 Internet verbinding & firewall binnen het datacentrum van de leverancier

30. De firewall infrastructuur voorziet in de volgende taken:
 - a. Controleert de informatiestromen tussen de aangesloten netwerken en partijen
 - b. Beslist op basis van regels (Security Policy) welke informatiestromen mogen worden doorgelaten, dan wel moeten worden tegengehouden
 - c. Handhaaft de privacy van de IT omgeving van gemeente Lopik ten opzichte van de buitenwereld
 - d. Logt en rapporteert pogingen om niet-geautoriseerde informatiestromen tot stand te brengen
 - e. Zorgt voor voldoende ontkoppeling van de aangesloten netwerken.
31. gemeente Lopik hanteert het principe dat communicatie niet mag, tenzij deze communicatie expliciet is toegestaan.
32. DPI-SSL is gewenst voor het decrypten c.q. controleren van SSL verkeer.
33. Het is mogelijk om al het verkeer wat over de externe firewall gaat te controleren op basis van technieken zoals IPS en URL filtering.
34. Voor de Internet verbinding en firewall gelden de volgende uitgangspunten:
 - a. De firewall infrastructuur bestaat uit een externe firewall en interne firewall
 - b. De externe en interne firewall mogen virtueel zijn
 - c. De firewall infrastructuur en de Gemnet/GGI-verbinding dienen redundant uitgevoerd te worden
 - d. De externe firewall bepaald verkeersstromen tussen gemeente Lopik en de buitenwereld, waaronder Internet en leveranciers van diensten
 - e. De interne firewall bepaald de verkeerstromen tussen netwerksegmenten binnen gemeente Lopik;
 - f. De interne firewall mag geen (performance) bottleneck vormen voor intern verkeer inclusief client-server, server-server, storage-storage en server-storage verkeer
 - g. De externe firewall mag geen (performance) bottleneck vormen voor verkeer tussen gemeente Lopik en de buitenwereld.
35. De aangeboden firewall dient alle gangbare Internet protocollen en toepassingen te ondersteunen. Het doorgeven of blokkeren kan per toepassing en/of protocol worden ingesteld. Gangbare toepassingen en protocollen op dit moment zijn onder meer:
 - a. Netwerk protocollen (zoals smtp, http, https, ftp, s-ftp, dns, ntp, ldap)

- b. Social media en Instant Messaging (zoals Facebook, Google+ en Skype)
 - c. Filesharing (zoals Dropbox, Skydrive, Google Drive)
 - d. Peer2Peer (zoals FastTrack, Kazaa, Edonkey, BitTorrent, Gnutella)
 - e. Streaming Audio en Video (zoals Youtube, Spotify, Netflix, iTunes).
36. De leverancier dient tegelijkertijd IPv4 en IPv6 te ondersteunen;

3.9 Security en informatiebeveiliging

Met betrekking tot Informatiebeveiliging worden door de gemeente de kaders gevolgd uit de Baseline Informatiebeveiliging Overheid (BIO). Deze baseline is opgezet rondom bestaande normen; de NEN/ISO 27002:2007 en NEN/ISO 27001:2013.

37. Leverancier dient deze normen te herkennen, erkennen en op zo kort mogelijke termijn te implementeren wanneer vereist op grond van de BIO.

Security

- 38. Misbruik (gebruik van Internet) moet op persoonsniveau te herleiden zijn.
- 39. Voor authenticatie wordt gebruik gemaakt van Microsoft Active Directory (AD).
- 40. Een gebruiker dient éénmalig een gebruikersnaam en wachtwoord in te vullen om toegang te krijgen tot de uiteindelijke sessie.
- 41. Waar mogelijk wordt gebruik gemaakt van Single Sign On.
- 42. De omgeving wordt pro-actief voorzien van de laatste beveiligingspatches voor alle software en OS componenten.
- 43. De virtuele werkplek is “read-only” (ook wel non-persistent of stateless genoemd). Wijzigingen worden zodoende niet opgeslagen met uitzondering van gebruikersconfiguratie (profiel) en applicatiedata.
- 44. Gebruikers kunnen zelf/handmatig geen software installeren of verwijderen. Bevoegde medewerkers kunnen wel via de Self Service Portal software toevoegen dan wel verwijderen aan zichzelf of andere gebruikers.
- 45. Gebruikers hebben alleen toegang tot software waar zij voor geautoriseerd zijn.
- 46. Standaard dient twee-factor authenticatie geconfigureerd en geactiveerd te zijn voor de volledige infrastructuur, o.a.:
 - a. Login werkplek
 - b. Groupware/Office365 (inclusief webmail)

Informatiebeveiliging

- 47. Leverancier heeft een actueel informatiebeveiligingsbeleid.
- 48. Leverancier geeft jaarlijks een TPM-verklaring 27001/ENSIA (zie: <https://2-control.nl/nl/it-audit/tpm-verklaring/>) af.
 - a. Leverancier voert als onderdeel hiervan jaarlijks zowel een penetratie- als vulnerability test uit om de omgeving.
- 49. Leverancier houdt logbestanden bij van informatiebeveiligingsincidenten m.b.t. de gemeente Lopik.
- 50. Leverancier houdt een logging bij van systeemgebruik. De volgende gebeurtenissen worden in ieder geval opgenomen in de logging:
 - Gebruik van technische beheerfuncties, zoals het wijzigen van configuratie of instellingen; uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore.
 - Gebruik van functioneel beheerfuncties, zoals het wijzigen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases).
 - Handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoord reset, uitgifte en intrekken van cryptosleutels.

- Beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services).
 - Verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen).
 - Handelingen van gebruikers, zoals goede en foute inlogpogingen.
 - Systeemtoegang, gebruik van online transacties en toegang tot bestanden.
51. Leverancier heeft maatregelen getroffen voor detectie, preventie en herstel om te beschermen tegen virussen.
 52. Bij het openen van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, automatisch plaats.
 53. Inkomende en uitgaande e-mails worden gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, (automatisch) plaats.
 54. Er zijn maatregelen om verspreiding van virussen tegen te gaan en daarmee schade te beperken (bijv. quarantaine en compartimentering).
 55. Leverancier heeft continuïteitsplannen voor herstel na aanvallen met virussen waarin minimaal maatregelen voor back-ups en herstel van gegevens en programmatuur zijn beschreven.
 56. Er behoren back-up kopieën van informatie en programmatuur te worden gemaakt en regelmatig te worden getest overeenkomstig een door de Leverancier ingesteld back-upbeleid.
 57. Er zijn (geteste) procedures voor back-up en recovery van informatie voor herinrichting en foutherstel van verwerkingen.
 58. Het netwerk wordt gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de betrouwbaarheid van het netwerk niet onder het afgesproken minimum niveau komt.
 59. Gegevensuitwisseling tussen vertrouwde en onvertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware.
 60. Bij transport van vertrouwelijke informatie over onvertrouwde netwerken, zoals het internet, dient altijd geschikte encryptie te worden toegepast.
 61. Leverancier heeft een actueel wachtwoordenbeleid:
 - De toewijzing van wachtwoorden behoort met een formeel beheerproces te worden beheerst.
 - Wachtwoorden worden op een veilige manier uitgegeven (controle identiteit van de gebruiker).
 - Tijdelijke wachtwoorden of wachtwoorden die standaard in software of hardware worden meegegeven worden bij eerste gebruik vervangen door een persoonlijk wachtwoord.
 - Gebruikers bevestigen de ontvangst van een wachtwoord.
 - Wachtwoorden zijn alleen bij de gebruiker bekend.
 - Wachtwoorden bestaan uit minimaal 10 karakters, waarvan tenminste 1 hoofdletter, 1 cijfer.
 - Wachtwoorden zijn maximaal 60 dagen geldig en mogen niet binnen 6 keer herhaald worden.
 62. Leverancier beheert fysieke en logische toegang tot poorten voor diagnose en configuratie.
 63. Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.
 64. Toegang tot besturingssystemen behoort te worden beheerst met een beveiligde inlogprocedure.
 65. Systemen voor wachtwoordbeheer behoren interactief te zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.

4 Ontwerp, installatie, configuratie, migratie, testen en implementatie back- en frontend

66. Leverancier stelt, in een verplichte nazorgfase van ten minste 2 kalendermaanden, tenminste 16 uren in de week beschikbaar aan medewerkers voor nazorg op locatie in Lopik. Het betreft tenminste een medewerker van de leverancier die aantoonbaar onderdeel uitmaakte van het projectteam van de transitiefase.

4.1 Algemeen

67. De leverancier is verantwoordelijk voor:
- het opstellen van het ontwerp en projectplan voor realisatie van de nieuwe omgeving
 - volledige inrichting van de back- en frontend
 - migratie van de data en programmatuur op de bestaande (virtuele) servers naar de nieuwe infrastructuur
 - implementatie van een desktop & applicatie delivery omgeving
 - packaging en distributie van applicaties
 - projectleiding, -uitvoering en advisering
 - inrichten beheerorganisatie

4.2 Virtuele werkplek via desktop- en applicatievirtualisatie op basis van SBC

68. De virtuele werkplek biedt de mogelijkheid om automatische vergrendeling van een sessie, die een bepaalde tijd inactief is, af te dwingen (door middel van een centraal in te stellen policy). Vanzelfsprekend moet de gebruiker van de sessie deze kunnen ontgrendelen (met behulp van de van toepassing zijnde authenticatiemethode).
69. De virtuele werkplek ondersteunt de mogelijkheid voor het aansluiten van meer dan één monitor.
70. De werkplekervaring dient op alle werkplekken hetzelfde te zijn ongeacht waar de gebruiker zich bevindt mits de gebruiker de beschikking heeft over voldoende kwaliteit internetverbinding.
71. De virtuele werkplek moet de mogelijkheid bieden om gebruiker gebonden instellingen op te slaan zodat deze weer kunnen worden hergebruikt wanneer de gebruiker opnieuw zijn werkplek opstart. Het profiel van de gebruiker wordt derhalve centraal opgeslagen, waardoor persoonlijke instellingen van de gebruiker werkplek onafhankelijk zijn.
72. De virtuele werkplek van een gebruiker ondersteunt het aansluiten en gebruiken van randapparatuur, zoals minimaal USB gebaseerde randapparatuur (zoals beeld- en geluidsapparatuur ten behoeve van Microsoft Teams/Zoom/Google Meet/etc) en monitoren.
73. De virtuele werkplek ondersteunt netwerkprinters alsmede multifunctionals.
74. De virtuele werkplek bevat functionaliteit om voor elke gebruiker een unieke combinatie van wachtwoord en loginnaam af te dwingen.
75. De virtuele werkplek biedt functionaliteit om bij gedetecteerd misbruik (aantal login fouten), die een in te stellen drempelwaarde overschrijdt, de toegang tot het systeem te blokkeren en automatisch een alert te geven.
76. De virtuele werkplek biedt de mogelijkheid voor een gebruiker om een sessie te vergrendelen zodat anderen geen toegang tot de computer kunnen krijgen en of informatie kunnen lezen (schermbeveiliging). Vanzelfsprekend moet dezelfde gebruiker ook weer de sessie kunnen ontgrendelen (met behulp van zijn loginnaam en wachtwoord).
77. De virtuele werkplek biedt de mogelijkheid om een vergrendelde sessie te laten ontgrendelen door een beheerder, die daarvoor speciale rechten heeft toegekend gekregen.

78. Voor gebruikersondersteuning dient schermovername op afstand mogelijk te zijn (ook door interne beheerteams en externe/derde leveranciers). Het scherm mag pas overgenomen worden na expliciete toestemming van de gebruiker.
79. Wijzigingen welke door de gebruiker gemaakt worden gedurende een sessie dienen bewaard te blijven en weer toegepast worden wanneer de gebruiker weer opnieuw inlogt.
80. Gebruikers dienen automatisch eventuele afdelingsschijven en homefolders toegekend te krijgen tijdens het opbouwen van een sessie.

4.3 Applicaties

81. Alle type applicaties dienen gepackaged dan wel geprepareerd te kunnen worden, zodat deze binnen de aan te bieden virtuele werkplek beschikbaar zijn en gebruikt kunnen worden.
82. Reeds beschikbare licenties van gemeente Lopik waarvan de nieuwe leverancier gebruik dient te maken: Microsoft Office 365 E3 (per Q3/Q4 2020)
83. De huidige in gebruik zijnde applicaties (per medio 2020) opgenomen in de bijlage dienen beschikbaar te zijn binnen/op de virtuele werkplek van de gebruiker van gemeente Lopik middels desktop- en applicatievirtualisatie op basis van SBC. Deze lijst zal na contractering nader afgestemd worden met de leverancier en kan daarmee nog wijzigen voor wat betreft het aantal en het type applicaties dat beschikbaar gesteld moet worden.
84. De gebruiker moet multimedia (Rich Media Applications, zoals Adobe Flash/Shockwave Player, Microsoft Silverlight, et cetera) zonder haperingen kunnen ervaren in de virtuele werkplek, waarbij het uitgangspunt voor de leverancier is dat de gebruiker de beschikking heeft over voldoende kwaliteit/breedbandige internetverbinding.
85. Voor wat betreft de rendering eist gemeente Lopik een oplossing die gedimensioneerd is waarbij de rendering binnen de lokale werkplekken hardware plaatsvindt. De nieuwe leverancier mag ervan uitgaan dat in de nabije toekomst en voor acceptatie van de nieuwe omgeving alle werkplekken hardware vervangen wordt door de gemeente. De leverancier dient te zijner tijd hiervoor de minimale hardware specificaties voor wat betreft o.a. de cpu-prestaties, gpu-prestaties en hoeveelheid werkgeheugen te verstrekken.
86. Mogelijkheid tot het blokkeren van applicaties door de beheerpartij.
87. Een gebruiker kan alleen applicaties opstarten op basis van toegekende rechten. Het startmenu dient alleen de applicaties te tonen waar de gebruiker rechten toe heeft (doel: het voorkomen van toegang tot en gebruik van ongeautoriseerde applicaties).
88. De virtuele werkplek en de bijbehorende standaard applicaties van een gebruiker heeft een volledig Nederlandstalige interface.
89. Aangeboden applicaties moeten kunnen worden gestart op basis van vooraf gedefinieerde bestands-typen en/of extensies.

4.4 WAN

90. De leverancier is verantwoordelijk voor de coördinatie en realisatie van WAN-verbinding(en) tussen het in te zetten datacentrum en het LAN van gemeente Lopik. Dit betekent dat de leverancier coördineert dat de huidige EVPN, bij KPN met gemeente Lopik als contracthouder, wordt aangesloten tussen het datacentrum en het LAN van de gemeente Lopik aan het Raadhuisplein 1, 3411 CH te Lopik. De WAN-verbinding betreft een redundante EVPN-verbinding met een minimale bandbreedte van tenminste 500 Mbps. Gemeente Lopik blijft/wordt contracthouder van deze verbinding. Gezien de relatief lange doorlooptijd van dergelijke trajecten vangt de leverancier direct na ondertekening aan met het aanvragen van deze verbinding namens gemeente Lopik.
91. Voor alle overige gebouwlocaties verzorgt de leverancier de beveiligde logische connecties van en naar het datacentrum over de reeds in gebruik zijnde fysieke dataverbindingen.

92. Leverancier verzorgt tevens de internetdienstverlening vanuit het datacentrum ten behoeve van in ieder geval de gebouwlocatie aan het Raadhuisplein te Lopik. De beschikbare internetbandbreedte bedraagt ten minste 300 Mbps, symmetrisch. Al het internetverkeer dient in principe via het datacentrum en de bijbehorende firewall(s) te verlopen.
93. De Gemnet/GGI-aansluiting dient bij voorkeur ook via het datacentrum te verlopen.
94. Leverancier levert, installeert, configureert de (additionele) routing/firewall netwerkkapparatuur benodigd ten behoeve van de redundante WAN-koppeling tussen het datacentrum en de gebouwlocatie aan het Raadhuisplein te Lopik. Hiervoor is de leverancier end-to-end verantwoordelijk. De benodigde routing/firewall-capaciteit ruimschoots dient voldoende capaciteit heeft gedurende de looptijd van de overeenkomst, rekening houdend met groeiend dataverkeer. Internet access wordt door de nieuwe leverancier via het datacentrum (t.b.v. de beveiliging) van de leverancier aan gemeente Lopik geleverd.

4.5 LAN

95. Leverancier is verantwoordelijk voor de configuratie en het testen van de netwerkkapparatuur en koppelvlakken tussen het datacentrum-, de WAN- en (W)LAN-netwerken.

4.6 Beheervoorzieningen

96. Vanuit het beheer van de virtuele werkplek moet selectief kunnen worden vastgesteld welk apparaat type wel of niet kan worden gebruikt door een gebruiker. Voorbeelden van type apparaten zijn: lokale printers, netwerkprinters, opslag lezen, opslag lezen en schrijven, lokale vaste opslag, lokale externe verwijderbare opslag (o.a. USB, kaartlezers), alle opslag, alle USB-apparatuur.
97. Indien gebruik wordt gemaakt van een virtuele werkplek vanaf een willekeurige (fysieke) werkplek buiten het netwerk van gemeente Lopik dan mogen de, op de (fysieke) werkplek aanwezige malware, spyware en virussen de functionaliteit van de virtuele werkplek niet aantasten of beïnvloeden.
98. Er mogen geen gegevens achterblijven op het (fysieke) apparaat dat wordt gebruikt om de virtuele werkplek te presenteren. Dit geldt minimaal voor applicatiegegevens, gebruikersdata en gegevens over de sessie, wachtwoorden en gebruikersnamen. Een uitzondering hiervoor geldt voor niet-beheerde devices.

4.7 Opslagvoorzieningen

99. Dataopslag van gemeente Lopik vindt in beginsel plaats in de Microsoft Office 365 omgeving van de gemeente.
 - a. Specifieke applicatie- dan wel infrastructuur gebonden opslagvoorzieningen (zoals bijbehorende databases, opslag ten behoeve van de werking van de backend infrastructuur, dan wel bestandenopslag op binnen de applicatieservers, etc.) dienen vanzelfsprekend niet gemigreerd te worden naar Microsoft Office 365.
 - b. De documenten opgeslagen binnen het DMS/RMA-systeem van de gemeente dienen niet binnen Microsoft Office 365 opgeslagen te worden.

4.8 Back-up en restore voorzieningen

100. Er dient één centrale back-up oplossing aangeboden te worden die een volledige back-up kan maken, inclusief de volledige Office365-omgeving van gemeente Lopik (waaronder Sharepoint, Teams, Exchange, etc.) en de lokale server bij gemeente Lopik (zie eis 23).
101. Voor alle servers dient een disaster recovery ingericht te worden.
102. In het kader van het tijd- en plaats-onafhankelijk werken dienen de back-up windows zo klein mogelijk gehouden te worden en bij voorkeur in de nachtelijke uren. In de avonduren mag er geen performance downgrade optreden in verband met de verschillende back-up policies.

103. Individuele bestanden, applicaties en databases moeten te herstellen zijn, naar de originele locatie en naar een andere op te geven locatie.
104. Ten aanzien van het back-up beleid gelden de volgende minimale retentietijden:
- | | |
|---|-----------|
| a. 1 - jaar back-up | : 2 jaar |
| b. 2 - maand back-up | : 1 jaar |
| c. 3 - full back-up | : 4 weken |
| d. 4 - incrementele / differentiële back-up | : 4 weken |

4.9 Remote access voorzieningen/thuiswerken

105. Voor alle medewerkers is:
- a. via een webbrowser, o.b.v. Microsoft Office 365 en aan de hand van 2-factor authenticatie i.c.m. softwarematige token toegang tot volledige werkplek, de volledige groupware functionaliteit beschikbaar (e-mail, agenda, contactpersonen, Teams etc.) van gemeente Lopik extern via het internet benaderbaar zonder dat een speciale (VPN)-verbinding hoeft opgezet te worden.
 - b. via een desktop- en applicatievirtualisatieclient is de gemeente Lopik werkplek benaderbaar (o.b.v. 2-factor authenticatie i.c.m. softwarematige token toegang tot volledige werkplek)
 - i. 50 gelijktijdige gebruikers / 125 unieke gebruikers
106. Via remote access dient de virtuele werkplek van een medewerker via het internet toegankelijk te zijn.
107. Knippen en plakken tussen applicaties onderling op de virtuele werkplek, vanuit de virtuele werkplek naar applicaties naar het onderliggende apparaat en andersom is niet toegestaan.
108. Lokaal (op de onderliggende client hardware zoals de laptops, thin client, desktop computer of mobiele apparaat) aanwezige/aangesloten randapparatuur, zoals printers, externe opslag, USB-apparatuur, beeld- en geluidsapparatuur ten behoeve van Microsoft Teams/Zoom/Google Meet/etc. moeten vanuit virtuele werkplek omgeving kunnen worden benaderd en gebruikt mits dit expliciet is toegestaan door gemeente Lopik. Toestemming is op groeps- en gebruiksniveau in te stellen.

4.10 E-mail-, contactpersonen- en agendasyndronisatie

109. Microsoft Office 365 (desktopversies van Office-apps, niet webversies) als kantoorautomatiseringssoftware moet beschikbaar zijn (licenties via gemeente Lopik) binnen de virtuele werkplek.

4.11 Beveiliging

110. De beveiligingssoftware van de virtuele werkplek is beschermd tegen alle mogelijke risico's zoals benoemd in de BIO. De beveiligingssoftware voldoet in alle aspecten aan de eisen zoals gesteld in de BIO en voorziet in programma(s) ten behoeve van:
- a. Bescherming tegen fishing/ cryptolocking/etc.
 - b. Bescherming/detectie tegen virussen, internetwormen en trojans.
 - c. Het filteren van in- en uitgaand verkeer middels een (personal) firewall.
 - d. Encryptie van data.
 - e. Actieve detectie en alarmering op verandering van systeembestanden en verdacht systeemgedrag.
111. De beveiligingssoftware dient centraal te worden beheerd waarbij de gebruikers de instellingen niet kunnen aanpassen.
112. De oplossing ondersteunt de mogelijkheid tot centraal instellen van de updatefrequentie van ten minste virustabellen en regels.
113. De beveiligingssoftware biedt permanente bescherming van processen en is ook in staat extern op de cliënt aangesloten apparaten via USB-poorten en andere poorten te scannen en te beveiligen.
114. De beveiligingssoftware is in staat het verkeer dat van en naar internet plaatsvindt vanaf de cliënt te scannen en tegen bedreigingen te beveiligen. Bijvoorbeeld als blijkt dat bij het openen van een webpagina

of downloaden van een bestand een bedreiging (bijvoorbeeld virus of ongewenste wijzigingen van de browserinstellingen) plaatsvindt deze te herkennen en te melden en te blokkeren.

115. De beveiligingssoftware biedt de mogelijkheid gedetecteerde virussen, internetwormen en trojans automatisch onschadelijk te maken en verspreiding verder tegen te gaan.

4.12 Multifunctionals

116. De huidige multifunctionals zijn van Canon (en in de toekomst via GT-Print van de VNG) en dienen in de nieuwe omgeving probleemloos te functioneren

117. De leverancier dient de multifunctionele printers te configureren binnen de infrastructuur gebruik makend van mogelijkheden van de software van Canon waarbij ten minste de volgende functionaliteiten worden gerealiseerd:

- a. Follow-me printing
- b. Beveiligd printen
- c. Toegangsbeveiliging gebaseerd op gebruikersgroepen

118. De officiële drivers van Canon dienen gebruikt te worden.

119. De functionaliteit van de huidige oplossing van Canon dient door de nieuwe omgeving ondersteund te worden. Gedacht moet worden aan scannen naar bestandslocatie, OCR opties et cetera.

120. De bestaande printers dienen in de nieuwe omgeving ondersteund te worden.

4.13 SaaS-leveranciers/hosting door derden

121. De leverancier verantwoordelijk voor het koppelvlak in de nieuwe ICT-infrastructuur aan de zijde van gemeente Lopik. Dit betekent dat de leverancier per applicatie in samenspraak met de applicatieprovider zorgdraagt voor de vereiste koppelingen, waarbij de leverancier alle benodigde aanpassingen in haar ICT-infrastructuur verzorgt.

4.14 Koppelingen

122. De leverancier is verantwoordelijk voor de inventarisatie, regie, uitvoering en realisatie m.b.t. alle benodigde koppelingen en de installatie, configuratie en implementatie (nieuwe koppelingen, updates/ testen en documentatie) van de koppelvlakken binnen haar ICT-infrastructuur.

5 Documentatie

123. De leverancier levert zowel de beheerdershandleidingen voor de I&A-afdeling alsmede de eindgebruikershandleidingen.

6 Software en licenties (gebruikersrecht)

124. Alle voor de dienstverlening benodigde programmatuur en licenties die de leverancier voor het leveren van de diensten inzet, dienen onderdeel uit te maken van deze geleverde dienstverlening.

- a. Uitzondering hierop zijn de volgende frontend licenties voor programmatuur die leverbaar zijn via gemeente Lopik als onderdeel van Microsoft Office 365 services.
- b. Microsoft Office 365 E3 licenties zijn reeds verworven en in gebruik door gemeente Lopik.
- c. Aanvullende Office 365 licenties, zoals maar niet uitsluitend Microsoft Windows 10 Enterprise/Microsoft Intune/Microsoft Enterprise Mobility + Security/Microsoft Azure Active Directory/Microsoft Azure Information Protection/Office 365 Advanced Threat Protection dient u buiten uw prijsopgave te laten, maar wel te specificeren, zodat gemeente Lopik volledige inzage

heeft in het totale aantal en type benodigde licenties en welke licenties er door de nieuwe leverancier geleverd worden dan wel door gemeente Lopik aangeschaft dienen te worden.

125. De te leveren software is in de praktijk bewezen standaardprogrammatuur.

7 Technisch beheer

126. De leverancier is verantwoordelijk voor het uitvoeren van het:

- a. serverbeheer
- b. storagebeheer
- c. netwerkbeheer (aan deze zijde van het datacentrum van de leverancier)
- d. databasebeheer
- e. back-up beheer
- f. anti-virus beheer

Van leverancier is een pro-actieve houding verwacht.

127. Het professioneel en op basis van ITIL technisch hosten en beheren van zowel de back- als frontend infrastructuur richt zich op het in stand houden, beheren en onderhoud van deze infrastructuur conform de minimale prestatienormen zoals opgenomen in de concept Service Level Agreement die ten tijde van de gunningfase beschikbaar wordt gesteld. De ICT-infrastructuur is de basis waarop applicaties kunnen draaien en bestaat uit het netwerk, de computer hardware, operating systems, beheer- en serversoftware en overige backup- en storage hardware.

128. Voor wat betreft de fysieke werplekken hardware op locatie van de gemeente is de leverancier ook verantwoordelijk voor het technisch beheer van het lokale besturingssysteem (Windows 10 of anders) alsmede de beveiliging. Dit beheer dient in principe gecentraliseerd, geautomatiseerd en op afstand via het netwerk plaats te vinden. In geval dat er applicaties lokaal geïnstalleerd dienen te worden, omdat dit technisch niet mogelijk is binnen de virtuele werkplek, is de leverancier ook verantwoordelijk voor het technisch testen, installeren, updaten en upgraden van deze applicaties, inclusief documentatie en de gemeente hierover tijdig te informeren.

129. Gemeente Lopik verzorgt zelf het beheer en onderhoud van het (W)LAN. Op afroep ondersteunt de leverancier hierin.

130. Gemeente Lopik is verantwoordelijk voor de stabiliteit en snelheid van het (W)LAN-netwerk alsmede het patchen van systemen en de (netwerk)componenten.

8 Service, support & onderhoud

8.1 Algemene eisen

131. De dienstverlening dient gebaseerd te zijn op ITIL. Er dient sprake te zijn van de volgende ITIL processen waarvoor leverancier verantwoordelijk is voor de uitvoering:

- a. incident, problem en change management
- b. gebruikers- en toegangsbeheer (identity & access management)
- c. configuratiemanagement, assetmanagement en lifecyclemanagement
- d. servicelevelmanagement inclusief rapportages
- e. event management
- f. capacity management
- g. security Management

2. Leverancier verzorgt het testen, de distributie en installatie van de updates en upgrades voor alle generieke applicaties op de virtuele werkplekken.
3. Delivery organisatie van de leverancier dient aan te sluiten op de I&A-organisatie van de gemeente Lopik.
4. Leverancier koppelt (bi-directioneel) haar eventuele service management tooling met die service management tooling van gemeente Lopik. De service management tooling van gemeente Lopik is leidend. De helpdesk registreert de meldingen, changes, service requests in de tool van gemeente Lopik namelijk TOPdesk. Leverancier gebruikt de service management tooling van gemeente Lopik voor de registratie van incidenten/problemen/vragen/klachten. Daarnaast kan een medewerker van gemeente Lopik via de Self Service Portal ook incidenten/problemen/vragen/klachten registreren dan wel aanvullen/reageren.

8.2 Helpdesk

132. Het op basis van ITIL registreren, oplossen en beantwoorden van incidenten, problemen en vragen met als doel het herstellen van verstoringen op een effectieve en efficiënte wijze, binnen de daarvoor gestelde service levels conform de opgenomen concept Service Level Agreement. Deze concept Service Level Agreement is opgenomen als onderdeel van de Gunningleidraad.
133. De helpdesk biedt een centraal meldpunt voor de ondersteuning van de medewerkers van gemeente Lopik ten aanzien van alle ICT-gerelateerde vragen. Voor alle meldingen, vragen en wensen moeten medewerkers terecht kunnen en zoveel mogelijk direct op weg geholpen worden. Alle meldingen worden geregistreerd, bewaakt en verwerkt in rapportages.
134. I&A-medewerkers van gemeente Lopik bellen of mailen de helpdesk van leverancier waar ze te woord worden gestaan door medewerkers die getraind zijn in de te ondersteunen producten van gemeente Lopik. De medewerkers moeten over de benodigde faciliteiten en kennis beschikken om tot een correcte en adequate afhandeling van de meldingen te komen. De volgende activiteiten worden in ieder geval uitgevoerd door de helpdesk van de leverancier:
 - Het via een centraal meldpunt, mail en telefoon ontvangen en registreren van meldingen van medewerkers met betrekking tot technische en functionele onvolkomenheden en functionele vragen en wensen.
 - Het oplossen/afhandelen/coördineren van meldingen door deze:
 - Eerst grondig te analyseren;
 - Zelf op te lossen/vraag te beantwoorden;
 - Door te verwijzen en/of het telefoongesprek doorzetten naar de relevante ICT-leverancier dan wel functioneel beheerder indien het applicatie-specifieke, niet-technische meldingen betreft.
 - Up-to-date houden van de juiste status van een melding alsmede het bijhouden / registreren van oplostijden.
 - Het verzamelen en registreren van informatie over de meldingen.
 - Het communiceren over de voortgang / oplossing van meldingen naar de melders en andere beheerpartijen.
 - Het afsluiten van meldingen indien de melding is afgehandeld.
135. De aangeboden helpdesk is in staat om en kenmerkt zich door het bieden van oplossend vermogen.
136. De helpdesk wordt uitgevoerd vanaf een vestiging van de leverancier.
137. Communicatie, registratie en rapportage vindt plaats in de Nederlandse taal.

8.3 Servicelevelmanagement inclusief rapportage

138. De leverancier dient een senior servicemanager verantwoordelijk te maken voor de integrale dienstverlening aan gemeente Lopik.
139. De aangewezen servicemanager is voor gemeente Lopik het eerste aanspreekpunt ten aanzien van alle aspecten van de Dienstverlening.

- 140. De aangewezen servicemanager treedt tijdens escalatie op als escalatiemanager richting gemeente Lopik.
- 141. De aangewezen servicemanager verzorgt de, in samenspraak gedefinieerde rapportages aan gemeente Lopik.
- 142. De aangewezen servicemanager is aanwezig bij het tactisch en strategisch overleg met gemeente Lopik.

8.4 Self Service Portal

- 143. Een Self Service Portal dient vanuit de virtuele werkplek beschikbaar te zijn voor medewerkers.
- 144. Via de Self Service Portal dienen medewerkers van gemeente Lopik zelf aanvragen in te kunnen dienen dan wel een aantal diensten/taken volledig geautomatiseerd zelf regelen. Dit dient op een gecontroleerde, volledig geautomatiseerde manier middels een workflow en afhankelijk van de juiste autorisatie plaats te kunnen vinden. De volgende functionaliteiten dienen in ieder geval gerealiseerd te worden:
 - a. Aanvragen dan wel toewijzen van additionele dataopslag-capaciteit aan een gebruiker
 - b. Aanvraag toegang software
 - c. Aanmaken tijdelijk login accounts AD
 - d. Aanvraag grotere home drive
 - e. Aanvraag meer opslagcapaciteit functionele e-mailbox
 - f. Password-reset functionaliteit
 - g. Aanpassen gebruikersgegevens (velden in AD)
 - h. Overzicht lidmaatschap van AD-groepen
 - i. Weblinks naar andere self-service portalen, bijvoorbeeld voor personele zaken (via SSO)
 - j. Aanmaken functionele mailbox voor bijvoorbeeld nieuwe medewerker
 - k. Toevoegen en verwijderen (personen aan) functionele mailbox
 - l. Aanmaken accounts
 - m. Software/applicaties installeren dan wel toewijzen aan een gebruiker
 - n. Autorisaties netwerkschijven/portaal (bv S:) aanpassen
 - o. Aanvragen restore bestand(en) en/of e-mail
 - p. Melden en registreren van incidenten alsmede het opzoeken van de status van een incident dan wel beantwoorden en/of aanvullen van informatie t.b.v. het gemelde incident
 - q. Aanvragen change (RFC)

Een aantal van de bovenstaande onderdelen vereisen mogelijk handmatige interventie. Deze onderdelen dienen via het self-service portaal aan te vragen te zijn, waarna vervolgens automatisch een opdracht wordt gemaakt binnen de service management tooling van de leverancier (bijvoorbeeld TOPdesk).

9 Onsite support

- 145. Op eerste verzoek van gemeente Lopik werkt leverancier mee aan het op zo kort mogelijk termijn beschikbaar stellen van medewerkers voor onsite support op locatie binnen de gemeente Lopik.