Bijlage 09 - Beschrijving huidige ICT-omgeving

ICT Beheer (All-in) – Stichting ICT Beheer (SIB)

Inhoud

1. Organisatiecontext

Bibliotheek Zuid-Kennemerland (BZK) en Cpunt zijn twee zelfstandige organisaties die voor hun ICT-dienstverlening nauw samenwerken. De infrastructuur en een belangrijk deel van het beheer worden gezamenlijk ingericht, terwijl beide organisaties ieder een eigen Microsoft-tenant en een eigen gebruikersomgeving hebben. Cpunt is deelnemer 1 en telt 233 gebruikers verdeeld over 7 locaties. BZK is deelnemer 2 en telt 130 gebruikers verdeeld over 10 locaties. De omgeving ondersteunt daarmee in totaal 363 gebruikers op 17 locaties.

De werkplekomgeving omvat 414 Windows laptops en desktops, 150 mobiele devices in een MAM/MDM-context en 1 centraal beheerde Mac-desktop bij Cpunt. Daarnaast is er bij Cpunt een apart maclokaal voor cursisten, dat buiten de reguliere device-aantallen valt en door Maxupply wordt beheerd. De meeste medewerkers werken op een persoonlijk device. Daarnaast zijn er gedeelde, vaste werkplekken voor specifieke functies, zoals baliewerkplekken voor de inname en uitgifte van bibliotheekmaterialen of voor ticketuitgifte.

De omgeving heeft naast kantoorautomatisering een duidelijke publieks- en ketencomponent. Op het netwerk zijn onder meer publieks-pc's, uitleen- en inleversystemen, pinapparatuur, gebouwtoegang, camerasystemen, oproep- en intercomsystemen, bonnenprinters, losstaande narrowcastsystemen, koffieautomaten en overige voorzieningen aangesloten. Een deel van deze voorzieningen wordt door derde partijen beheerd of gemonitord, terwijl de netwerkverbinding en de afstemming met de ICT-leverancier in de huidige situatie bij de gezamenlijke infrastructuur blijven.

2. Werkplekbeheer en apparaatbeheer

De werkplekomgeving bestaat hoofdzakelijk uit Windows 11-laptops en -desktops die via Microsoft Intune worden beheerd en als Entra Joined-apparaten aan een van beide tenants zijn gekoppeld. Voor beheer op afstand wordt Datto RMM gebruikt. De werkplekinrichting kent een hoge mate van standaardisatie, maar bevat ook specifieke uitzonderingen voor baliewerkplekken, publieksvoorzieningen en sectorgebonden randapparatuur.

2.1 Uitrol en basisconfiguratie

Nieuwe werkplekken worden uitgerold met Windows Autopilot, deels via pre-provisioning. De basisconfiguratie bestaat uit een gestandaardiseerde Windows 11-installatie met drivers, koppeling aan Entra ID en opname in Intune. Vaste instellingen, waaronder tijdzone, energiebeheer en zakelijke wifi-profielen, worden centraal vastgelegd. Onnodige standaardfunctionaliteit binnen Windows wordt waar nodig verwijderd of beperkt. Gedeelde werkplekken zijn vooral aanwezig op plekken waar randapparatuur, zoals scanners, RFID-readers, paskaartlezers, bonnenprinters of ticketprinters, aan één vaste opstelling gekoppeld is.

Naast de reguliere Windows-werkplekken hebben mobiele telefoons, zowel zakelijk als privé, via Mobile Application Management (MAM) toegang tot zakelijke resources. Bij Cpunt is daarnaast 1 Mac-desktop in Intune opgenomen via Apple Business Manager. Het afzonderlijke Maclokaal voor cursisten valt buiten de reguliere werkplekstandaard en wordt functioneel gescheiden gehouden.

2.2 Applicatiebeheer

Standaardapplicaties worden centraal beheerd en uitgerold. Het gaat onder meer om Microsoft 365-toepassingen, softphone-software, printvoorzieningen en de standaardset die nodig is voor de dagelijkse kantoorautomatisering. Aanvullende applicaties worden, afhankelijk van rechten en licenties, beschikbaar gesteld via het bedrijfsportaal. Dat geldt bijvoorbeeld voor Adobe-software, waarvan de afname via SURF loopt. Voor specifieke toepassingen worden clients of koppelingen gericht op bepaalde werkplekken geplaatst, zoals de Wise-client op balie-pc's bij Cpunt of de toevoeging van Teams-licenties aan Yealink-ruimtesystemen bij BZK.

Niet alle applicaties ondersteunen dezelfde identiteits- of beheerstandaard. Waar mogelijk worden SaaS-toepassingen met Entra gekoppeld via SSO of SAML. In de huidige situatie bestaan daarnaast nog derdepartijtoepassingen of deelvoorzieningen met een eigen, niet-SSO-ondersteunde identiteitsvoorziening.

2.3 Patch- en updatebeheer

Voor patch- en updatebeheer wordt een combinatie van voorzieningen gebruikt. Het Microsoft-besturingssysteem en de Microsoft-applicaties worden bijgehouden via AutoPatch. Firmware-updates worden centraal bewaakt via HP Connect. Voor overige applicaties wordt PatchMyPC ingezet voor application lifecycle management. Browser- en antivirusupdates worden met hogere frequentie uitgerold. De combinatie van deze mechanismen maakt dat de basiswerkplek grotendeels centraal en uniform kan worden bijgewerkt.

2.4 Opslag

Voor gegevensopslag wordt primair gebruikgemaakt van Teams, SharePoint en OneDrive. Teams en SharePoint worden gebruikt voor team- en afdelingsgebonden informatie, terwijl OneDrive als persoonlijke opslaglocatie dient. Bekende Windows-mappen worden naar OneDrive omgeleid, zodat lokale bestanden gesynchroniseerd worden. Lokale opslag op de C-schijf is versleuteld met BitLocker. USB-opslag kan alleen beschrijfbaar worden gebruikt als het medium versleuteld is.

3. Identiteits- en toegangsbeheer

De identiteitsvoorziening is hybride ingericht. Gebruikersaccounts ontstaan nog in een on-premise Active Directory en worden via Entra ID Connect gesynchroniseerd naar Entra ID. De huidige leverancier beheert zowel de cloudcomponenten als de nog aanwezige on-premise identiteitsvoorzieningen die voor legacy- en hybride functies nodig zijn.

3.1 Authenticatie en Single Sign-On

Authenticatie op de beheerde werkplekken verloopt met Windows Hello for Business en MFA. Na aanmelding op het device worden gebruikers automatisch aangemeld op Microsoft 365-diensten en, waar deze koppeling aanwezig is, op SaaS-applicaties die via SSO of SAML met Entra verbonden zijn. Voor een aantal derde partijen of oudere voorzieningen bestaat nog een afwijkende authenticatiestroom zonder volledige SSO-ondersteuning.

3.2 Voorwaardelijke toegang en compliancebeleid

Toegang tot applicaties en data is gekoppeld aan device compliance en de identiteit van de gebruiker. Voor beheerde werkplekken wordt gewerkt met beleid op basis van Intune en Conditional Access. Niet-beheerde apparaten kunnen slechts beperkt toegang krijgen, met name tot webtoepassingen. Voor specifieke toepassingen die via het private datacenter beschikbaar worden gesteld, is voor bepaalde gebruikers een VPN-verbinding nodig. Dat geldt met name voor de legacy- en hybride componenten die niet rechtstreeks als moderne SaaS-dienst beschikbaar zijn.

3.3 Accountbeheer

Voor beheer en administratie is een scheiding aangebracht tussen reguliere gebruikersaccounts en beheeraccounts. Voor tenantbeheer door de huidige leverancier wordt gebruikgemaakt van GDAP en Microsoft Lighthouse. In de huidige situatie zijn daarnaast nog lokale on-premise beheeraccounts aanwezig voor het beheer van legacycomponenten. Zowel de organisaties als de leverancier beschikken over break-glass accounts.

4. Netwerk en connectiviteit

4.1 Lokale netwerkinfrastructuur

Op alle 17 locaties is een LAN- en wifi-infrastructuur aanwezig op basis van Fortinet-componenten. De omgeving omvat 19 firewalls, 40 switches en 140 access points. De netwerkomgeving wordt centraal beheerd via FortiManager en aanvullend gemonitord met tooling van de huidige ICT-leverancier. Toegang tot het zakelijke wifi-netwerk voor beheerde werkplekken vindt plaats op basis van Entra ID en Intune.

Voor wifi worden meerdere SSID’s gebruikt. Daaronder vallen onder meer de interne kantoorautomatiseringsomgeving, publieksvoorzieningen en specifieke draadloze voorzieningen voor doelgroepen of gebruikssituaties. PublicRoam wordt als wifi-dienst gebruikt voor publieks- of gasttoegang. Het netwerk is logisch gesegmenteerd voor medewerkers, publieksdiensten, gebouwbeheer, audiovisuele installaties, multifunctionals, printers en overige gekoppelde apparaten. Dynamic Access Control via FortiSwitch/FortiGate-integratie is in de huidige situatie deels ingericht, maar de segmentatie berust nog niet volledig daarop en wordt voor een deel nog traditioneel ondersteund door vaste aansluit- en configuratiemethoden.

Naast de eerder benoemde systemen zijn ook overige voorzieningen op het netwerk aangesloten, zoals koffieautomaten, oproep- en intercomsystemen, camerasystemen, inkloksystemen, losstaande narrowcastsystemen bij Cpunt en bonnenprinters. Deze categorie is functioneel relevant omdat zij in de huidige situatie wel netwerk-, segmentatie- of leveranciersafstemming vergt, ook als het functioneel beheer elders ligt.

4.2 WAN-verbindingen en SD-WAN

Alle locaties zijn via SD-WAN via hun lokale internet breakout gekoppeld aan een van de twee hoofdlocaties: Haarlem Centrum voor BZK en Hoofddorp Raadhuisplein voor Cpunt. De hoofdlocaties zijn onderling en met het private datacenter verbonden. De twee hoofdlocaties beschikken over een dubbele internetaansluiting en redundante firewalls. Voor de verbindingen wordt gebruikgemaakt van Ziggo, KPN en Helden van Nu.

4.3 Veilige externe toegang

Voor een beperkt aantal medewerkers is externe toegang tot legacy-applicaties mogelijk via Microsoft Always On VPN. Deze voorziening is gekoppeld aan de private datacenteromgeving van de huidige leverancier. De VPN wordt gebruikt om toegang te krijgen tot applicaties en hybride voorzieningen die in of via het private datacenter beschikbaar zijn en die nog niet naar een volledig cloudmodel zijn overgezet. De combinatie van client-VPN, on-premise PKI en datacenterkoppeling is daarmee onderdeel van de huidige situatie en hangt direct samen met de legacy-inrichting die ook in paragraaf 6.2 wordt beschreven.

4.4 DNS en DHCP

DHCP wordt verzorgd vanuit de FortiGate-omgeving. Interne DNS is nog gebaseerd op Microsoft DNS, omdat er nog een legacy-omgeving op basis van Active Directory aanwezig is. Voor externe DNS wordt voor BZK gebruikgemaakt van Argeweb en voor Cpunt van MijnDomein.

5. Communicatie en samenwerking

5.1 E-mail en e-mailbeveiliging

E-mail loopt via Exchange binnen Microsoft 365. De organisaties gebruiken hierbij hun eigen tenant en hun eigen licentie-inrichting. SPF, DKIM en DMARC zijn voor Cpunt en BZK verschillend ingericht; de concrete technische invulling wordt in dit document niet verder uitgewerkt. Controle op in- en uitgaande e-mail vindt plaats met de standaard beveiligingsvoorzieningen die binnen de gebruikte Microsoft-licenties beschikbaar zijn.

5.2 Productiviteit en samenwerking

Voor productiviteit en samenwerking wordt gebruikgemaakt van Microsoft 365, waaronder Teams, SharePoint, OneDrive en de Office-applicaties. BZK werkt met A3-licenties. Cpunt werkt met E3-licenties en daarnaast met F3-licenties voor specifieke gebruikersgroepen. Beide organisaties beschikken over een eigen Azure-subscription die in de huidige situatie met name wordt gebruikt voor uitgebreide opslag van logbestanden.

5.3 Telefonie

In het tweede kwartaal van 2026 zijn BZK en Cpunt gemigreerd naar de gehoste Xelion-telefonieomgeving bij Maxxus. De omgeving ondersteunt softphones en een beperkt aantal vaste toestellen. De koppeling met Active Directory en de beschikbaarheidsinformatie uit Outlook maakt deel uit van de huidige inrichting. De software voor de softphones wordt via het Intune-bedrijfsportaal beschikbaar gesteld.

5.4 Videoconferencing

Voor videoconferencing maakt BZK gebruik van Yealink-systemen. De licenties worden door de organisatie zelf beheerd en via Fellowmind (voorheen Xperity) afgenomen. Het onderhoud van de hardware ligt bij de organisatie; de ICT-leverancier verzorgt de koppeling van de Teams-licentie in de tenant aan het device en de vergaderzaalresource.

5.5 Printinfrastructuur

De fysieke levering, installatie, reparatie en supplies van printers liggen bij externe partijen. Het technisch beheer van de printdiensten en de netwerkkoppelingen ligt bij de ICT-leverancier. Binnen BZK wordt Printix gebruikt. Binnen Cpunt wordt PaperCut gebruikt; deze inrichting is in de huidige situatie hybride en bevat naast cloudcomponenten nog een lokale component. Bij Cpunt kan functioneel beheer bepaalde printqueues naar devices pushen en beperkt troubleshooten. Een deel van de multifunctionals is gekoppeld aan Xafax voor betaald printen en kopiëren voor publiek. De aan Xafax gekoppelde printers kunnen daarnaast scanfunctionaliteit richting externe e-mailadressen ondersteunen.

6. Applicaties en clouddiensten

De applicatieomgeving bestaat uit een combinatie van gedeelde platformdiensten, deelnemer-specifieke SaaS-applicaties, hybride voorzieningen en legacycomponenten. De huidige leverancier ondersteunt waar nodig bij installatie, koppeling, netwerktoegang, SSO-inrichting, tenantconfiguratie of afstemming met derden. Onderstaande tabellen geven per leverancier of voorziening de belangrijkste applicaties, het type, de gebruiksfunctie, de wijze van toegang of koppeling en de relatie met de ICT-leverancier weer.

6.1 SaaS-applicaties

Gedeelde leveranciers en diensten

Leverancier	Applicatie / item	Type	Gebruik / functie	Toegang / koppeling	Relatie met ICT-leverancier
Adobe / SURF	Adobe Creative Cloud	SaaS / clientsoftware	Creatieve software zoals Acrobat, Photoshop en InDesign	Installatie of beschikbaarstelling via bedrijfsportaal; licentiegebonden	Ondersteuning op werkplek- en licentieniveau
EKZ	Inlever- en uitleenstations	OT / netwerkgebonden systeem	Selfservice voor lenen en inleveren van materialen	Direct gekoppeld aan netwerk; leverancier kan op afstand ondersteunen	Afstemming nodig bij issues of projecten
KPN	Internet / mobiele telefonie	Dienst	Internet en in een aantal gevallen mobiele telefonie	WAN / internetdienst	SPOC via ICT-leverancier voor internet; mobiele telefonie deels rechtstreeks
Maxxus	Xelion	Gehoste telefoniedienst	Softphones en beperkt aantal vaste toestellen	Integratie met AD / Outlook; client via bedrijfsportaal	Incidentgedreven en operationele afstemming
Microsoft	Microsoft 365	Cloudplatform	Exchange, Teams, SharePoint, OneDrive, Defender en Intune	Tenantgebaseerde cloudtoegang; SSO waar van toepassing	Beheer door huidige ICT-leverancier
PublicRoam	Publiekswifi	Wifi-dienst	Gast- en publieksinternet	Draadloze toegang via eigen SSID	Netwerkafstemming met ICT-leverancier
Veeam	Veeam Backup	Back-updienst	Back-up van Microsoft 365-data	Back-up vanuit cloudomgeving	Beheerd door huidige ICT-leverancier
Ziggo	Internet	Dienst	Internetverbindingen	WAN / internetdienst	SPOC via ICT-leverancier

Cpunt – applicaties en clouddiensten

Leverancier	Applicatie / item	Type	Gebruik / functie	Toegang / koppeling	Relatie met ICT-leverancier
Adobe / SURF	Adobe Creative Cloud	SaaS / clientsoftware	Creative Cloud voor medewerkers met licentie	Beschikbaar via bedrijfsportaal	Werkplek- en licentieondersteuning
Automatic Signal	Genetec	Netwerkgebonden camerasysteem	Camerasystemen	Aangesloten op netwerk; externe leverancier ondersteunt op afstand	Afstemming bij issues of projecten
CCV, Euro Events, Eijsink, Worldline & STN/Worldline	Pinapparaten	Netwerkgebonden betaalvoorziening	Pinbetalingen	Aangesloten op netwerk	Afstemming bij issues of projecten
EKZ	Inlever- en uitleenstations	OT / netwerkgebonden systeem	Uitleen- en innameapparatuur	Aangesloten op netwerk	Afstemming bij issues of projecten
Maxupply	Maclokaal	Afzonderlijke leeromgeving	Maclokaal voor cursisten	Eigen beheer door derde partij op apart VLAN	Geen regulier werkplekbeheer
Poolmanager	Poolmanager	Hybride / cloud in transitie	Planningstool	Toegang via thuiswerkomgeving / private datacenterkoppeling	Incidentele technische ondersteuning
Probiblio	AFAS InSite / AFAS Profit	SaaS / externe applicatie	ERP voor HR en financiën	Gebruikers- en/of leverancierskoppelingen	Ondersteuning alleen waar technische afstemming nodig is
Rosystems / Salto	Gebouwtoegang	Netwerkgebonden systeem	Tags en sloten voor gebouwtoegang	Koppeling met beheersysteem; transitie naar hybride cloud loopt	Afstemming bij issues of projecten
SDI	Wise	Applicatie / client + back-end	Bibliotheeksysteem voor boeken- en klantenbeheer	Client op balie-pc's; netwerk- en werkplekkoppeling	Incidentele ondersteuning; uitrol via Intune
STN	Kassasoftware	Netwerkgebonden applicatie	Kassasoftware	Aangesloten op netwerk	Afstemming bij issues of projecten
Ticketmatic	Ticketmatic - BOCA Printers	SaaS + randapparatuur	Ticketingsysteem en ticketprinters	Software / printers op specifieke werkplekken	Incidentele ondersteuning bij installaties
ToshibaTec	PaperCut	Hybride printvoorziening	Printomgeving binnen Cpunt	Netwerk, printers en hybride PaperCut-omgeving	ICT-leverancier eerste aanspreekpunt bij printproblemen
Verito	Business Central - Exsion	SaaS	ERP en rapportage	Cloudtoegang; Exsion-rapportage via Excel	Incidentele ondersteuning waar nodig
Xafax	EasyAccount / publieks-pc's	Publieksdienst / externe omgeving	Publiekscomputers, print- en betaalsysteem	Zero clients via RDS-omgeving van Xafax; netwerkgekoppeld	Afstemming nodig bij issues of projecten
Yesplan	Yesplan	SaaS	Evenementplanning	Cloudtoegang	Incident- of projectgedreven afstemming

BZK – applicaties en clouddiensten

Leverancier	Applicatie / item	Type	Gebruik / functie	Toegang / koppeling	Relatie met ICT-leverancier
Adobe / SURF	Adobe Creative Cloud	SaaS / clientsoftware	Creative Cloud voor medewerkers met licentie	Beschikbaar via bedrijfsportaal	Werkplek- en licentieondersteuning
Argeweb	Domeinregistratie	Domeindienst	Domeinregistratie en extern DNS voor BZK	Beheer via portal	Wijzigingen via portal / afstemming
Axiell	V-Smart en V-Insight	Legacy / hybride applicatie	Bibliotheeksysteem met koppeling naar on-premise webtoepassing en uitleenapparatuur	Draait via private datacenteromgeving	Incidentgedreven afstemming
CCV	Pinapparaten	Netwerkgebonden betaalvoorziening	Pinbetalingen aan de balies	Aangesloten op netwerk	Incident- en projectgedreven contact
Cocoon	Cocoon	Clouddienst	Beeldbank	Cloudtoegang	Beperkte technische afstemming indien nodig
Deskbird	Deskbird	SaaS	Werkplekreservering	SSO-koppeling met Entra	Cloudtoepassing
Duzz ICT	Narrow casting schermen	Netwerkgebonden systeem	Narrowcasting voor klantcommunicatie	Aangesloten op netwerk	Incident- en projectgedreven contact
Exact	Exact Globe	Legacy / applicatie	Financieel beheer en rapportage	Huidige toepassing; vervanging gepland	Incidentgedreven contact
Fellowmind	Microsoft Dynamics	SaaS	CRM en customer service	Specifieke Microsoft-licenties; cloudtoegang	Incident- en projectgedreven contact
Johnson Controls	Tag-beheer tool	Netwerkgebonden systeem	Gebouwtoegangssysteem	Aangesloten op netwerk	Incident- en projectgedreven contact
NMBRS	NMBRS	SaaS	HR-systeem	SSO-koppeling met Entra	Cloudtoepassing
Ovatic	Ovatic	SaaS	Ticketing, activiteitenplanning en zalenboeking	Cloudtoegang	Incidentgedreven contact
Plek	Plek	SaaS	Sociaal intranet	Webtoepassing met SSO-koppeling	Cloudtoepassing
Printix	Printix	Cloud printvoorziening	Follow-me printen	Cloudkoppeling met MFP's en werkplekken	Incidentgedreven contact
Quinyx	Quinyx	SaaS	Personeelsplanning	SSO-koppeling met Entra	Cloudtoepassing
SDI	Wise	SaaS / applicatie in voorbereiding	Bibliotheeksysteem; invoering voorzien in 2027	Pre-projectfase	Voorbereidende werkzaamheden
ToshibaTec	Multifunctional copier/printer	Netwerkgebonden printvoorziening	Printen, scannen en kopiëren voor kantoor en klanten	Gekoppeld aan Printix en Xafax	Afstemming met ICT-leverancier en Xafax
Veeam	Veeam Backup	Back-updienst	Back-up van Teams, SharePoint en Exchange	Back-up vanuit cloudomgeving	Beheerd door huidige ICT-leverancier
Visotek	Provision ISR	Netwerkgebonden camerasysteem	Bewakingscamera's en video-opname	Aangesloten op netwerk	Incident- en projectgedreven contact
Xafax	EasyAccount / publieks-pc's	Publieksdienst / externe omgeving	Publieks-pc's en betaalfunctionaliteit	Koppeling met eigen netwerkdeel en RDS-omgeving van Xafax	Incident- en projectgedreven contact

6.2 Legacy-applicaties en datacenter

De private datacenteromgeving van de huidige leverancier fungeert in de huidige situatie als onderlaag voor een beperkt aantal legacy- en hybride componenten. Deze omgeving is geen algemene productielaag voor alle applicaties, maar ondersteunt specifiek die voorzieningen die nog niet volledig cloudgebaseerd functioneren.

Legacy- en datacentercomponenten

Omgeving	Component	Type	Gebruik / functie	Toegang / koppeling
Private datacenter huidige leverancier	Vsmart	Legacy-applicatie	Bibliotheeksysteem van BZK; beoogde beschikbaarheid tot circa eind 2027	Toegang voor gebruikers of koppelingen verloopt via bestaande omgeving; externe leverancier heeft directe toegang tot servers
Private datacenter huidige leverancier	Poolmanager	Hybride voorziening	Planningstool; overgang naar cloud voorzien in Q3 2026	Gebruikers hebben voor bepaalde scenario's toegang via thuiswerkomgeving / VPN
Private datacenter huidige leverancier	PaperCut (Cpunt)	Hybride printvoorziening	Lokale componenten naast cloudcomponenten; overgang voorzien in Q3 2026	Externe leverancier heeft toegang tot het hybride systeem op een locatie van deelnemer 1
Private datacenter huidige leverancier	Active Directory	Onderliggende infrastructuur	Bron voor accountaanmaak en synchronisatie	Beheer door huidige leverancier
Private datacenter huidige leverancier	Microsoft PKI	Onderliggende infrastructuur	Ondersteunt certificaatgebonden voorzieningen, waaronder VPN	Beheer door huidige leverancier
Private datacenter huidige leverancier	VPN-voorziening	Onderliggende infrastructuur	Maakt toegang tot legacy- en hybride componenten mogelijk	Gebruikt voor beperkte groep medewerkers
Private datacenter huidige leverancier	SQL Server	Onderliggende infrastructuur	Ondersteunt Poolmanager	Alleen benodigd voor specifieke legacy/hybride toepassing

Netwerkgebonden en extern beheerde voorzieningen

Domein	Leverancier / voorziening	Type	Gebruik / functie	Toegang / koppeling
Camerasystemen	Automatic Signal / Genetec, Visotek / Provision ISR	Netwerkgebonden systeem	Direct of indirect gekoppeld aan het netwerk	Externe leverancier kan ondersteunen; afstemming via ICT-leverancier
Gebouwtoegang	Rosystems / Salto, Johnson Controls	Netwerkgebonden systeem	Beheersysteem in datacenter; transitie naar hybride cloud loopt	Leveranciersafstemming nodig
Narrowcasting	Duzz ICT en losstaande Cpunt-schermen	Netwerkgebonden systeem	Schermen in panden voor communicatie	Aangesloten op netwerk; derde partij kan erbij
Publieksdiensten	Xafax	Externe publieksomgeving	Publieks-pc's, betaald printen en kopiëren	Eigen netwerkdeel / RDS-omgeving gekoppeld aan interne netwerkvoorzieningen
Uitleen en inname	EKZ	OT-omgeving	Systemen voor inname en uitleen van materialen	Leverancier kan op afstand ondersteunen

7. Servicemanagement en helpdesk

De dienstverlening is ingericht volgens ITIL-processen voor incident-, problem- en changemanagement. De huidige leverancier vervult de rol van primaire servicedesk voor ICT-gerelateerde meldingen. Daarnaast zijn binnen beide organisaties functioneel beheerders actief die medewerkers ondersteunen bij functionele vragen en die ook een belangrijke rol hebben in de afstemming met leveranciers.

De praktijk is minder lineair dan een strikt single point of contact-model. Gebruikers melden zich in de huidige situatie bij functioneel beheer, direct bij de ICT-leverancier of in sommige gevallen rechtstreeks bij een andere leverancier. Wanneer meldingen verkeerd zijn gerouteerd, komen deze terug bij functioneel beheer voor herroutering of escalatie. Escalatie richting de ICT-leverancier verloopt via de servicedesk van functioneel beheer en de servicemanager van de ICT-leverancier.

De overlegstructuur bestaat uit een operationeel overleg (OO), een tactisch overleg (TO) en een strategisch overleg (SO). Het operationeel overleg vindt wekelijks plaats en wordt per deelnemer afzonderlijk gevoerd. Het tactisch overleg is gezamenlijk en vindt eenmaal per zes weken plaats. Het strategisch overleg is eveneens gezamenlijk en vindt één à twee keer per jaar plaats.

Domein	Kernactiviteit	ICT-leverancier	FB	Derde partij	Toelichting
Werkplek en apps	Intune-beheer, packaging, bedrijfsportaal, remote beheer	Ja	Beperkt, vooral functionele input	Ja, bij leverancierspecifieke software	ICT-leverancier beheert de technische basis; FB heeft vooral inhoudelijke of functionele rol
Identity en tenant	AD, Entra, Conditional Access, GDAP/Lighthouse	Ja	Nee	Beperkt	Technisch beheer ligt bij ICT-leverancier; enkele derde partijen gebruiken nog eigen identiteitsvoorzieningen
Netwerk	FortiGate, switches, access points, SD-WAN en segmentatie	Ja	Nee	Ja	Derde partijen hebben voor gekoppelde systemen soms eigen toegang of afstemming nodig
Print en publieksdiensten	Technisch beheer printkoppelingen, publieks-pc's, betaalprint	Ja	Ja	Ja	FB doet functionele instellingen of beperkte troubleshooting; derden verzorgen hardware, software of publieksdiensten
Gekoppelde apparatuur en externe systemen	Camerasystemen, toegangssystemen, pin, narrowcasting, bonnenprinters, uitleenapparatuur	Netwerk en afstemming	Beperkt	Ja	Het functioneel of technisch eigenaarschap ligt vaak bij een derde partij, terwijl netwerk- en ketenafstemming bij de ICT-leverancier ligt

8. Beveiliging, monitoring en continuïteit

8.1 Endpoint-beveiliging

De werkplekken zijn voorzien van een gestandaardiseerde beveiligingsbasis. In de broninformatie worden daarbij Microsoft Defender Antivirus en Antimalware, Microsoft Defender Firewall, hardwaregebaseerde beveiliging via Device Guard, blokkade van onveilige openbare netwerken en lokale beveiligingsinstellingen genoemd die verouderde authenticatiemechanismen uitschakelen. Daarnaast is uitgebreide logging op endpoints geactiveerd voor detectie, troubleshooting en ondersteuning.

De beveiligingsinrichting sluit aan op de centrale werkplekstandaard en op het gebruik van Intune, Entra, compliancebeleid en Conditional Access. Voor een aantal ketens en derde partijen bestaat echter nog een hybride of afwijkende situatie, bijvoorbeeld doordat niet alle systemen volledige SSO-ondersteuning bieden of doordat nog directe toegang tot specifieke voorzieningen noodzakelijk is.

8.2 Monitoring en SOC/SIEM

De netwerkinfrastructuur wordt 24/7 gemonitord. Dat betreft in elk geval firewalls, switches en access points via FortiManager en aanvullende tooling van de huidige ICT-leverancier. Daarnaast vindt op onderdelen leveranciersspecifieke monitoring plaats, bijvoorbeeld bij multifunctionals of gekoppelde apparatuur. Binnen de huidige situatie is geen afzonderlijke, expliciet benoemde SOC/SIEM-dienst als aparte voorziening beschreven; de monitoring is primair gekoppeld aan netwerkbeheer, endpointbeheer en operationeel technisch beheer.

8.3 Back-up en herstel

Voor continuïteit worden twee complementaire back-upvoorzieningen gebruikt. De eerste betreft een dagelijkse back-up van de in het private datacenter aanwezige componenten, met langetermijnretentie in de back-up- en cloudomgeving van de leverancier. De tweede betreft een aparte back-upvoorziening voor gegevens uit de Microsoft-omgeving, waaronder Exchange, SharePoint, Teams en OneDrive.

De omvang van de back-upscope voor Microsoft 365 bedraagt 429 gebruikersaccounts, verdeeld in 279 voor Cpunt en 150 voor BZK, met een gezamenlijke dataomvang van circa 13 TB. De back-upvoorziening is daarmee niet alleen gericht op de private datacentercomponenten, maar ook op de clouddata van beide organisaties.