

ICT Infrastructuur Architectuur

Parkstad-IT

2022

Klantversie

Algemene informatie

Document eigenaar:	Victor Abratanski (Bureauhoofd Beheer en Lead architect Parkstad-IT)
Organisatie:	Parkstad-IT
Vastgesteld door / dd:	Versie 2.0 is door het AMT vastgesteld op 17 augustus 2020
Vertrouwelijkheidsclassificatie:	Intern openbaar
Documentstatus:	Vastgesteld
Versie datum:	24 juni 2022
Versie:	2.5

Versieoverzicht

Versie	Datum	Auteur	Status	Belangrijkste wijzigingen t.o.v. vorige versie
1.9	22/10/2019	Victor Abratanski	Ter vaststelling	
2.0	12/08/2020	Elze Veldhuis	Ter vaststelling	
2.1	19/10/2020	Elze Veldhuis	Vastgesteld	Versie 2.0 is vastgesteld in PIT MT van 17-8-2020. Hoofdstuk Security toegevoegd.
2.2	18/01/2021	Elze Veldhuis	Ter accordering MT	Technische referentie architectuur plaatje en hoofdstuk "beheerarchitectuur" toegevoegd.
2.3	02/02/2021	Victor Abratanski	Finale check	Ontdubbelen verschillende versies
2.4	24/08/2021			Hoofdstuk 13 eruit gehaald en als apart document gepubliceerd.
2.5	23/06/2022	Victor Abratanski	Geactualiseerd	

Bronvermelding

Documenttitel	Als input gebruikt	Vervangen door het document
Documentatie Parkstad-IT:		
•		
•		
Geraadpleegde literatuur en documenten derden:		
•		

Documentrouting

Voor dit document geldt de volgende documentrouting:

- Auteurs van de verschillende PIT Beheerclusters;
- Eindredacteur;
- MT Parkstad-IT.

Vervolg nadat het document is vastgesteld

- Ter beschikking te stellen aan alle GR-PIT deelnemers.

Leeswijzer

Toelichting op het invullen van een bepaalde hoofdstuk / paragraaf wordt aangegeven tussen "< >". Deze secties kunnen uit de tekst worden verwijderd.

Inhoudsopgave

1.	Inleiding	4
1.1	Doel	4
1.2	Doelgroep	4
1.3	Achtergrond	4
1.4	Samenhang met andere documenten	4
2.	Clouddiensten	5
3.	Algemeen	6
4.	Hardware	6
4.1	Werkplek	6
4.2	Laptop	7
4.3	Virtuele desktop	7
4.4	Printers	7
4.5	Overige randapparatuur	7
5.	Software	7
5.1	Systeemsoftware	7
5.2	Drive-letters	8
5.3	Gebruik	8
6.	Computerservers	8
6.1	Intel servers	8
6.2	Oracle platform	8
6.3	Storage	8
6.4	Systeemsoftware	9
7.	Monitoring	9
8.	Database platformen	9
9.	Netwerk	10
9.1	Centraal	10
9.2	WAN	10
9.3	LAN	10
9.4	Netwerk software	10
10.	Licenties	10
11.	Randapparatuur	11
12.	Security	11

1. Inleiding

1.1 Doel

De ICT-infrastructuur is een complex geheel van componenten en onderlinge afhankelijkheden. Dagelijks worden wijzigingen doorgevoerd om de infrastructuur toekomstbestendig te houden. De hoeveelheid data verdubbelt elke 2 jaar, het “Nieuwe Werken” vraagt om nieuwe functionaliteiten, clouddiensten integreren en integrale ketenrelaties moeten ondersteund worden.

Om het geheel beheersbaar te houden is een IT-infrastructuur architectuur onmisbaar. De architectuur borgt de beschikbaarheid van de bedrijfsprocessen conform SLA. Dit document omschrijft de technische automatiseringsarchitectuur van Parkstad-IT en dient bij een aanbestedingstraject als “Programma van Randvoorwaarden” gelezen te worden.

Parkstad-IT beheert de IT-infrastructuur voor de gemeenschappelijke ICT-voorzieningen en stelt deze beheersbaar beschikbaar aan:

- Deelnemers van de Gemeenschappelijke Regeling Parkstad-IT (GR-PIT);
- Ketenrelaties (Mondriaan Zorggroep, Leger des Heils, CWI, Uitzend- en detacheringsbureaus, etc.);
- Externe klanten (diverse gemeentes in Zuid-Limburg, Regio Parkstad Limburg, MCC 112, etc.).

Parkstad-IT is voor al haar deelnemers verantwoordelijk voor het technisch beheer van de gehele ICT-infrastructuur. Het Technisch Applicatiebeheer is als additionele dienst af te nemen. Voor een totaaloverzicht van de Parkstad-IT dienstverlening wordt verwezen naar haar Producten & Dienstencatalogus.

1.2 Doelgroep

Dit document is bedoeld voor partijen die zich bezighouden met de selectie van nieuwe soft- en hardware, ICT-toepassingen ontwikkelen, Informatiemanagers en de medewerkers van Parkstad-IT.

De lezer wordt verondersteld een ICT-achtergrond te hebben, daar dit een technisch document is.

1.3 Achtergrond

Parkstad-IT beheert de infrastructuur en garandeert een hoge mate van beschikbaarheid en betrouwbaarheid. Middels de Automatiseringsarchitectuur borgt Parkstad-IT dat nieuwe hard- en software conflictvrij ingezet kan worden en de technische borging in kennis en ICT- componenten voorhanden is. Het is van belang de procedure “Aanschaf nieuwe hardware en software” correct te doorlopen. Hou rekening met de architectuureisen. Voordat software en hardware mag worden aangeschaft, moet Parkstad-IT eerst toestemming ervoor verlenen.

1.4 Samenhang met andere documenten

De Enterprise architectuur van een organisatie wordt gevormd door de volgende domeinarchitecturen en bijbehorende thema's:

1. Bedrijfsarchitectuur:
 - a. Markten, klanten en verkoopkanalen;
 - b. Producten en Diensten;
 - c. Bedrijfsprocessenmodel (bedrijfsfunctiemodel);
 - d. Organisatiemodel;
 - e. Besturingsmodel (incl. KPI's);

2. Informatiearchitectuur:

- a. Informatiefunctiemodel;
- b. Het bedrijfsobjectenmodel;
- c. Gegevensmodel;
- d. Applicatiearchitectuur;

3. Technologie architectuur:

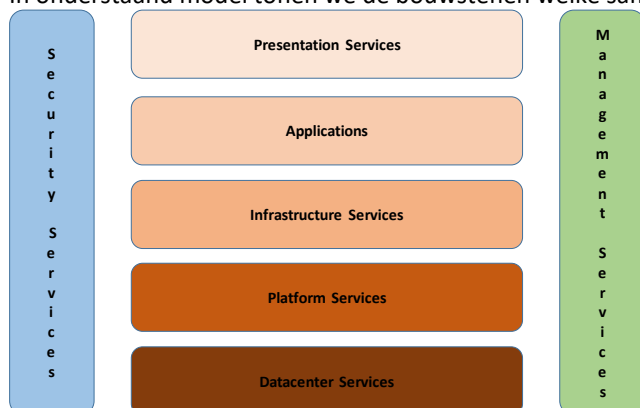
- a. Integratie architectuur (middleware);
- b. Platform architectuur;
- c. Netwerk architectuur;
- d. Beheerarchitectuur.

De nadruk in dit document ligt op de Technologie architectuur van de gehele door Parkstad-IT beheerde ICT-infrastructuur.

Naast bovenstaande inrichting van de verschillende architectuur domeinen, heeft de Automatiserings-architectuur relaties met de volgende documenten:

- Richtlijnen ICT-gebruik;
- Securitybeleid.

In onderstaand model tonen we de bouwstenen welke samen de IT Infrastructuur vormen.



2. Clouddiensten

Alvorens Clouddiensten worden ingezet, is per situatie specifiek onderzoek noodzakelijk. In alle gevallen van Clouddiensten moet worden afgestemd met Parkstad-IT. Middels het Changeproces kan het verzoek tot toetsing worden ingediend.

Op zich staande toepassingen in de “cloud” plaatsen is vanuit ICT technisch het meest eenvoudig te regelen. Echter de meeste toepassingen hebben koppelingen met andere toepassingen en hiermee neemt de complexiteit toe. Vanwege de externe koppelingen neemt de complexiteit voor het incidentproces toe. Zeker als er koppelingen zijn tussen SAAS leveranciers waar Parkstad IT geen zicht op heeft.

Gegevensuitwisseling geschiedt middels EnableU2Secure. Iedere klant beschikt over een eigen Fortinet vDOM, virtuele Firewall. In het vDOM mogen de servers onderling geen communicatie hebben. Single Sign-On (SSO) en Active directory uitlezen tbv een Clouddienst geschiedt op basis van Microsoft Azure AD.

Koppeling zijn in het verleden opgetuigd met:

- VPN-tunnel is niet toegestaan;
- Exchangekoppeling EWS (Exchange Web Services);
- DMZ servers (Microsoft Windows Servers) op basis van Reverse proxy of zogenaamd Port Proxy.
- Een eigen DMZ dienst waarbij beheer hiervan bij de aanbieder clouddienst is belegd;
- De standaard browser om Clouddiensten te ontsluiten is Microsoft Edge (op basis van chromium).

Nieuwe SAAS applicaties moeten kunnen koppelen met de API Gateway van Parkstad IT omwille veilige toegang tot services in het Parkstad IT Applicatielandschap. Al het berichtenverkeer wordt gemonitord en ge-audit.

3. Algemeen

Alvorens nieuwe software / hardware aangekocht mag worden, moet eerst instemming verkregen worden van de Informatiemanager van de aanvraag-organisatie. De Informatiemanager (van de klant) start middels het Changeproces het verzoek tot toetsing op om door Parkstad-IT te laten onderzoeken of de software / hardware past in de ICT-infrastructuur van Parkstad-IT.

Parkstad-IT toetst of de nieuwe software voldoet aan de technische eisen welke gesteld zijn op de diverse onderdelen. De security check maakt hier standaard onderdeel van uit.

Van iedere toepassing moet vanuit de gebruikersorganisatie een Functioneel Beheerder (FB) benoemd zijn. Deze fungeert als aanspreekpunt en intermediair naar de softwareleverancier en Parkstad-IT. De Technisch Applicatiebeheerder (TAB) voert de technische regie naar leverancier en de diverse technische disciplines binnen Parkstad-IT (Server- en storagebeheer, Netwerkbeheer, Databasebeheer, Werkplekbeheer en Telefoniebeheer). Afhankelijk van de omvang, in overeenstemming met categorisering door Projectmanagement van Parkstad IT, kan er een Projectleider worden toegewezen. De kosten voor projectleiding en de technische disciplines zijn voor rekening van de klant.

Naast een variabel pakket (zie Producten & Dienstencatalogus Parkstad-IT) zijn enkele vaste componenten verplicht. Denk in deze aan virusprotectie, Microsoft Exchange, Microsoft Office Pro Plus, standaardisatie randapparatuur, etc.

4. Hardware

4.1 Werkplek

De werkplekstandaard is een Dell Wyse Thin Client met beeldscherm welke connecteert naar de virtuele VMWare Horizon Desktop. De TC (Thin Client) wordt vervangen door een actueel model wanneer hier een technische of functionele reden voor is. In zeer specifieke afwijkende gevallen kan Parkstad-IT beslissen hiervan af te wijken en een Desktop PC te plaatsen. Parkstad IT beschikt ook over een performance virtuele Horizon Desktop tbv met verhoogde grafische en reken capaciteit tbv CAD en andere zwaardere toepassingen.

4.2 Laptop

De laptops worden voorzien van een “vrije inrichting”, losgekoppeld van het interne netwerk en vrijgegeven conform BYOD (Bring Your Own Device). Middels VMWare Work Space One (WSO) wordt de laptop remote beheerd en bedrijfsbeleid afgedwongen.

4.3 Virtuele desktop

Als virtuele desktop wordt alleen gebruik gemaakt van VMWare Horizon View. Deze is hardware en operating systeem (OS) onafhankelijk. Parkstad IT hanteert Microsoft Windows Desktop als standaard. Naast de reguliere Desktop is ook de performance Desktop beschikbaar. Thuiswerken behoort tot de mogelijkheden. Alle klanten gebruiken hetzelfde Win10 template en specifieke applicaties worden virtueel aangeboden. De virtuele Desktop Work Space One (WSO) van VMWare is bij Parkstad-IT ook de standaard voor Mobile Device Management (MDM).

4.4 Printers

Middels “follow me” wordt geprint. De multifunctionele apparaten kunnen eveneens scannen, kopiëren en faxen. Vanwege de ketenrelaties (MCC 112) worden enkele afwijkende printers eveneens ondersteund. In 2022 wordt “follow me” printen als generieke dienst aangeboden door Parkstad IT na gezamenlijk doorlopen van Europese Aanbesteding GT Print.

4.5 Overige randapparatuur

Alleen randapparatuur welke voldoet aan de standaard van Parkstad-IT mag gekoppeld worden aan het interne netwerk en wordt door Parkstad-IT ondersteund.

Randapparatuur met een “embedded operating system” (Bv Windows ingebouwd in de randapparatuur) welke niet door Parkstad IT is ontwikkeld kan Parkstad IT niet ondersteunen en in beheer nemen.

De software / firmware moet actueel zijn en voorzien van support en updates, ip-instellingen instelbaar, koppeling minimaal CAT5, eventuele bestandsoverdracht middels minimaal SMB v2 / Secured (sFTP). De gebruikersnaam en wachtwoord zijn instelbaar.

In de Producten & Diensten Catalogus van Parkstad-IT zijn overzichten opgenomen van de standaard door Parkstad-IT ondersteunde on-premise hardware- en softwareproducten.

5. Software

Als besturingssysteem voor de werkplekken geldt Windows 10 (build 20H2) met Microsoft Edge (op basis van chromium) als standaard browser. Derhalve moeten nieuwe applicaties Windows 10/ MS Office Pro Plus geschikt zijn. Werkplekken niet afkomstig van Parkstad-IT, worden niet ondersteund en worden niet in het netwerk opgenomen. Niet alle GR-PIT deelnemers zitten anno juni 2022 op de nieuwste Windows build.

5.1 Systeemsoftware

Standaard gebruikt Parkstad-IT de volgende systeemsoftware:

- VMWare tbv server en werkplek virtualisatie
- SCCM 2012
- AppVolumes
- AppV

- MSI
- ThinApp
- UEM
- Trend Micro
- Edge
- Oracle

De standaard kantoorautomatisering software is MS Office Pro Plus uit de Office 365 suite.

VMWare View wordt ingezet voor werkplek en applicatie virtualisatie. Gewerkt wordt met de principes van “linked clone” en “non-persistent pool”. Applicaties worden middels AppVolumes virtueel aangeboden.

5.2 Drive-letters

Drive-letters uniformering voor alle GR-PIT deelnemers:

- Vanwege applicatie ontwikkeling v.w.b. o.a. WorkspaceOne (WSO) en AppVolumes, is het noodzakelijk dat er gekozen wordt voor alleen de basis driveletters “V” en “P”. “V” voor de gemeenschappelijk omgeving en “P” voor de persoonlijke omgeving.

5.3 Gebruik

De gebruiker krijgt voor de werking beperkte rechten en de applicatie mag tijdens de normale werking géén data en/of settings (register) wegschrijven naar de lokale Desktop. Eveneens is het wegschrijven van data naar het gebruikersprofiel niet toegestaan. Licentie activatie op basis van hardware kenmerken is niet toegestaan.

6. Computerservers

6.1 Intel servers

DellEMC is de server standaard van Parkstad-IT en deze wordt regelmatig aangepast aan de laatste ontwikkelingen. Servers worden middels VMWare ESX virtueel aangeboden. Om optimaal gebruik van de totale servercapaciteit en serverbeschikbaarheid te garanderen, wordt VMWare DRS en VMWare HA ingezet over twee geografische gespreide datacenters.

DellEMC VxRails worden ingezet als hardware voor zowel server- als werkplek virtualisatie. De VxRails ten behoeve van de werkplek virtualisatie zijn eveneens voorzien van Nvidia GRID kaarten voor een betere grafische beleving.

De infrastructuur componenten zijn software defined als voorbereiding op een hybride omgeving tussen on-premise en cloud.

6.2 Oracle platform

OracleVM en Linux OS vormen de basis voor de Oracle databases. Oracle versie 19 is de standaard.

De systemen zijn gekoppeld aan de EMC Unity SAN middels VPLEX.

6.3 Storage

Parkstad-IT maakt gebruik van de volgende storage systemen:

- 2 x EMC Unity 550F (Full flash inclusief VPLEX);
- 2 x EMC Unity 450F (Full flash inclusief VPLEX);
- Brocade fiber switches (32 Gb/s).

Voor de back-up van alle data/servers wordt Veeam ingezet.

6.4 Systeemsoftware

Het gewenste besturingssysteem op de virtuele servers is Windows 2022.

Een typische onderverdeling is:

- A. Business applicaties (Financiën, HRM, etc.);
- B. Front-end desktop applicaties (KA);
- C. Back-end applicaties (e-mail service, telefonie, conferencing services).

De Business applicaties behoren tot de Informatie architectuur en zijn de verantwoordelijkheid van de klant. Front-end en back-end applicaties behoren tot de IT-Infrastructuur en zijn de verantwoordelijkheid van Parkstad-IT. Onderkent wordt dat beiden gemeenschappelijke belangen hebben.

7. Monitoring

Voor de monitoring van onze ICT-infrastructuur wordt gebruik gemaakt van:

- NetCrunch voor Windows systeembewaking;
- NOD32 als virusscanning op Windows en Exchange servers;
- Nieuwe servers worden middels een VMWare template uitgerold;
- Oracle Enterprise Manager monitort de Oracle omgeving;
- Orion monitort de netwerkomgeving;
- TrendMicro wordt gebruikt als virusscanner op de Windows werkplekken.

8. Database platformen

Parkstad-IT ondersteunt standaard de volgende database types:

- SQL-server 2022 (named instance);
- Oracle 19 op Linux;

De SQL-database draait niet op de applicatieserver maar op een databaseserver omwille van licentie-gebruik. De toepassing (Oracle cliënt) mag geen speciale eisen stellen aan "Default Home" op de PC.

9. Netwerk

9.1 Centraal

In de datacenters staan Cisco 6513 als een VSS cluster waar alle servers aan gekoppeld zijn. Hieraan gekoppeld zijn dubbele Cisco 4509 switches welke de koppeling vormen richting distributie switches en netwerken. De transitie naar Cisco ACI is in volle gang waardoor de netwerkcore migreert van traditioneel naar ACI.

De communicatie met de buitenwereld wordt afgehandeld middels een uitgebreid FortiNet platform. Iedere Parkstad-IT klant heeft een eigen virtuele Firewall (vDOM).

De internetkoppeling bestaat uit een rechtstreekse 10 Gb/s verbinding met AMS-IX in Amsterdam en is redundant uitgevoerd.

In 2022 is de implementatie van Cisco DNA (Software Defined Networking voor end devices) gestart. De Cisco Nexus 9K modellen worden steeds prominenter in het datacenter. In 2022 wordt eveneens het datacenter netwerk vervangen door Cisco ACI (Software Defined Networking voor datacenter). Het bovengenoemde Cisco 6513 VSS cluster komt te vervallen.

9.2 WAN

De klantlocaties op de hoofdring zijn in een Wide Area Network (WAN) gekoppeld met een 10 Gb/s darkfiber verbinding. Subringen naar kleinere locaties zijn gekoppeld met een 1 Gb/s dark fiber.

Kleine locaties zoals sporthallen, begraafplaatsen zijn over het internet gekoppeld middels een VPN-tunnel.

9.3 LAN

PC's zijn in Local Area Networks (LAN) gekoppeld middels 1 Gb full duplex waarbij TCP/IP als netwerkprotocol wordt gebruikt.

9.4 Netwerk software

Voor de monitoring van het netwerk wordt Orion ingezet. Alle actieve componenten worden bewaakt en alarmering is ingeregeld. De Helpdesk van Parkstad-IT beschikt eveneens over een visualisatie van het netwerk en ziet de actuele status.

Cisco DNA en Cisco ACI ten behoeve van Software Defined Networking (SDN).

10. Licenties

Parkstad-IT stelt software uitsluitend beschikbaar als aan de licentievoorwaarden van de leverancier is voldaan. Het invoeren van de licenties moet geschieden volgens een van onderstaande principes;

- Licentie activatie middels de Microsoft Azure Cloud;
- De toepassing heeft een generieke licentiecode voor alle installaties zodat speciale activering procedures per installatie niet nodig is;
- De toepassing heeft een "papieren" licentiecode en activering is niet nodig;
- De toepassing heeft een licentiebestand welke centraal te plaatsen is;
- De toepassing is licentiecode vrij.

Als de toepassing is voorzien van een hardware licentie in de vorm van een “dongle”, dan moet dit een USB “dongle” zijn. De applicatie moet dan de mogelijkheid ondersteunen deze centraal aan te bieden via het ip-netwerk. Een overweging is eveneens om te werken met een licentievorm op basis van concurrent users in plaats van named users.

11. Randapparatuur

Als aan de toepassing specifieke randapparatuur wordt gekoppeld, zal Parkstad-IT deze randapparatuur vooraf dienen te beoordelen. De koppeling is gestandaardiseerd op een RJ45 netwerkaansluiting. In uitzondering wordt apparatuur gekoppeld middels WiFi.

Alleen randapparatuur welke voldoet aan de standaard van Parkstad-IT mag gekoppeld worden aan het netwerk en wordt door Parkstad-IT ondersteund.

Randapparatuur met een “embedded operating system” (Bv Windows ingebouwd in de randapparatuur) welke niet door Parkstad IT is ontwikkeld, kan Parkstad-IT niet ondersteunen en in beheer nemen.

Het gebruik van lokale modems direct gekoppeld aan werkplekken is niet toegestaan.

Voor ondersteuning van de leverancier kan gebruik worden gemaakt van de faciliteit “telewerk voor leveranciers toegang”. In overleg met Parkstad-IT kan bekeken worden onder welke strikte regels de leverancier op afstand toegang kan krijgen tot de systemen.

12. Security

Parkstad-IT werkt volgens de BIO (Baseline Informatiebeveiliging Overheid) die een afgeleide is van de ISO-27001 standaarden. Dit houdt ook in dat de afgenomen dienst een BBN classificatie (Basis Beveiliging Niveau) krijgt en dat aan de hand daarvan een selectie van maatregelen genomen dient te worden aan de kant van de betrokken partijen.

Indien dit niet specifiek vermeld wordt, gaan we uit van de classificatie BBN2 en alle maatregelen die hierbij horen. Bij het inpassen van een dienst of product wordt samen met de Security Officer een vertaling gemaakt welke maatregelen extra aandacht behoeven.

De overheid volgt de standaarden die op de ‘pas toe of leg uit’-lijst van het Forum Standaardisatie staan. De BIO is gebaseerd op de NEN-ISO/IEC 27002:2017 en vanuit de BIO wordt verwezen naar de NEN-ISO/IEC 27001:2017. Het aansluiten van SAAS producten gebeurt door middel van koppelingen die daarvoor bedoeld zijn en met inachtneming van de richtlijnen van forum voor standaardisatie (denk aan bijvoorbeeld TLS en PKI overheid certificaten).

De ICT-infrastructuur van PIT wordt gedeeld met meerdere partijen. Dat houdt ook in dat we een afweging maken of een dienst alleen beschikbaar gemaakt wordt voor 1 GR-PIT deelnemer of voor allen. Keuzes kunnen invloed hebben om 1 of meerdere deelnemers en in extreme gevallen zullen we deze ook moeten betrekken bij beslissingen waarbij zij het risico delen. Veel van de infrastructuur is gesegmenteerd om onder andere risico's te beperken. Bij de overdracht van informatie van de ene zone naar de andere worden passende logische toegangscontroles ingericht. Denk aan inspectie, authenticatie en gebruik van veilige protocollen.

Het beheer in de ICT-infrastructuur (ook op afstand) gebeurt onder toezicht van een systeembeheerder en wordt gelogd in daartoe behorende systemen. Wijzigingen op configuratie items gebeuren pas na goedkeuring door de Changemanager van Parkstad-IT en worden vastgelegd in Topdesk.

Parkstad-IT gaat er vanuit dat bij een nieuwe dienst de beveiligingseisen expliciet zijn opgenomen in de met de productleverancier afgesloten contracten. Dat KPI's zijn vastgelegd en rapportages hierover zijn meegenomen in de aangeboden oplossing. Als de aangeboden oplossing zelf risico's bevat, zal de aanbieder met een risicoafweging helder moet maken wat de consequenties hiervan zijn voor de organisatie. Expliciet moet zijn gemaakt welke risico-consequenties geaccepteerd worden en welke gemitigeerd moeten zijn met passende maatregelen bij het aangaan van de overeenkomst.

Parkstad-IT vereist dat een aanbieder ook de GBIT voorwaarden volgt. GIBIT staat voor Gemeentelijke Inkoopvoorwaarden bij IT. Deze uniforme inkoopvoorwaarden helpen gemeenten bij het professionaliseren van de inkoop van haar ICT-diensten en –producten.