

## **Bijlage C.3 ICT Richtlijnen en randvoorwaarden**

**1. Definities**

**2. Hosting**

**3. Richtlijnen en randvoorwaarden**

**3.1. Inleiding**

**3.2. Richtlijnen (principes)**

**3.2.1. Inleiding**

**3.2.2. Algemene principes**

**3.2.3. Beveiligingsrichtlijnen voor Webapplicaties**

**3.3. Randvoorwaarden**

**3.3.1. Huidige infrastructuur**

**3.3.2. Huidig applicatielandschap**

# 1. Definities

## Technisch Beheer

Richt zich op het in stand houden, beheren en onderhoud van de IT-infrastructuur en heeft ITIL als standaard. De IT-infrastructuur (zie figuur 1, paragraaf 3.3.1) is de basis waarop applicaties kunnen draaien en bestaat uit het netwerk, de computers en operating systems en overige randapparatuur. KPN voert voor de VRH dit beheer uit. In het geval van applicaties die door een leverancier worden gehost (bijvoorbeeld ingeval van SAAS, software as a service) is het technisch beheer een verantwoordelijkheid van de betreffende leverancier.

## Applicatiebeheer

Onder dit beheer wordt verstaan het in stand houden van de bedrijfsapplicaties en gegevensverzamelingen van de organisatie. Applicatiebeheer houdt zich bezig met de creatie, beheer en wijzigen van applicaties naar aanleiding van geconstateerde fouten of veranderende technische of functionele eisen. ASL is hiervoor de standaard. ASL is nieuwer dan en deels geïnspireerd door ITIL.

Binnen de VRH is het uitgangspunt dat applicatiebeheer een taak van de leverancier van de applicatie is, omdat dit over het algemeen applicatie-specifieke technische kennis vereist.

## Functioneel beheer

Functioneel beheer houdt zich bezig met het beheren van de informatievoorziening in een organisatie. De bedrijfsapplicaties worden gebruikt door de gebruikersorganisatie en moeten eventueel aan veranderende eisen worden aangepast. Het beschrijven van deze wijzigingen, het (laten) doorvoeren van de voorgestelde wijzigingen en het controleren van de wijzigingen behoort tot het takenpakket van de Functioneel Beheerders van de VRH. Functioneel Beheer heeft als standaard BiSL. Functioneel Beheer is in basis de enige vorm van beheer die door de VRH zelf wordt gedaan.

## Hosting

Het leveren, beheren en onderhouden van de infrastructuur (inclusief verbindingen) en de beschikbaar gestelde applicatie, bijvoorbeeld als SAAS.

## Beschikbaarheid

De totale tijdsduur waarin VRH daadwerkelijk van de applicatie gebruik heeft kunnen maken uitgedrukt in een percentage van de totale tijdsduur gemeten gedurende één (1) kalendermaand. Gepland onderhoud wordt niet meegerekend bij het bepalen van de beschikbaarheid (het beschikbaarheidspercentage).

### Single Sign-On

Uitgangspunt dat gebruiker met zijn bestaande VRH-account de applicatie kan gebruiken binnen de toegekende autorisaties:

- De gebruiker krijgt géén aparte inloggegevens voor de applicatie, hiervoor wordt het VRH-account gebruikt.
- Als de gebruiker al op een VRH-werkplek is ingelogd met zijn VRH-account, dan wordt hij automatisch hiermee ingelogd in de applicatie.
- Als de gebruiker op een niet-VRH-werkplek werkt, dan krijgt hij na één keer inloggen met zijn VRH-account toegang tot de applicatie.

### Systeem

Onder systeem wordt in dit document verstaan een geautomatiseerd informatiesysteem waarmee informatie over objecten of personen beheerd - verzameld, bewerkt, geanalyseerd, geïntegreerd en gepresenteerd - kan worden. Een systeem omvat hardware (de technische infrastructuur) en software (de applicatie).

## 2. Hosting

In 2012 heeft de directie van de VRH *Het Nieuwe Werken ambitie 2015* geaccordeerd. In dit document staan de volgende opmerkingen die in dit kader relevant zijn:

- "ICT-middelen en kantoorautomatisering gericht op 'anywhere, anytime, any device'".
- "De VRH wil inzetten op web-based oplossingen zoals SAAS en cloud computing".

Met de implementatie van Het Nieuwe Werken is gekozen voor het beleid "Cloud tenzij". Dat betekent dat de VRH steeds meer afstapt van het aanbieden van applicaties uit een "eigen" serveromgeving. In plaats daarvan worden applicaties door leverancier kant en klaar aangeboden, vaak in een abonnementsmodel. Daarbij zijn de zorgen voor servers, technische prestaties, licenties, etcetera, voor de leverancier. De VRH is betrokken bij het functionele beheer van deze omgevingen.

Steeds meer medewerkers bij de VRH werken met verschillende applicaties. Om het gebruikersgemak te verhogen, wordt gewerkt met Single Sign-On. Als een gebruiker is ingelogd op een VRH-werkplek kan een aangesloten applicatie worden opgestart via Single Sign-On, zonder dat aparte aanmelding bij de applicatie nodig is. Het moet hiertoe mogelijk zijn voor de applicaties om aan te sluiten op de Active Directory van de VRH.

### 3. Richtlijnen en randvoorwaarden

#### 3.1 Inleiding

Dit document beschrijft de richtlijnen (architectuur en informatiebeleid) en randvoorwaarden als van toepassing op het aan te besteden systeem. Dit document is vanuit de huidige ICT infrastructuur te zien als een eis waar het aan te bieden systeem aan dient te voldoen. Het document vormt overkoepelend het kader voor het programma van eisen en wensen (Bijlage A.4 aanbestedingsleidraad).

Als bijlage bij de aanbesteding zijn het informatiebeleid VRH 2015-2020 (Bijlage C.8) en de Veiligheidsregio Referentie Architectuur, de VeRA (Bijlage C.9) meegestuurd. Deze documenten vormen, samen met dit document, het ICT kader voor deze aanbesteding.

#### 3.2 Richtlijnen (principes)

##### 3.2.1 Inleiding

VRH heeft een aantal principes voor de informatievoorziening benoemd. Deze principes zijn in deze paragraaf beschreven. De eisen die hieruit voortkomen zijn opgenomen in Bijlage A.4 van de aanbestedingsleidraad.

##### 3.2.2 Algemene principes

|            |  |
|------------|--|
| VRH-A-1    | Eenmalige invoer, meervoudig gebruik   |
| Statement  | Gegevens worden bij de bron gehaald  |
| Rationale  | <u>Toelichting:</u><br>Om maximale consistentie te bereiken in vastlegging van gegevens die in meerdere systemen nodig zijn is het van groot belang om deze eenmalig in te voeren.<br><u>Voorbeeld:</u><br>Medewerkergegevens worden op veel plaatsen in de organisatie gebruikt en het is wenselijk dat gegevens niet steeds opnieuw ingevoerd hoeven te worden |
| Implicatie | <ul style="list-style-type: none"><li>Indien van toepassing zullen er koppelingen moeten komen met systemen van andere organisaties en met interne kernregistraties</li></ul>  |

|            |  |
|------------|--|
| VRH-A-2    | Koppelbaar   |
| Statement  | Voor uitwisseling van gegevens wordt gewerkt met open standaarden  |
| Rationale  | <p><u>Toelichting:</u><br/>De VRH werkt in meerdere ketenprocessen samen met ketenpartners. Naast het onderling kunnen uitwisselen van gegevens moet er ook gegevens met financiële instellingen uitgewisseld kunnen worden. Gebruik van een gegeven uit een ander systeem dient conform open standaarden te gaan zodat bij eventuele vervanging van een van de systemen koppelingen zoveel mogelijk in stand kunnen worden gehouden.</p> <p><u>Voorbeeld:</u><br/>Bij de uitwisseling van financiële gegevens met bijvoorbeeld de BNG worden open standaarden gebruikt.</p> |
| Implicatie | <ul style="list-style-type: none"> <li>• De relevante open standaarden voor koppelingen met andere systemen dienen te worden ondersteund</li> </ul>  |

|            |  |
|------------|--|
| VRH-A-3    | Kernregistratie medewerkers  |
| Statement  | Gegevens over medewerkers worden door verschillende bronnen geleverd aan de Kernregistratie Medewerkers, waar deze gegevens ook weer voor afnemers beschikbaar zijn  |
| Rationale  | <p><u>Toelichting:</u><br/>De Kernregistratie Medewerkers is het centrale punt voor die medewerkergegevens die door meerdere processen worden gebruikt. In 2017 wordt de Kernregistratie Medewerkers binnen VRH in gebruik genomen. Het streven is om het aantal directe koppelingen tussen systemen te minimaliseren en levering en afname van medewerkergegevens via de Kernregistratie Medewerkers te laten verlopen.</p> |
| Implicatie | <ul style="list-style-type: none"> <li>• Bronhouders moeten medewerkergegevens die in meerdere processen gebruikt worden leveren aan de Kernregistratie Medewerkers</li> <li>• Afnemers moeten medewerkergegevens afnemen van de Kernregistratie Medewerkers</li> </ul>  |

|            |   |
|------------|---|
| VRH-A-4    | Doelmatig gebruik   |
| Statement  | Gebruik gemeenschappelijke systemen   |
| Rationale  | <p><u>Toelichting:</u><br/> Indien er vanuit meerdere (bedrijfs)processen en (bedrijfs)activiteiten behoefte is aan functionaliteit, zal hiervoor indien mogelijk een reeds aanwezig systeem of module worden ingezet. Indien een gemeenschappelijk systeem er nog niet is of noodzakelijke functionaliteit ontbeert, zal er een nieuw systeem of module moeten worden verworven.</p>   |
| Implicatie | <ul style="list-style-type: none"> <li>• Indien functionaliteit, beveiliging en kosten gelijkwaardig zijn, verdient het de aanbeveling om zoveel mogelijk gemeenschappelijke systemen te gebruiken. Oftewel: bestaande functionaliteit dient zoveel mogelijk hergebruikt te worden</li> <li>• Indien een oplossing voor meerdere (bedrijfs)processen en (bedrijfs)activiteiten wordt ingezet is zij modulair van opzet waarbij de componenten afzonderlijk zijn te gebruiken en afzonderlijk van elkaar zijn te vervangen.</li> <li>• Het modulaire karakter is belangrijk: een applicatieve functie is een afgebakend geheel aan functionaliteiten, dat als zodanig vervangen kan worden.</li> </ul> |

|            |  |
|------------|--|
| VRH-A-5    | Beschikbaarheid  |
| Statement  | Zorg voor informatie die in alle gevallen 24/7 raadpleegbaar is  |
| Rationale  | <p><u>Toelichting:</u><br/> Een aantal systemen worden gebruikt tijdens incidenten, crisis of rampen. Op die momenten is beschikbaarheid, performance en capaciteit van functionaliteit en/of gegevens van groot belang. Daarnaast zijn er systemen die gegevens leveren ten behoeve van de systemen die tijdens een incidenten, crisis of rampen worden gebruikt.</p> <p><u>Voorbeeld:</u><br/> De VRH kent medewerkers met een reguliere dagtaak en medewerkers met een taak binnen de repressieve dienst en/of een piket functie. Zij voeren administratieve werkzaamheden op onregelmatige tijden uit.</p> |
| Implicatie | <ul style="list-style-type: none"> <li>• Indien een systeem gegevens bevat die tijdens een incident, crisis of ramp geraadpleegd kunnen worden, zullen er specifieke maatregelen moeten worden genomen met betrekking tot beschikbaarheid van de gegevens.</li> </ul>  |

|            |  |
|------------|--|
| VRH-A-6    | Bewezen betrouwbaar  |
| Statement  | Gebruik bij voorkeur bewezen standaard oplossingen   |
| Rationale  | <u>Toelichting:</u><br>Een overheidsorganisatie die actief is in de veiligheidsketen zal bij uitstek betrouwbaar moeten zijn. Dit betekent dat systemen die daarbij gebruikt worden ook een bewezen betrouwbaarheid moeten hebben. Bij voorkeur wordt hierbij gebruik gemaakt van informatiesystemen die reeds bij vergelijkbare organisatie in omvang/complexiteit in gebruik zijn. |
| Implicatie | <ul style="list-style-type: none"> <li>• Indien er toch een specifieke oplossing moet worden ontwikkeld (maatwerk) dan stelt dit hoge eisen aan het test traject (bijvoorbeeld testen tijdens oefeningen)</li> </ul>   |

|            |   |
|------------|---|
| VRH-A-7    | Het Nieuwe Werken   |
| Statement  | Locatie- en tijdonafhankelijk werken is de norm   |
| Rationale  | <u>Toelichting:</u><br>Werkzaamheden binnen een veiligheidsregio vinden nadrukkelijk verspreid plaats, zowel op VRH locaties als op locaties van derden zoals het kantoor van de landelijke organisaties in Arnhem. Ook zijn er werkzaamheden die zich niet houden aan reguliere kantoor tijden. Daarnaast verandert de maatschappij in haar houding t.o.v. werk.<br><u>Voorbeeld:</u><br>Een aantal medewerkers van de VRH hebben zowel een reguliere dagtaak en een taak binnen de repressieve dienst en/of een piket functie. Daarnaast vinden de werkzaamheden van de VRH plaats over diverse locaties. |
| Implicatie | <ul style="list-style-type: none"> <li>• Oplossingen dienen bij voorkeur web gebaseerd te worden aangeboden</li> </ul>  |

|            |   |
|------------|---|
| VRH-A-8    | Documentenbeheer  |
| Statement  | Documenten worden opgeslagen met behulp van document management functionaliteit   |
| Rationale  | <u>Toelichting:</u><br>Documenten dienen op een gestructureerde manier te worden opgeslagen zodat deze documenten met meerdere personen kunnen worden gedeeld. Documenten zijn via meerdere ingangen vindbaar zijn voor geautoriseerde gebruikers.<br><u>Voorbeeld:</u><br>Het financiële dossier omvat document management functionaliteit en heeft de mogelijkheid om documenten op een afgesproken moment over te dragen aan het record management systeem |
| Implicatie | <ul style="list-style-type: none"> <li>• Vanuit andere systemen zal een koppeling moeten kunnen worden gemaakt met een documenten beheer systeem</li> <li>• Papier documenten worden gescand en digitaal aangeboden</li> </ul>  |

|            |   |
|------------|---|
| VRH-A-9    | Record management   |
| Statement  | Documenten worden gearhiveerd in een record management systeem  |
| Rationale  | <p><u>Toelichting:</u><br/>De archivering van documenten vindt plaats in een record management applicatie. Document management systemen leveren documenten aan bij het record management systeem op een nader vast te stellen moment</p> <p><u>Voorbeeld:</u><br/>Vernietigingstermijnen e.d. worden centraal vanuit het record management systeem bewaakt.</p> |
| Implicatie | <ul style="list-style-type: none"> <li>Document management systemen moeten documenten kunnen aanbieden bij het record management systeem, waarna het document management systeem de eigen versie verwijdert (zodat er geen dubbelingen van het document ontstaan, met alle mogelijke onduidelijkheden van dien)</li> </ul>                                      |

|            |  |
|------------|--|
| VRH-A-10   | Informatiebeveiliging & privacy  |
| Statement  | De gegevens binnen de informatievoorziening van de VRH worden te allen tijde veilig beheerd, om de risico's met betrekking tot beschikbaarheid, integriteit en vertrouwelijkheid tot een aanvaardbaar niveau te reduceren.   |
| Rationale  | <p><u>Toelichting:</u><br/>De opslag en de uitwisseling van (persoons)gegevens van VRH en onze (keten)partners vindt veilig plaats, conform vigerende wet- en regelgeving, waaronder de Wet bescherming persoonsgegevens en het Auditkader Informatieveiligheid Veiligheidsregio's. Conform de risicogedreven aanpak betekent dit dat gegevens beschikbaar zijn op het moment dat ze nodig zijn (beschikbaarheid), ze juist en volledig zijn (integriteit) en slechts toegankelijk voor bevoegde personen (vertrouwelijkheid).</p> |
| Implicatie | <ul style="list-style-type: none"> <li>Externe (beheer)partijen welke voor VRH gegevens bewerken of verwerken zijn gehouden aan de voor VRH of leverancier van toepassing zijnde wet- en regelgeving. In contracten tussen VRH en deze partijen worden de afspraken hieromtrent specifiek en concreet gemaakt. Monitoring op de uitvoering vindt plaats door een ingerichte audit- en rapportagecyclus.</li> </ul>   |

### 3.2.3 ICT-Beveiligingsrichtlijnen voor Webapplicaties

De leverancier van de webapplicatie dient te voldoen aan een optimaal veilig ingerichte dienstverlening van de webapplicatie. De hierbij toegepaste beveiligingsmaatregelen hebben niet alleen betrekking op de webapplicatie zelf, maar ook op de beheeromgeving en de omringende hard- en softwareomgeving, die noodzakelijk is om de webapplicatie te laten functioneren.

De leverancier dient hiervoor aantoonbaar de volgende domeinen te hebben ingericht:

### **Beleidsdomein**

Beschrijving van randvoorwaarden op strategisch niveau, om de webapplicatie veilig te doen functioneren, zodat de juiste ondersteuning wordt geleverd voor het bereiken van de afgesproken doelstellingen. Bevat conditionele en randvoorwaardelijke elementen die van toepassing zijn op de overige lagen, zoals doelstellingen, informatiebeveiligingsbeleid, strategie en vernieuwing, organisatiestructuur en architectuur.

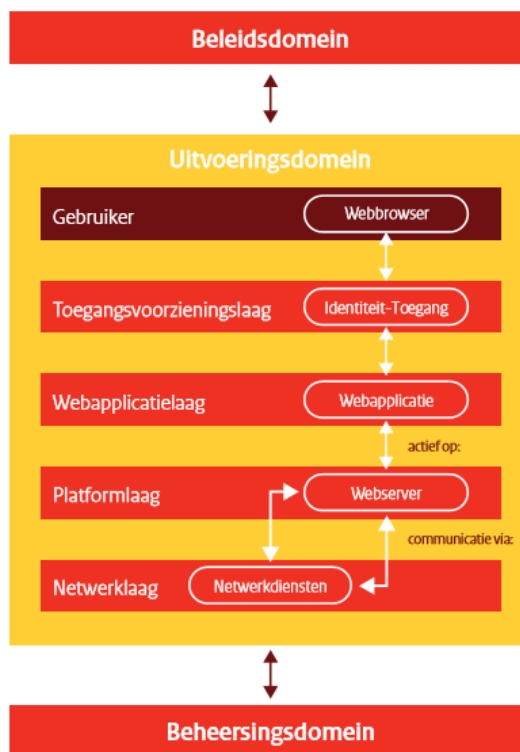
### **Uitvoeringsdomein**

Beschrijving van beveiligingsmaatregelen van de infrastructuur rondom de webapplicatie, zoals toegangsvoorzieningen, de webapplicatie zelf, het platform, webservers en netwerken.

### **Beheersingsdomein**

Beschrijving van evaluatieaspecten en meetaspecten, evenals de beheerprocessen die noodzakelijk zijn voor de instandhouding van de ICT-diensten rondom de webapplicatie.

De onderstaande afbeelding vat de inrichting van deze domeinen samen:



Zie voor een nadere toelichting het document 'ICT-Beveiligingsrichtlijnen voor Webapplicaties' van het Nationaal Cyber Security Centrum d.d. september 2015.

## 3.3 Randvoorwaarden

### 3.3.1 Huidige ICT-infrastructuur

De VRH heeft levering en beheer van de ICT-infrastructuur, inclusief netwerken, in zijn geheel uitbesteed. Sinds 1-1-2016 is de dienstverlening voor deze omgeving bij KPN ondergebracht (zie ook Figuur 1 Technische infrastructuur architectuur). VRH heeft functioneel beheer, informatie-management en contractmanagement intern belegd. De huidige kantoorautomatisering wordt via een Citrix-omgeving aangeboden aan de gebruikers. Een deel van de medewerkers heeft een laptop waarop de kantoorautomatisering van de VRH via een Citrix-omgeving wordt aangeboden. Verder zijn op alle VRH-kazernes desktops met Citrix-toegang tot de kantoorautomatisering aanwezig. In het kader van Het Nieuwe Werken is de Citrix-omgeving ook te benaderen vanaf een willekeurige PC (bijvoorbeeld een PC thuis). Iedere medewerker van de VRH heeft een VRH-account (gebruikersnaam en wachtwoord). Uitgangspunt dat een gebruiker met zijn bestaande VRH-account de applicaties kan gebruiken binnen de toegekende autorisaties (Single Sign-On). Applicaties zijn gehost bij de leverancier van de ICT-infrastructuur of gehost door of namens de leverancier van een specifieke applicatie. Voor printen en scannen beschikt de VRH over multifunctionals met OCR-functionaliteit.

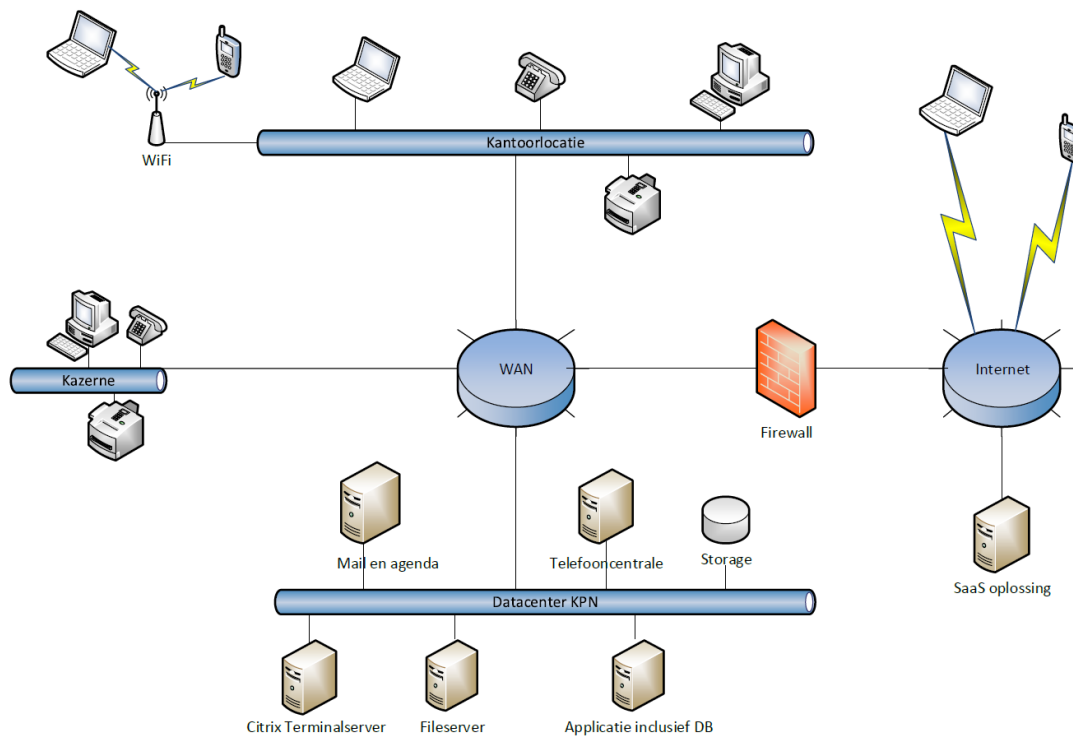
Het besturingssysteem op de VRH-werkplekken is Windows 8 (64 bit). Hierop draait binnen de Citrix-omgeving standaard MS Office 2013, MS Internet Explorer 11 en Chrome. De VRH heeft hierbij de voorkeur voor IE11 omdat KPN deze browser beter kan ondersteunen.

Overige voorwaarden voor aansluiting op de technische infrastructuur:

- Systemen moeten om in staat zijn om aan te sluiten op de multi tenant terminal server omgeving van KPN.
- Het internet-verkeer tussen het te leveren systeem en de VRH-infrastructuur verloopt middels een proxy, het te leveren systeem moet op deze wijze kunnen werken.
- Voor aansluiting op de Active Directory van de VRH (ten behoeve van Single Sign-On) wordt ondersteuning van ADFS gevraagd. Indien dit niet mogelijk is kan als alternatief SAML worden gebruikt als koppelvlak.
- Het te leveren systeem maakt bij voorkeur geen gebruik maken van Java, omdat ondersteuning hierop bewerkelijk is.

De functionaliteit die in deze opdracht wordt gevraagd moet op de volgende platforms gebruikt kunnen worden:

- VRH-werkplekken (laptop en desktop)
- Werkplekken die niet door de VRH worden beheerd en aangeboden zoals thuis PC's;



Figuur 1 Technische infrastructuur architectuur

### 3.3.2 Huidig applicatielandschap

In deze paragraaf is een beschrijving opgenomen van het huidige applicatielandschap bij de VRH, voor zover relevant voor de huidige opdracht. Een systeem is relevant als:

- het nu functionaliteit biedt die als onderdeel van deze opdracht wordt vervangen
- het gegevens bevat of kan bevatten die uitgewisseld worden of kunnen worden met de te selecteren applicatie

| Element                  | Systeem (leverancier)                  | Toelichting |
|--------------------------|--|-------------|
| Financiële administratie | Exact Financials                       |             |
| Factuurverwerking        | Exact Synergy Enterprise               |             |
| Scan en coderen facturen | Scan en herkensoftware (Scansys)       |             |
| Rapportage en analyse    | Speedbooks                             |             |
| Multifunctionals         | Ricoh                                  |             |
| Workflow                 | Onderdeel van Exact Synergy Enterprise |             |
| Archief (DMS & RMA)      | Onderdeel van Exact Financials         |             |

Onderstaande tabel geeft een beeld van de relaties van het financiële systeem en gerelateerde systemen en voorzieningen.

| <b>Element</b>                                  | <b>Systeem (leverancier)</b>                 | <b>Hosting</b> | <b>Toelichting</b>   |
|---|--|----------------|--|
| Personeelsregistratie en salarisadministratie   | Workforce (ADP)                              | ADP            | In 2014 heeft de VRH het personeels- en salarissysteem Workforce van ADP aangeschaft. Betalingsgegevens worden vanuit de salarisadministratie in Workforce periodiek overgedragen naar de te selecteren financiële applicatie.               |
| Facilitair Management Informatie Systeem (FMIS) | Axxerion                                     | KPN            | In FMIS is onder andere de registratie voor contractmanagement ondergebracht.  |
| Document Management Systeem (DMS)               | Corsa (BCT)                                  | BCT            | In 2013 heeft de VRH het DMS Corsa van BCT aangeschaft. Dit systeem wordt gebruikt voor dossiervorming, archivering en postregistratie. In dit systeem worden wel financiële beleidsstukken maar geen facturen opgeslagen.                   |
| Managementinformatie (Business Intelligence)    | Datawarehouse en BI-tool QlikSense (Qlik)    | KPN            | In 2016 heeft de VRH een datawarehouse in gebruik genomen. Als visualisatietool voor dashboards en analyse wordt QlikSense gebruikt. Er is nog geen koppeling tussen het huidige financiële systeem en het datawarehouse tot stand gebracht. |
| Kernregistratie Medewerkers                     | IAM Identity- & Accesmanagement (Tools4Ever) | KPN            | Zie toelichting bij principe VRH-A-3.  |
| Identificatie                                   | Active Directory                             | KPN            | Onderdeel van kantoorautomatisering voor het realiseren van Single Sign-On.  |
| Vakbekwaamheid-managementsysteem                | AG5  |                | In 2012 geïmplementeerd om alle oefeningen en opleidingen van de operationele medewerkers te registreren.  |
| Operationele planningssoftware                  | Roster CAS                                   |                | In 2013 voor de gehele VRH ingevoerd om te komen tot één regionaal dienstrooster.  |