Den Haag

Programma van Eisen

Kernsysteem Werk en Participatie

20.388-SZW

Datum
9 april 2021
Auteur
Gemeente Den Haag, Bedrijfsvoering

0.1 Definitie van Programma van Eisen (PvE)

De functionele en niet-functionele eisen die gelden voor het Kernsysteem Werk en Participatie zijn beschreven in dit document en de hieronder vermelde bijlagen.

Bijlage nr.	Document Titel
4	GIBIT 2020 inkoopvoorwaarden
5	Gemeentelijke ICT kwaliteitsnormen v2020 2.0
12	Termenlijst Werk en Participatie
16	Baseline Informatiebeveiliging Overheid versie 1.04
18	Applicatielandschap en koppelvlakken
20	UC01 Bepalen Dienstverlening
21	UC02 Regisseren Ontwikkeling
22	UC03 Nazorg en Begeleiding na plaatsing
23	UC04 Beëindigen Dienstverlening
24	UC05 Uitvoeren Activiteit
25	UC06 Vaststellen Ontheffing
26	UC07 Bepalen Maatregel
28	Informatiebeheer – Haagse MMS (minimale metadataset)
29	Informatiebeheer - Stamtabellen
30	Tactisch beleid Logging
31	Tactisch beleid Encryptie
32	Aansluitvoorwaarden WS Gateway Externe Consumer
33	Aansluitvoorwaarden WS Gateway Provider

0.2 Terminologie

In het PvE zijn functionele -, inkoop - en gemeentelijke ICT (inkoop) termen gehanteerd.

- De functionele termen en de inkoop termen zijn beschreven respectievelijk in de Termenlijst Werk en Participatie (Bijlage '12. Termenlijst Werk en Participatie') en in Begrippenlijst van de Aanbestedingsleidraad. Deze termen zijn standaard (niet cursief) en met een hoofdletter geschreven.
- De ICT (inkoop) termen, beschreven in de *GIBIT 2020*, zijn cursief en met een hoofdletter geschreven.

INHOUDSOPGAVE

1. Kernsysteem Werk en Participatie (KWP)

1.1 Doel KWP

Het Kernsysteem Werk en Participatie (KWP) is een regiesysteem dat zich richt op de ontwikkeling van de Burger. Het doel is om mensen aan Werk te helpen, of als dat niet kan te laten participeren. De basis van het systeem is een Perspectiefplan en een proces van voortdurend leren en bijstellen.

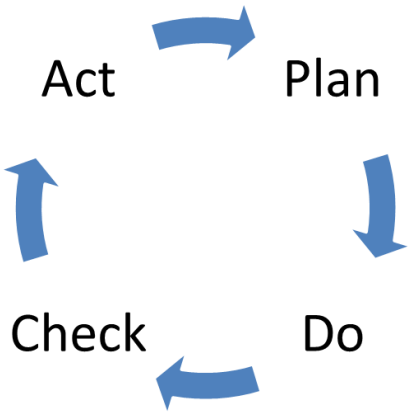
Het KWP moet uitblinken in het faciliteren van de ontwikkeling van de Burger én moet het platform zijn waarmee (in de toekomst) gekoppeld kan worden met partners zoals Instrumentenleveranciers, andere overheidsdiensten, vrijwilligersorganisaties en Werkgevers.

1.1.1 Plan

De basis van het Perspectiefplan is het Burgerprofiel waarin een accuraat en herkenbaar beeld staat van wat de Burger kan en wil. Op basis van de mogelijkheden wordt een Haalbaar perspectief opgesteld waar in meerdere stappen naartoe gewerkt wordt. Op basis van het Haalbaar perspectief en datgene wat nog ontbreekt in het Burgerprofiel wordt één of meer Activiteit(en) gepland.

1.1.2 Do

Na uitvoering van Activiteiten wordt het Resultaat meetbaar vastgelegd in het Burgerprofiel in vorm van opgedane vaardigheden, verbeterde leefgebieden, etc. De uitvoering van een Activiteit zelf wordt niet door het kernsysteem ondersteunt.



Figuur A: Plan Do Check Act

1.1.3 Check

Ontwikkeling wordt zichtbaar op basis van het Resultaat van Activiteiten. Dat bepaalt of het geplande Resultaat wordt bereikt en het Perspectiefplan nog steeds passend is.

1.1.4 Act

Indien nodig wordt het Haalbaar perspectief bijgesteld en aangescherpt, wordt gezocht naar beter passende Activiteiten en kunnen nieuwe Activiteiten worden gepland.

1.2 VNG-werklandschap als referentiekader

Gemeente Den Haag (GDH) herkent zich in en sluit zich aan bij de Dienstverlening zoals die is vormgegeven in het VNG-werklandschap. In de use cases, gebruikt bij de functionele eisen, is daarom een relatie gelegd tussen de functionele behoefte en de VNG Dienstverleningstegels, zie Figuur B.

Zie hiervoor http://www.vngrealisatie.nl/sites/default/files/2020-12/Werklandschap%202.0.pdf

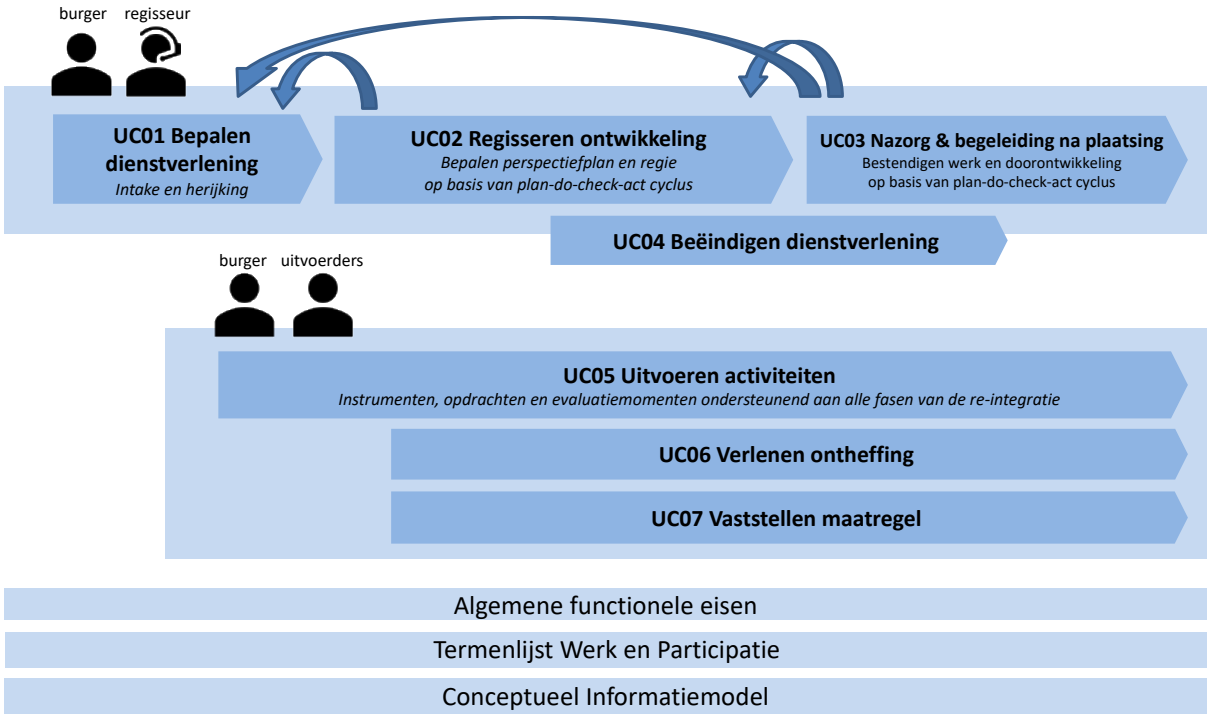
Figuur B: VNG-werklandschap werknemer

1.3 Functionele eisen

Voor de Aanbesteding van KWP is een set met functionele eisen opgesteld waar KWP minimaal aan moet voldoen.

De opbouw van de set van functionele eisen is als volgt:

1. Use cases
2. Algemene functionele eisen
3. Termenlijst Werk en Participatie
4. Conceptueel Informatiemodel



Figuur C: Overzicht van set aan functionele eisen

1.3.1 Use cases

De bijlagen '20. UC01 Bepalen Dienstverlening' tot en met '26. UC07 Bepalen Maatregel' bevatten de use cases. De use cases beschrijven procesmatig welke functionaliteit KWP dient te leveren en zijn daarmee een eis.

De use cases zijn zo functioneel mogelijk beschreven om ruimte te geven aan meerdere oplossingen. Ze beschrijven het 'WAT' en niet 'HOE' de functionaliteit ingevuld moet worden.

Er is onderscheid gemaakt in regie- en uitvoerende use cases. In de regie use cases (UC01 t/m UC04) bepalen Burger en Regisseur hoe Burger werkt aan zijn ontwikkeling door middel van zijn Perspectiefplan. In de uitvoerende use cases (UC05 t/m UC07) voeren Burger en Uitvoerder hier onderdelen van uit.

Onderstaande leeswijzer geldt voor alle use cases.

- De basic flow van een use case beschrijft de meest gangbare manier waarop het proces verloopt.
- Alternatieve flows beschrijven situaties die kunnen optreden, aanvullend op de basic flow.
- Waar Burger als actor is vermeld kan ook Professional de actor zijn, zodat minder computervaardige Burgers door Professional geholpen kunnen worden.

- Actoren maken direct gebruik van het KWP en zijn in de use case stappen schuingedrukt weergeven.
- Termen beginnen met een hoofdletter en zijn in de Termenlijst Werk en Participatie gedefinieerd.
- KWP wordt niet in alle stappen expliciet genoemd, echter alle informatie in de use cases moet gelezen worden als interactie tussen KWP en een actor en is daarmee een eis.

1.3.2 Algemene functionele eisen

Aanvullend op de use cases zijn algemene functionele eisen opgesteld. De algemene functionele eisen kennen geen specifieke volgorde en gelden voor alle use cases, zie paragraaf 2.1.

1.3.3 Termenlijst Werk en Participatie

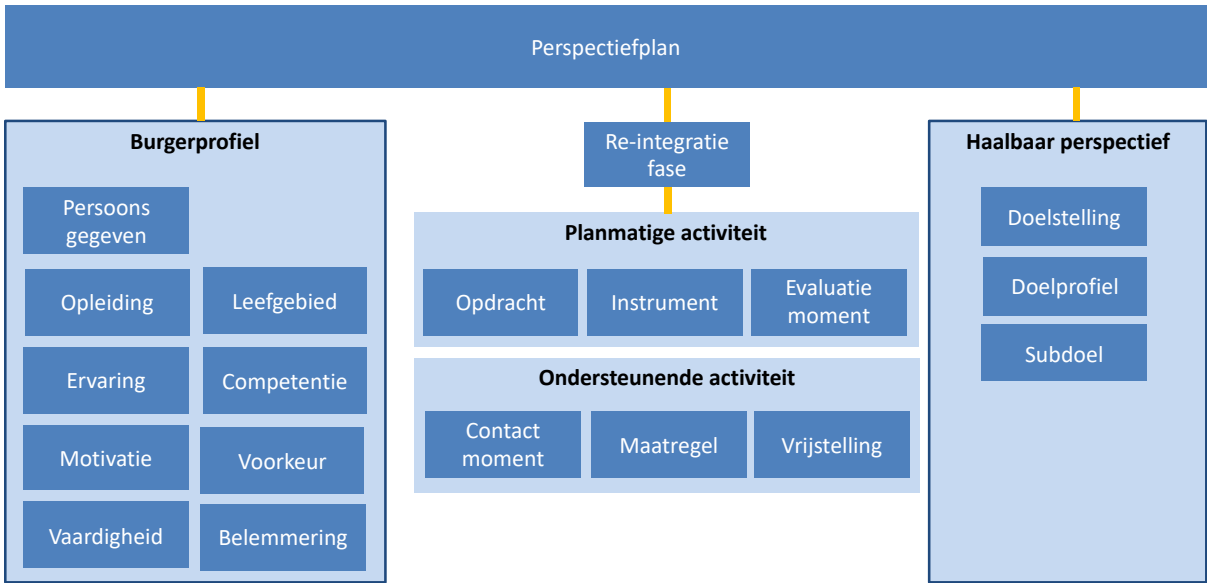
In de termenlijst Werk en Participatie zijn de begrippen gedefinieerd die in de functionele en niet-functionele documentatie zijn gebruikt. Bij het beoordelen van de eisen dienen deze termen integraal meegenomen te worden.

1.3.4 Conceptueel Informatiemodel

Het conceptueel Informatiemodel beschrijft de informatieobjecten die KWP minimaal moet kunnen vastleggen. Met conceptueel wordt bedoeld dat de essentie van de informatie vastgelegd moet kunnen worden. De wijze waarop dit gebeurt mag afhangen van de specifieke oplossing die wordt geboden.

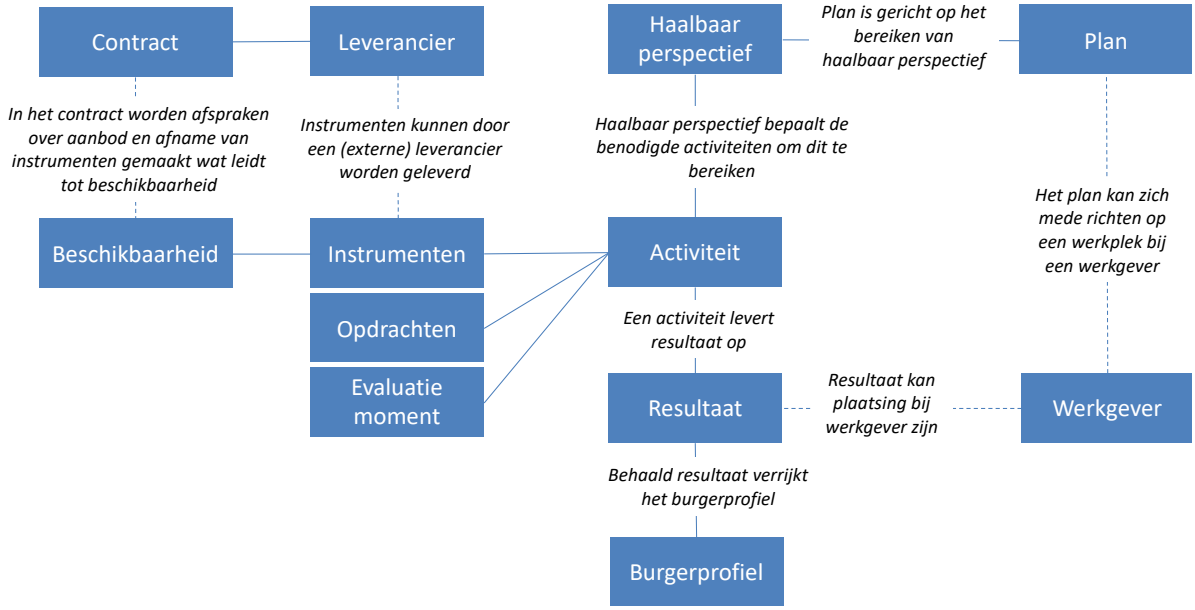
De informatie die minimaal benodigd is, is via twee invalshoeken gemodelleerd, namelijk vanuit het Perspectiefplan en vanuit Activiteiten. De wijze waarop de informatiemodellen worden ingevuld mag afhangen van de manier waarop dit in KWP van een specifieke *Leverancier* is opgelost. De informatieobjecten zijn gedefinieerd in de termenlijst.

In de algemene functionele eisen worden figuren D en E gebruikt om te stellen dat minimaal de afgebeelde informatieobjecten in KWP kunnen worden vastgelegd.



Figuur D: Informatieobjecten Perspectiefplan

Het Perspectiefplan bestaat uit een Burgerprofiel, een Haalbaar perspectief en Activiteiten. Het Burgerprofiel beschrijft de situatie van Burger. Het Haalbaar perspectief beschrijft de situatie waar Burger naar toe kan en wil ontwikkelen. Planmatige Activiteiten worden door Burger uitgevoerd om tot het Haalbaar perspectief te komen. Ondersteunende Activiteiten kunnen op niet-geplande momenten helpen om tot het Haalbaar perspectief te komen.



Figuur E: Samenhang informatieobjecten

1.4 Niet-functionele eisen

KWP moet voldoen aan de volgende niet-functionele eisen:

1. De niet-functionele eisen die in dit document zijn beschreven, zie paragraaf 2.1
   Deze zijn specifiek opgesteld door GDH.
2. De Gemeentelijke Inkoopvoorwaarden bij IT, zie bijlage '04. GIBIT 2020 inkoopvoorwaarden'.
3. De *Gemeentelijke ICT-kwaliteitsnormen* en de daarin voorgeschreven *Interoperabiliteitseisen*, normen en standaarden, zie bijlage '05. Gemeentelijke ICT-kwaliteitsnormen v2020 2.0'.
4. De 'Gemeentelijke Model Architectuur' (GEMMA), zie de eisen in paragraaf 2.1
5. De Baseline Informatiebeveiliging Overheid (BIO) voor het deel van de dienstenleverancier dat van toepassing is voor KWP, zie bijlage '16. Baseline Informatiebeveiliging Overheid versie 1.04'.
6. De VNG BBN2+ maatregelen, zie paragraaf 2.2

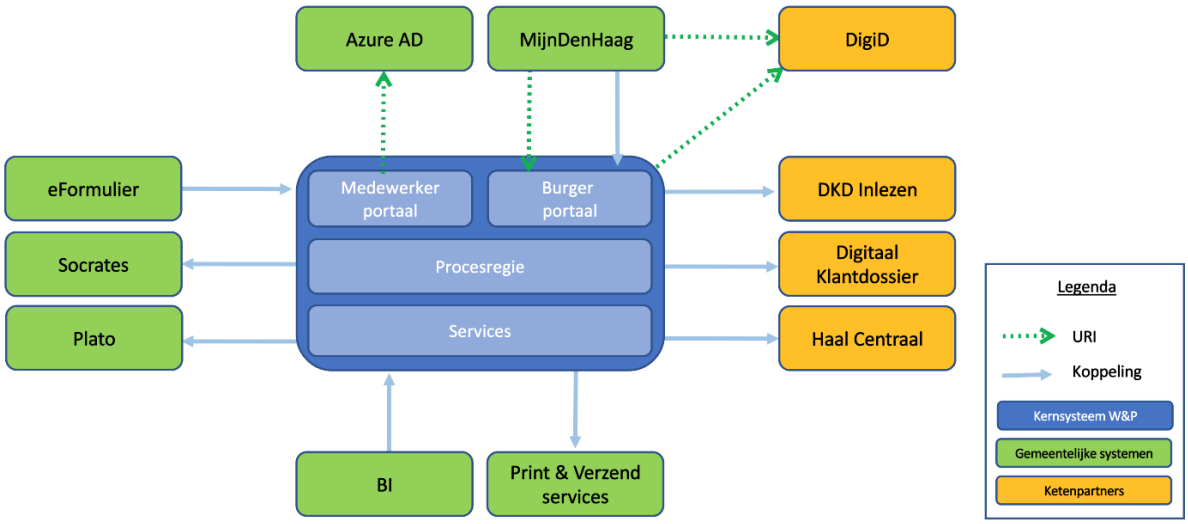
Zowel GEMMA als BIO zijn bindend volgens het principe 'pas toe of leg uit'. Essentiële eisen voor GDH zijn daarom expliciet als eis opgenomen in het PvE.

1.5 Applicatielandschap en koppelvlakken

Figuur E toont het deel van het applicatielandschap van GDH waarin KWP moet worden ingepast. Alle vermelde *Koppeling*en zijn vereist. Nadere details van de *Koppeling*en zijn beschreven in Bijlage '18. Applicatielandschap en koppelvlakken'.

Na gunning zullen de interfacespecificaties van de *Koppeling*en, ten behoeve van de realisatie en *Implementatie*, beschikbaar gesteld worden. Bijlage '18. Applicatielandschap en koppelvlakken' bevat informatie voor zover die nodig is voor het uitbrengen een aanbod en Inschrijving.

Figuur F toont de vier KWP-componenten in lijn met het Common Ground 5-lagen model. Het Common Ground model is richtinggevend voor KWP.



Figuur F: Applicatielandschap GDH voor KWP

2. Eisen Kernsysteem Werk en Participatie

2.1 Functionele en Niet-functionele eisen GDH

Voor het gemak en overzicht zijn de eisen gegroepeerd per paragraaf. De indeling is arbitrair want soms zijn eisen aan meer dan één paragraaf toe te wijzen. Er is voor gekozen dat niet te doen maar elke eis enkelvoudig – uniek - in de tabel op te nemen.

Algemeen:

- Waar in de eisen sprake is van *Koppeling* of *Koppeling*en heeft dit betrekking op de *Koppeling*en die zijn beschreven in de Bijlage '18 Applicatielandschap en koppelvlakken', zie eventueel ook paragraaf 1.5
- Waar in de eisen sprake is van *Conversie* heeft dit betrekking op de datamigratie en de initiële vulling, die beschreven is in Bijlage '19 Datamigratie en Initiële vulling'

Par.	Nr.	Eis
1		**Aanbesteding**
1	1	Inschrijver is in staat en verplicht tot Implementatie en configuratie van KWP: - conform minimaal het Programma van Eisen inclusief *Conversie* en *Koppeling*en; - met een kwaliteit die minimaal in overeenstemming is met het aangebodene ten behoeve van Subgunningscriterium 4; - met een scope die minimaal is zoals omschreven in uw Inschrijving ten behoeve van Subgunningscriterium 3. Dit zodat KWP gereed is voor gebruik en voldoet aan de geschetste verwachting op uiterlijk 09 augustus 2022.
1	2	Inschrijver verklaart dat alle bij Inschrijving overlegde gegevens juist, volledig en naar waarheid zijn ingevuld en gestand kunnen worden gedaan gedurende de gehele looptijd van de *Overeenkomst*, inclusief eventuele verlengingen van de *Overeenkomst*. GDH behoudt zich het recht voor op ontbinding van de *Overeenkomst* en/of een schadevergoeding in geval van onjuiste en/of onvolledige informatie en/of het niet kunnen nakomen hetgeen bij Inschrijving aangeboden is.
1	3	Alle communicatie (in woord en geschrift) tussen Inschrijver en GDH vindt plaats in de Nederlandse taal.
1	4	Binnen twee maanden na gunning stellen Inschrijver en GDH samen een *Implementatieplan* op. Hierin wordt opgenomen hoe de applicatie wordt geïmplementeerd en hoe *Conversie* vanuit het huidige systeem naar het nieuwe plaatsvindt.
1	5	Inschrijver dient vooraf toestemming te vragen aan GDH als Inschrijver tijdens de uitvoering van de *Overeenkomst* gebruik wil maken van onderaannemers. GDH kan aan deze toestemming voorwaarden verbinden.

Par.	Nr.	Eis
2		**Algemene Functionele eisen**
		Algemeen functioneel
2	1	KWP moet voldoen aan de functionele beschrijving zoals uitgewerkt in de, als bijlage opgenomen, hieronder vermelde use cases: UC01 Bepalen Dienstverlening UC02 Regisseren Ontwikkeling UC03 Nazorg en Begeleiding na plaatsing UC04 Beëindigen Dienstverlening UC05 Uitvoeren Activiteit UC06 Vaststellen Ontheffing UC07 Bepalen Maatregel
		Perspectiefplan
2	2	KWP biedt de mogelijkheid om Activiteiten verplicht te maken binnen een Perspectiefplan en hierin eventueel een vaste volgorde in af te dwingen en/ of gelijktijdig in te zetten.
2	3	Het automatisch aanmaken van Activiteiten en Taken is configureerbaar.
		Burgerportaal
2	4	Alle interactie met Burger, zoals beschreven in de use cases, gebeurt via een Burgerportaal. Hierin moet Burger tenminste toegang hebben tot zijn profielgegevens en een overzicht van zijn zaken, incl. status en bijbehorende Documenten.
2	5	Het moet mogelijk zijn gegevens die voor intern gebruik zijn bedoeld, af te schermen voor Burger.
2	6	Het Burgerportaal van de oplossing hanteert zowel dezelfde 'look-and-feel' als hetzelfde adres als MijnDenHaag.nl. Zie hiervoor https://www.denhaag.nl/nl/bestuur-en-organisatie/beleid-en-regelgeving/huisstijl/de-huisstijl-van-de-gemeente-den-haag-downloads.htm
2	7	Bij het ontwerp van het Burgerportaal is het 'mobile first' beleid gehanteerd.
2	8	KWP biedt de mogelijkheid om Professional namens Burger te laten handelen, op een zodanige manier dat in de Zaak wordt vastgelegd dat deze handelingen zijn gedaan op aangeven van Burger en dat Burger hiervan in kennis wordt gesteld (Verlengde arm).
2	9	Het moet mogelijk zijn om statistische gegevens van het gebruik van KWP door Burger te raadplegen. Voorbeelden hiervan zijn: • het % aantal velden dat wordt ingevuld door Burger; • het % dat het profiel/Perspectiefplan gesloten wordt, vrijwel meteen nadat het geopend is;

Par.	Nr.	Eis
		• het % Burgers dat daadwerkelijk de cv en overige Documenten aan het plan toevoegt.
2	10	Het taalniveau voor het Burgerportaal is B1.
		Configuratie
2	11	Alle stamgegevens, zoals vaardigheden, Competenties en selectielijsten (zoals 'reden beëindiging'), moeten configureerbaar zijn.
2	12	De catalogi voor Instrumenten, Opdrachten en Doelprofielen en de informatie-objecten die daarmee samenhangen, zoals beschreven in het Conceptueel Informatiemodel, moeten onderhoudbaar zijn. Het onderhouden moet als taak toegekend kunnen worden aan Gebruikersrollen (autorisatiematrix). Met onderhouden wordt bedoeld het aanmaken van een nieuwe versie van een object, wijzigen van bestaande objecten, het zetten van een einddatum op de geldigheid van een object.
2	13	Professional kan zowel de rol van Regisseur als Uitvoerder hebben. Dit moet in de autorisatiematrix als Gebruikersrol gedefinieerd kunnen worden.
2	14	Regisseur kan zowel automatisch aangemaakte Activiteiten, als handmatig aangemaakte Activiteiten, achteraf wijzigen of verwijderen.
		Data
2	15	Voor zover Burgers en Professionals gelijktijdig toegang hebben tot dezelfde informatie (als de autorisaties dit toestaan) is er geen verschil: de actualiteit van informatie is voor iedereen gelijk.
2	16	De historie van gegevens en Documenten moet zowel voor Professional als voor Burger zichtbaar gemaakt kunnen worden.
2	17	De historie van gegevens en Documenten mag alleen worden gelezen, niet gemuteerd.
2	18	Gegevens en Documenten moeten verwijderd kunnen worden, bijvoorbeeld als sprake is van een fout of als deze niet horen bij een Zaak.
2	19	Van elk gegeven of Document dat gebruikt wordt ten behoeve van de Zaak moet herleidbaar zijn wat de bron is van dat gegeven of Document en op welk moment het verkregen is.
2	20	KWP logt handelingen en raadplegingen van alle Gebruikers binnen de context van een Zaak, zodat achteraf zichtbaar is wie welke actie op welk moment heeft uitgevoerd.
2	21	Het Perspectiefplan omvat minimaal de samenhang en elementen zoals is geschetst in het Conceptueel Informatiemodel.

Par.	Nr.	Eis
2	22	De inzet van Activiteiten en het Resultaat hiervan kent minimaal de samenhang en elementen zoals geschetst in het Conceptueel Informatiemodel.
2	23	Het is, in de tijd of gelijktijdig, mogelijk om meer dan één Perspectiefplan te hebben. Deze zijn altijd gebaseerd op hetzelfde Burgerprofiel.
2	24	De ontwikkelingen en wijzingen in het Burgerprofiel en Haalbaar perspectief zijn op een tijd-as zichtbaar voor Burger en Professional. KWP geeft inzicht in lopende en afgeronde Activiteiten.
2	25	KWP biedt de mogelijkheid om meerdere soorten Doelprofielen te hanteren zoals: kansrijk beroepsprofiel, Arbeidsmarktprofiel, Inburgeringsprofiel, maatschappelijk fit profiel.
2	26	KWP biedt de mogelijkheid om verwijzingen naar afspraken die zijn vastgelegd in Haags Afspraken Systeem (HAS) te kunnen vastleggen bij een Zaak.
2	27	Alle gegevens en Documenten worden altijd vastgelegd in context van een Zaak.
2	28	Het moet mogelijk zijn om bij de inzet van een Instrument het aantal uren Aanwezigheid, verzuim en no-show te registreren.
2	29	Na sluiten van de Zaak is het niet meer mogelijk de Zaak te bewerken.
2	30	Het moet mogelijk zijn wijzigingen die van toepassing zijn op Zaken van meerdere Burgers in één keer uit te voeren (bulk verwerking). Bijvoorbeeld een deelname aan een Activiteit.
		Eenmalig inwinnen, meervoudig gebruik
2	31	Gegevens worden éénmalig ingewonnen en meervoudig gebruikt.
2	32	Burger en Professional kunnen gegevens uit een authentieke bron alleen in de authentieke bron zelf wijzigen.
2	33	Als gegevens uit een authentieke bron volgens Burger niet kloppen dan kan dit in KWP genoteerd worden en kan het proces vervolgen.
2	34	Burger moet desgevraagd toestemming kunnen geven voor het delen van gegevens met interne en externe partijen, tenzij er vanuit doelbinding al toestemming is om die gegevens te delen.
		Interactie
2	35	Professional kan op een Activiteit feedback geven, zoals een compliment of een tip.
2	36	Burger kan een vraag aan Professional stellen en Professional kan deze beantwoorden.

Par.	Nr.	Eis
2	37	Burger kan een Document uploaden (bijv. certificaat) in de context van een Zaak.
2	38	Documenten of gegevens die via een andere weg dan het Burgerportaal binnengekomen zijn, moeten handmatig door Professional kunnen worden toegevoegd aan de Zaak.
2	39	Zowel Burger als Professional kunnen van de gegevens die zij invoeren eerst een concept opslaan, voordat het wordt gepubliceerd.
		Output
2	40	Documenten moeten gegenereerd kunnen worden.
2	41	De opbouw en format van Documenten moeten door GDH aangepast kunnen worden.
2	42	De standaard tekstblokken moeten door GDH aangepast kunnen worden.
2	43	De huisstijl van GDH moet op alle Documenten toegepast kunnen worden.
2	44	Een versie van het Perspectiefplan kan als Document worden gemaakt met een specifieke titel. Voorbeeld: 'Plan van Aanpak t.b.v. de Participatiewet'.
		Signalen
2	45	KWP kan een Signaal sturen naar Burger om deze te attenderen op nieuwe berichten in het Burgerportaal, via e-mail en/of SMS (al naar gelang de voorkeur van Burger).
2	46	KWP kan een Signaal sturen bij bepaalde wijzigingen van het Perspectiefplan aan geabonneerde Professionals en Burgers.
2	47	Het is configureerbaar in KWP welke wijzigingen in het Perspectiefplan leiden tot een Signaal.
2	48	KWP is in staat om een Signaal te geven, bijvoorbeeld als een Opdracht[1] en/of Instrument over tijd is of de deadline nadert.
		Werkverdeling
2	49	Iedere Zaak en Taak is gekoppeld aan Professional of een team welke verantwoordelijk is voor de opvolging ervan.
2	50	Professionals moeten ingedeeld kunnen worden in een team. KWP moet zo ingericht kunnen worden, dat nieuwe zaken automatisch worden toegewezen aan een team. Het team wordt de 'eigenaar' van de Zaak/Taak.
2	51	Taken moeten automatisch toegewezen (kunnen) worden aan het team of Professional die verantwoordelijk is voor de opvolging van de Zaak.

[1] Conform Bijlage '12. Termenlijst Werk en Participatie'

Par.	Nr.	Eis
2	52	KWP moet zo ingericht kunnen worden, dat bestaande zaken en Taken handmatig kunnen worden toegewezen aan een ander team of Professional.
		Zoeken
2	53	De dossiers van Burger moeten gevonden kunnen worden op basis het BSN of het administratienummer van Burger in GDH. Ook moet dit kunnen met (combinaties van) andere gegevens zoals naam, geboortedatum en adres.
3		**Functioneel beheer**
3	1	Het wijzigen van de bewaartermijn van Documenten/ informatie-objecten moet via de autorisatiematrix toegekend kunnen worden aan een specifieke Gebruikersrol zodat Gebruikers de standaard bewaartermijn kunnen aanpassen.
3	2	Er kan een duidelijk afgebakend onderdeel ingericht worden voor de beheerrol met hierin minimaal: Gebruikersbeheer, logging, Gebruikersstatistieken.
3	3	Het dient mogelijk te zijn om toegang tot functionaliteiten en gegevens te scheiden voor de diverse Gebruikers, rollen en SZW-organisatieonderdelen.
3	4	De Administrator rechten kunnen worden toegewezen aan een separate beheerrol voor functioneel beheer.
3	5	Er zijn noodstop mechanismen, zoals het in één keer kunnen uitloggen van alle actieve gebruikers, waarmee stapeling van fouten kan worden voorkomen
3	6	Inschrijver voorziet in digitale Nederlandstalige *Documentatie*, waaronder Gebruikershandleidingen.
3	7	Inschrijver zorgt ervoor dat de tijdzone ingesteld is op Central European Time (CET), GMT+1 Amsterdam.
3	8	GDH moet in staat zijn om aanpassingen aan de configuratie zelfstandig uit te voeren, waaronder minimaal autorisatiemodel, organisatiestructuur, Taken, procesflows en templates.
3	9	Er is een standaardprocedure voor escalatie bij Inschrijver.
3	10	KWP moet de mogelijkheid bieden om (test-) data te anonimiseren.
3	11	Export van Gebruikersgegevens moet mogelijk zijn ter controle van de autorisatie.
3	12	Zaaktypes kunnen worden gedefinieerd en geconfigureerd, specifiek voor GDH.
3	13	Een zaaktype kan worden gewijzigd ten behoeve van nieuwe zaken, zonder dat dit directe invloed heeft op afgesloten en lopende zaken.

Par.	Nr.	Eis
4		**Service Level Agreement**
4	1	Inschrijver levert de SLA bij Inschrijving waarin concrete *Service Levels* ter zake van het in artikel 8.3 GIBIT-2020 bedoelde *Onderhoud* worden vastgelegd en waarin maatregelen zijn opgenomen ter zake van het al dan niet halen van de afgesproken *Service Levels*. De SLA is onderdeel van de *Overeenkomst* en wordt jaarlijks geëvalueerd.
4	2	De SLA bevat onder andere afspraken over: -De te gebruiken tooling; -Het vastleggen en onderhoud van het SLA en de Dossier Afspraken en Procedures (DAP) (bijvoorbeeld 1x per jaar); -Servicemanagement-overleg (bijvoorbeeld 1x per maand of kwartaal); -De inhoud en frequentie van SLA-rapportages; -De te hanteren normen voor de performance; -Acties en verbetermaatregelen vanuit de performancerapportages; -Normen voor afhandelen van escalaties en klachten (Termijnstelling bijvoorbeeld binnen 2 dagen). - Definities en werkwijze van Incidentbeheer. De minimale KPI's/*Service Levels* zijn opgenomen in dit Programma van Eisen. Deze dienen als minimale eisen in uw SLA opgenomen te zijn.
4	3	Inschrijver doet na gunning een voorstel voor de DAP rondom de dienstverlening en Governance op uitvoerend niveau. GDH en Inschrijver maken de DAP daarna in samenspraak af.
4	4	De beheerorganisatie van GDH wordt proactief geïnformeerd bij verstoringen in de continuïteit van KWP. De wijze waarop zal worden beschreven in de DAP.

Par.	Nr.	Eis
4	5	Bij een incident wordt hieraan een prioriteit toegekend. Per prioriteit gelden voor Inschrijver de onderstaande reactie- en oplostijden, welke onderdeel zijn van de op te leveren SLA: Prio 1: Kritisch Eén of meerdere (kritische) bedrijfsprocessen van de eindgebruikersorganisatie kunnen niet worden uitgevoerd met een hoog potentieel risico voor de bedrijfscontinuïteit. Er is geen functieherstel/ workaround beschikbaar. - Binnen 4 uur oplostijd, *Reactietijd* binnen vijftien (15) minuten na melden van het incident. Prio 2: Hoog Eén of meerdere (kritische) bedrijfsprocessen van de eindgebruikersorganisatie kunnen niet worden uitgevoerd met een hoog potentieel risico voor de bedrijfscontinuïteit. Er is wel een functieherstel/ workaround beschikbaar. - Binnen 8 uur oplostijd, *Reactietijd* binnen half (1/2) uur na het melden van het Incident, Standaardverzoek of ticketupdate. Prio 3: Midden Individuele Gebruikersproblemen van de eindgebruikersorganisatie en beheerorganisatie met een laag potentieel risico voor de bedrijfscontinuïteit. Er is mogelijke functieherstel/ workaround beschikbaar. - Binnen twee (2) werkdagen oplostijd, *Reactietijd* binnen 4 uur. Prio 4: Laag Individuele Gebruikersproblemen van eindgebruikers of beheerders zonder potentieel risico voor de bedrijfscontinuïteit. Voor het oplossen van het probleem is een afspraak acceptabel en er is mogelijke functieherstel voorhand. - Binnen vijf (5) werkdagen oplostijd, *Reactietijd* binnen 8 uur. Oplostijd. Dit is de tijd vanaf het moment dat het incident aan Inschrijver gemeld is tot het moment dat functieherstel geboden is. Prioriteit. Bij verschil van inzicht over de prioritering heeft GDH het eindoordeel over de prioriteit.
4	6	Incidentbeheer vindt plaats conform de definities en werkwijze zoals beschreven in de SLA.
4	7	Wijzigingen in de keten (van componenten die gezamenlijk de *Koppeling* vormen) worden wederzijds vooraf expliciet gemeld, geaccepteerd en geaccordeerd door zowel Inschrijver als GDH.
4	8	KWP dient minimaal geschikt te zijn voor 1500 gelijktijdige Gebruikerssessies (1000 Professionals - binnen netwerk - plus 500 Burgers - buiten netwerk).
4	9	Het is altijd duidelijk te zien op elk scherm in welke omgeving (acceptatie- en productie-omgeving) de Gebruiker zich bevindt, door middel van bijvoorbeeld een kleurstelling of een andere visuele voorziening.
4	10	In de KWP ontwikkel-, test- en acceptatie-omgeving moeten de *Koppeling*en beschikbaar zijn voor testen. Als voor een *Koppeling* geen testversie beschikbaar is dan, dient Inschrijver een gesimuleerde versie beschikbaar te stellen.
4	11	De Recovery time Objective (RTO) bedraagt 8 uur.

Par.	Nr.	Eis
4	12	De Recovery point Objective (RPO) bedraagt 4 uur.
4	13	Logging (auditfile) van alle mutaties mag niet door Gebruikers uitgeschakeld of gemuteerd kunnen worden.
4	14	De logfile (auditfile) moet eenvoudig door functioneel beheer zijn terug te lezen en te exporteren.
4	15	Beheerfuncties met betrekking tot error logs, moeten beschikbaar zijn voor de beheerorganisatie GDH. Gegevens (error logs) moeten door de beheerorganisatie geëxporteerd kunnen worden.
4	16	Inzage in Logging moet te filteren zijn: velden moet kunnen toegevoegd of verwijderd worden zodat verschillende weergaves gemaakt kunnen worden met beperkte gegevens, zodat bijvoorbeeld persoonsgegevens, zoals geboortedatum en BSN, uitgefilterd kunnen worden.
4	17	De *Beschikbaarheid* van de oplossing kan door GDH gemonitord worden.
4	18	Inschrijver heeft een Nederlandstalige helpdesk. De helpdesk is het centrale punt voor het melden van incidenten, het stellen van vragen, indienen van wijzigingsvoorstellen en geeft informatie/ inzicht in de afhandeling daarvan. De helpdesk van Inschrijver levert zowel telefonische ondersteuning als ondersteuning via e-mail en/of een web portaal.
4	19	KPI: Inschrijver levert maandelijkse een rapportage op over het prestatieniveau van de geleverde diensten, doorlooptijden en *Beschikbaarheid*. De rapportage bevat minimaal de overzichten van: -het aantal aangemelde incidenten, vragen en wijzigingsvoorstellen inclusief de status en de details (zoals verwerkingstijden versus norm etc.) daarvan; -het aantal gelijktijdige Gebruikerssessies, gemiddelde en de pieken; -de *Beschikbaarheid* onderscheiden naar dag, week en maand; -de performance; -de gerealiseerde Recovery time en Recovery point (zo vaak als van toepassing); - de aantallen (bijv. Gebruikers) in relatie tot het prijsmodel; - de implementaties van voorgestelde wijzigingen, patches, *Update(s)* en releases; - alle opgetreden beveiligingsincidenten, threats en datalekken; - de betaalde en openstaande facturen.
4	20	Inschrijver biedt een inzagemogelijkheid op de lopende en afgehandelde incidenten/verstoringen die door, of ten behoeve van, GDH aangemeld zijn.
5		**Continuïteit dienstverlening**
5	1	Alle *Koppeling*en kunnen gemonitord worden. Dit moet gedaan kunnen worden door (bevoegde) beheerders zonder verdere handelingen vanuit Inschrijver.
5	2	Inschrijver richt haar ontwikkel- (O) en een testomgeving (T) technisch zo in dat die een goede afspiegeling zijn van KWP in de Productie-omgeving, zodat geborgd wordt dat bij het ontwikkelen en testen de specifieke GDH-eigenschappen adequaat zijn meegenomen in de uitrol van *Update(s)* en Releases.

Par.	Nr.	Eis
5	3	Releases worden in overleg met GDH uitgerold. Releasebeheer: · Er is een eenduidige procedure rond het uitleveren van nieuwe releases · Er is een overzicht aanwezig met releasebeschrijvingen · Functioneel Beheer en Gebruikers kunnen de release zowel in de acceptatie- als in de productie-omgeving testen en hebben hier voldoende tijd voor. · De release wordt pas in productie genomen als deze akkoord is bevonden door de GDH-beheerorganisatie. · GDH wordt proactief geïnformeerd over bugs in het huidige systeem. · Releases worden uitgebracht tussen 19:00 uur en 07:00 uur, of in het weekend.
5	4	Het dient mogelijk te zijn om per tenant data te herstellen, met voorziene herstelprocedures, zonder impact op andere tenant. In de *Programmatuur* zijn maatregelen genomen om bij conflicten of calamiteiten de integriteit van databases en minimaal dataverlies te garanderen (recordlocking, roll-backfunctie e.d.).
5	5	Bij een multi-tenant omgeving heeft GDH geen last van het opschalen van andere tenants.
5	6	Geleidelijk (autonoom) opschalen van de omgeving moet mogelijk zijn.
5	7	Het maken van backups wordt uitgevoerd gelijk aan de criteria die gelden voor *Onderhoud* zoals gedefinieerd in *GIBIT 2020* artikel 8.
6		**Documentatie**
6	1	Inschrijver geeft de specificaties voor dataportabiliteit. Deze specificaties voor dataportabiliteit bevatten voor de export én import van data tenminste: a. de beschrijving van betekenis van de data van entiteit, attributen en waardenbereik; b. de beschrijving van betekenis en relaties (kardinaliteit) tussen gegevens; c. het formaat waarin data kan worden geëxporteerd/geïmporteerd; d. welke gegevens en metadata wel en niet worden meegenomen en het formaat waarin dat plaatsvindt; e. de beschrijving van de import en exportfunctionaliteit die het softwareproduct ondersteunt; f. de data die niet in de import en export meegenomen wordt omdat deze geen eigendom is van Opdrachtgever; g. opgave van de technische formaten die voor dataportabiliteit gebruikt worden.
7		**KWP-opleiding**
7	1	Inschrijver dient een onafhankelijke opleidingsomgeving (naast de acceptatie- en de productie-omgeving) beschikbaar te kunnen stellen, die representatief is voor de productie-omgeving (look & feel en functionaliteit) van het Burgerportaal zowel als van het medewerkersportaal.
7	2	Het opleidingsplan is onderdeel van het *Implementatieplan*.

Par.	Nr.	Eis
7	3	Inschrijver dient E-learning modules aan te leveren voor elk van de volgende doelgroepen: de functioneel beheerders, de Gebruikers, de Key-users en de callcenter medewerkers. Na het volgen van de opleiding dienen: o de functioneel beheerders in staat te zijn om - de applicatie functioneel in te richten (configuratie); - beheer van Gebruikers, rollen en autorisaties uit te voeren; - de logging te raadplegen en te kunnen interpreteren; - de acceptatietest uit te voeren en dienen o de Gebruikers, de Key-users en de callcenters medewerkers in staat te zijn om - de acceptatietest uit te voeren; - inhoudelijke systeemkennis te kunnen leveren aan trainingen/online; - leeractiviteiten en coaching on the job te kunnen bieden aan de Gebruikers; - de ervaring van de klant in het Burgerportaal goed te kunnen inschatten en in het gebruik te kunnen ondersteunen.
7	4	De door Inschrijver beschikbaar gestelde E-Learning modules zijn actueel en sluiten volledig aan bij de functionaliteit van de beschikbare releases van de ICT-oplossing.
7	5	Voor de functioneel beheerders dienen praktijkoefeningen en casussen beschikbaar gesteld worden om de benodigde praktijkervaring op te doen.
7	6	Tijdens de *Implementatie* stelt Inschrijver ervaren consultants ter beschikking met grondige kennis ten behoeve van o.a. 'coaching on the job' voor functioneel beheerders, Key-users en trainers. Van hen wordt een analyserend, meedenkend, flexibel, dienstverlenend en probleemoplossend vermogen verwacht.
7	7	Inschrijver dient ondersteuning te leveren bij het maken van up to date materiaal dat GDH wil maken voor het eigen opleidingsmateriaal, dit ter aanvulling op de door Inschrijver te leveren E-Learning modules. Denk hierbij aan digitaal materiaal zoals filmpjes, handleidingen, etc.
8		**Stuurinformatie en rapportage**
8	1	Het moet voor zowel GDH-medewerkers als -managers, etc. mogelijk zijn om operationele stuurinformatie te raadplegen, zowel per Professional als voor een groep (bijv. team). Het betreft operationele stuurinformatie zoals: - Taken - Werkvoorraad/ caseload per medewerker - Signalering termijnen - Taakverdeling (rol werkverdeler) - Prestaties. Het moet mogelijk zijn de getoonde uitvoer te exporteren.
8	2	Een Gebruiker moet eenvoudige overzichten kunnen samenstellen, gebaseerd op de operationele stuurinformatie genoemd in de vorige eis (par 8 nr. 1) en de selectie definitie op kunnen slaan. Daarnaast moet het mogelijk zijn de getoonde uitvoer te exporteren, in bijvoorbeeld csv-formaat.

Par.	Nr.	Eis
8	3	Er is een rapportage beschikbaar die voldoet aan de richtlijnen die door het CBS zijn opgesteld. Deze statistiek bevat informatie over re-integratievoorzieningen die door gemeenten zijn ingezet. Gemeenten leveren de gegevens voor de SRG maandelijks aan het CBS. In de richtlijnen is beschreven welke gegevens geleverd dienen te worden en waar de levering aan moet voldoen. Zie: Richtlijnen en documentatie (SRG) op cbs.nl
8	4	Er is een rapportage beschikbaar die voldoet aan de richtlijnen die door het Inlichtingenbureau zijn opgesteld. De Belastingdienst Toeslagen is verantwoordelijk voor de betaling van kinderopvangtoeslag. Om het recht op kinderopvangtoeslag definitief vast te kunnen stellen, moet de Belastingdienst Toeslagen weten op welke momenten aanvragers van de kinderopvangtoeslag een re-integratietraject hebben gevolgd. Alle gemeenten leveren hun gegevens over doelgroepouders ieder kwartaal aan bij het Inlichtingenbureau. Zie: Handleiding doelgroepouders-kinderopvangtoeslag op inlichtingenbureau.nl
8	5	Er is een rapportage beschikbaar die voldoet aan de richtlijnen die door CBS zijn opgesteld. De bijstandsuitkeringenstatistiek (BUS) geeft informatie over aantallen bijstandsuitkeringen en aantallen personen met een bijstandsuitkering. De uitkeringen worden verstrekt in het kader van de Participatiewet, de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers (IOAW), de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ) en het Bijstandsbesluit zelfstandigen (BBZ). Zie: Richtlijnen en documentatie (SRG) op cbs.nl
8	6	Er is rapportage beschikbaar die voldoet aan de richtlijnen die door het Agentschap SZW opgesteld. Deze rapportage is voor verantwoording voor de subsidie ESF (Europees Sociaal Fonds). Bedrijven en (Overheids-) instellingen kunnen van deze subsidie gebruik maken. Het doel van Duurzame Inzetbaarheid (ESF 2014-2020) is om mensen langer en productief aan het werk te houden en in te zetten op leeftijdsbewust personeelsbeleid. Zie hiervoor 'Toolkit gemeenten' op uitvoeringvanbeleidszw.nl
9		**Architectuur en standaarden**
9	1	Inschrijver zorgt ervoor dat Burgers toegang kunnen krijgen tot KWP zonder zich opnieuw te hoeven aanmelden. Burgers zullen zich eerst aanmelden via het portal van GDH (MijnDenHaag) met Digid (en in de nabije toekomst ook via DigiD Machtigen, Idensys, mogelijk iDIN).
9	2	KWP maakt (verplicht) gebruik van de authenticatievoorziening van GDH, inclusief multi-factor-authenticatie (2FA) door middel van Single Sign On voor het authenticeren van de Gebruikers.
9	3	KWP maakt gebruik van Single Sign On (SSO) op basis van het OpenID Connect/OAuth2 of SAML2 protocol.
9	4	Voor versies van de gebruikte authenticatie protocollen geldt dat een gangbare versie wordt gebruikt. Hiervoor geldt de huidige hoogst beschikbare versie of de hoogste versie -1.
9	5	Toegang tot KWP en het verlenen van rechten aan GDH-medewerkers vindt altijd plaats d.m.v. AD groep lidmaatschap.

Par.	Nr.	Eis
9	6	KWP ondersteunt de mogelijkheid voor federatieve authenticatie, waarbij gekoppeld wordt naar Azure AD.
9	7	KWP ondersteunt de mogelijkheid om gegevens te importeren vanuit een CSV-bestand.
9	8	KWP voldoet te allen tijde aan de wettelijke eisen ten aanzien van digitale toegankelijkheid. Voor de huidige eisen zie, https://www.digitoegankelijk.nl/wetgeving/wat-verplicht
9	9	KWP moet benaderbaar te zijn via een “fully qualified domain name”. Er zal een denhaag.nl naam worden toegekend aan KWP. Voor de cliënt zal denhaag.nl te allen tijde zichtbaar zijn in de URL.
9	10	Gebruikers kunnen van KWP gebruik maken met alle gangbare en moderne browsers; in ieder geval worden ondersteund de recente versies en de -1 versies van Chrome, Edge, Safari en Firefox.
9	11	Op mobile devices (Android en IOS) moet KWP gebruikt kunnen worden met gangbare browsers, zoals Safari, Chrome en de Android-browser, en versies.
9	12	KWP slaat Documenten/ informatieobjecten alleen op in DMS/Plato.
9	13	KWP kan Documenten/ informatieobjecten naar behoefte ophalen uit DMS/Plato.
9	14	Alle *Koppeling*en van KWP met andere applicaties en systemen moeten plaatsvinden via versleutelde verbindingen.
9	15	API-*Koppeling*en van KWP met andere applicaties moeten tenminste geauthentiseerd worden met een client-certificaat. In het geval dat een Gebruiker bekend is, moet ook de identiteit worden overgedragen.
9	16	Als KWP *Koppeling*en heeft met landelijke voorzieningen (bijv. een basisregistratie) en/of SaaS-systemen die door GDH gebruikt worden, dan identificeren de SaaS-applicaties zich namens GDH.
9	17	KWP wordt aangeboden als SaaS-applicatie.
9	18	KWP is een webapplicatie.
9	19	KWP wordt gehost in een aparte tenant/omgeving. Dit wil zeggen dat er geen delen van de applicaties of databases worden gedeeld met andere klanten van de Inschrijver.
9	20	Self-signed certificaten zijn in geen enkele omgeving toegestaan.
9	21	KWP past database encryptie toe bij de opslag van persoonsgegevens.
9	22	Het benaderen van KWP dient via het https-protocol (de toepassingslaag volgens het TCP/IP model) te geschieden.

Par.	Nr.	Eis
9	23	Voor het functioneren van KWP op het cliënt device zijn geen verdere instellingen, dan wel installaties benodigd. Dit geldt zowel voor het cliënt device als ook in de browser.
9	24	KWP mag geen gebruik maken van plug-in componenten (zoals o.a. Microsoft Active X, Microsoft Silverlight, Microsoft Click-Once, Adobe Flash en Java plug-in).
9	25	TLS moet geconfigureerd zijn en blijven conform de adviezen, richtlijnen en verdere overwegingen van het NCSC ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS), versie 2.1 (https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1), waarbij er gebruik gemaakt dient te worden van "GOEDE" -instellingen, met uitzondering van daar waar er geen "GOEDE" -instelling beschikbaar is, dient een "VOLDOENDE" -instelling toegepast te worden. Op moment van schrijven zijn TLS 1.2 en 1.3 als goede instelling beschreven door het NCSC.
9	26	Het gebruik van display protocollen, denk hierbij aan b.v. RDP/ICA/PCOIP, voor het benaderen van KWP is niet toegestaan (ook niet ingepakt in het http en/of https-protocol).
9	27	Op de API-*Koppeling*en vindt de authenticatie van aanbieders en afnemers (van data) plaats met PKI-overheid-service certificaten.
9	28	Voor versies van gebruikte protocollen geldt dat een gangbare versie wordt gebruikt. Hiervoor geldt de huidige hoogst beschikbare versie of de hoogste versie -1.
9	29	Email die namens @denhaag.nl wordt verzonden moet verlopen via de smtp relay service van GDH.
9	30	Voor (veilige) overdracht van bestanden wordt gebruik gemaakt van SSH File Transfer Protocol of Secure File Transfer Protocol of SFTP via de SFTP-service van GDH in overeenstemming met bijlage ‘30. Tactisch beleid Encryptie’.
9	31	*Koppeling*en met andere applicaties (zowel binnen als buiten GDH) moeten verlopen via de API Gateway Service van GDH, in overeenstemming met de bijlagen ‘32. Aansluitvoorwaarden WS Gateway Externe Consumer’ en ‘33. Aansluitvoorwaarden WS Gateway Provider’. (NB. Beide bijlagen bevatten links naar aanvraagformulieren, voor intern GDH gebruik, deze hebben geen invloed op de strekking van de aansluitvoorwaarden.)
9	32	KWP moet gegevens kunnen uitwisselen (invoer/uitvoer) met andere systemen via een RESTful API *Koppeling*.
9	33	KWP moet in staat zijn om eigen gegevens aan te bieden aan andere systemen voor uitwisseling (invoer/uitvoer) via een RESTful API *Koppeling*; De API wordt aangeboden op basis van een URI (e.g. https://api.denhaag.nl); De API biedt standaard http-methoden (e.g. GET, POST, PUT, en DELETE) aan; en gebruikt het JSON media-type.k
9	34	RESTful API's die door KWP worden aangeboden ondersteunen ten minste de huidige 'productie' versie (n) en de eerstvolgende versie (n+1).
9	35	KWP moet gegevens kunnen uitwisselen (invoer/uitvoer) met andere systemen via een SOAP Webservice op basis van een WSDL-interface beschrijving.

Par.	Nr.	Eis
9	36	KWP moet gegevens kunnen uitwisselen (invoer/uitvoer) met andere systemen via de overheidskoppelvlakstandaard Digikoppeling; Hierbij moet ondersteuning worden geboden voor WUS en ebMS(2).
9	37	KWP voert zelf procesregie (procesorkestratie, werkverdeling, werkbak), volgens eigen procesdefinities c.q. procescatalogus.
9	38	KWP levert zelf een zaakregistratie, volgens een eigen zaaktypecatalogus. Dit is inclusief het genereren van zaaknummers.
9	39	KWP moet zaakgericht werken ondersteunen, conform de eisen van RGBZ, het Informatiemodel Zaken (zie https://www.gemmaonline.nl/index.php/Informatiemodel_Zaken_(RGBZ) en https://www.gemmaonline.nl/index.php/GEMMA_2_Katern_Zaakgericht_Werken#Wat_is_Zaakgericht_werken3F).
9	40	KWP moet zaakgericht werken ondersteunen, conform de eisen van ImZTC (https://www.gemmaonline.nl/index.php/Informatiemodel_Zaaktypen_(ImZTC).
9	41	Het te gebruiken netwerk (het internet of Digi-netwerk koppelnetwerken zoals GGI-Netwerk) voor de uitwisseling van gegevens wordt bepaald door het betrouwbaarheidsniveau van de dienst (API) die wordt afgenomen.
10		**Informatiebeveiliging en Privacy**
10	1	Inschrijver staat ervoor in dat met de *ICT-Prestatie* door GDH kan worden voldaan aan de normen voor informatiebeveiliging, zoals vermeld in de Gemeentelijke ICT-kwaliteitsnormen opgenomen (voor zover relevant voor de *ICT-Prestatie*) en de BIO.
10	2	Inschrijver voldoet met KWP aan het uitgangspunt dat de toegang van medewerkers tot persoonsgegevens wordt bepaald op basis van roll-based-access. Dat valt uiteen in de volgende verplichtingen: a. In overleg met GDH wordt een autorisatiematrix gemaakt. b. De autorisatiematrix is vastgesteld op basis van 'need to know' en 'need to access'.
10	3	Inschrijver stemt ermee in, dat na gunning een Data Protection Impact Assessment (DPIA) plaatsvindt. De specifieke vorm wordt nader afgestemd. De kosten hiervoor moeten inbegrepen zijn in de prijsopgave voor KWP. Eventuele aanpassingen die door Inschrijver ondernomen dienen te worden naar aanleiding van de DPIA, zijn voor rekening van Inschrijver.

Par.	Nr.	Eis
10	4	Zonder expliciete opdracht daartoe vanuit GDH wordt in KWP geen automatische besluitvorming ex art. 22 AVG toegepast. Er wordt zonder expliciete opdracht daartoe vanuit GDH ook geen gebruik gemaakt van profilering. Daarmee wordt bedoeld: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.
10	5	KWP biedt functionaliteiten om een kopie van persoonsgegevens van een inwoner te maken. Deze functionaliteiten dienen via de autorisatiematrix aan één of meer Gebruikersrollen te kunnen worden toegekend.
10	6	Datalekken worden zo snel mogelijk, dus zonder onredelijke vertraging, direct en in ieder geval binnen 24 uur bij GDH gemeld. Inschrijver treft maatregelen om de gevolgen van het datalek zo veel mogelijk te beperken.
10	7	KWP legt – in logging/ audittrail bestanden – alle gegevens vast van bewerkingen, handelingen en pogingen daartoe die relevant (kunnen) zijn voor het uitvoeren van audits en onderzoeken gericht op informatiebeveiliging en security. De vastgelegde gegevens dienen eenvoudig doorzoekbaar te zijn.
10	8	Inschrijver kan door middel van een ICV of TPM jaarlijks aantonen dat zij voldoet aan de Baseline Informatiebeveiliging Overheid (BIO), waarbij aantoonbaar voldaan wordt aan de BBN2+ maatregelen in paragraaf 2.2
10	9	Inschrijver voldoet aan de 'Code of Practice for Information Security controls' gebaseerd op NEN-EN-ISO/IEC 27002:2017 voor Cloud services, te weten de NEN-EN-ISO/IEC 27017:2015
10	10	Inschrijver zegt toe jaarlijks een ISAE3402 verklaring type 2 of een SOC2 verklaring te halen dan wel een qua informatiebeveiliging en zekerheid vergelijkbare verklaring. Ook zal de toepassing jaarlijks worden getoetst op de implementatie van BIO. Inschrijver dient daar jaarlijks zijn medewerking aan te verlenen door vragen te beantwoorden en daar waar nodig bewijs voor aan te leveren.
10	11	Alle accounts die door beheerders van Inschrijver gebruikt worden, zijn gekoppeld aan natuurlijke personen.
10	12	Inschrijver staat GDH toe audits ten aanzien van informatiebeveiliging bij Inschrijver uit te voeren of te laten uitvoeren.
10	13	Inschrijver legt dezelfde (beveiligings-) eisen op aan onderaannemers/subcontractors als gelden voor Inschrijver voor de uitvoering van het contract met GDH.
10	14	Kopieën van de gegevens van GDH worden vernietigd zowel in de productieomgeving als de back-up bij beëindiging van het contract tussen Inschrijver en GDH.
10	15	Inschrijver meldt informatiebeveiligingsincidenten direct aan de daartoe aangewezen functionaris van GDH.

Par.	Nr.	Eis
10	16	KWP maakt geen inbreuk op de *Beschikbaarheid*, integriteit en vertrouwelijkheid van andere op het netwerk aangesloten systemen.
10	17	KWP bevat controlemechanismen waarmee ten minste transactie- en verwerkingsfouten kunnen worden gedetecteerd. Dat valt uiteen in de volgende eisen: a. Het Burgerservicenummer (BSN) moet uniek, bij één persoon voorkomen binnen de applicatie. b. Het is mogelijk om de applicatie zo in te richten, dat tijdens het invoeren van mutaties automatisch controles worden uitgevoerd op onmogelijke of onwaarschijnlijke invoer. Bij de controles is instelbaar of deze controles als een fout (hard/stop) of als een waarschuwing (let op) weergeven worden.
10	18	Voor zover KWP gebruik maakt van encryptietechniek, wordt aan GDH de bijbehorende encryptiesleutel(s) meegeleverd.
10	19	GDH wordt onmiddellijk geïnformeerd bij dagvaardingen en onderzoeken van Inschrijver en/of andere klanten van Inschrijver door toezichthouders.
10	20	Bij dagvaardingen en onderzoeken door toezichthouders van Inschrijver en/of andere klanten van Inschrijver worden geen gegevens en/of data van GDH gedeeld.
10	21	De aanroep van een dienst (API) wordt vastgelegd in logbestanden ongeacht of de aanroep succesvol was of niet. Zie ook de BBN2+ maatregelen.
10	22	Voor de acceptatie-, de productie- en de opleidingsomgeving (indien hiervan de optie wordt benut) van KWP is, met uitzondering van gepland *Onderhoud*, de vereiste *Beschikbaarheid* minimaal 99,5% per dag, 7 dagen per week,
10	23	KWP beschikt over een niet-muteerbare audit-trail waarin automatisch registratie en opslag van de volgende gegevens plaats vindt: 1) alle handelingen (functionaliteiten) die door Gebruikers met betrekking tot metagegevens, processen, Documenten, dossiers of andere objecten worden verricht; 2) de Gebruiker, datum en tijd van de uitvoering van de handeling.
10	24	KWP wordt ingericht conform de relevante eisen t.a.v. logging vanuit de BIO en door GDH gestelde eisen conform bijlage '30. Tactisch beleid Logging'.
10	25	Inschrijver dient te beschikken over functionarissen die verantwoordelijk zijn voor informatieveiligheid.
10	26	Functionarissen van Inschrijver op het gebied van informatieveiligheid dienen aantoonbaar marktconform gekwalificeerd te zijn op het vakgebied (certificeringen, opleidingen, trainingen, erkende autoriteit op het vakgebied).
10	27	Inschrijver neemt aanvullende maatregelen ten aanzien van privacybescherming. Dat valt uiteen in de volgende eisen: a. Inschrijver heeft een schriftelijk privacybeleid dat is goedgekeurd door het management; b. Inschrijver heeft een datalekprotocol; c. Inschrijver heeft iemand binnen de organisatie benoemd die verantwoordelijk is voor privacy.

Par.	Nr.	Eis
10	28	KWP moet gehost worden binnen de Europese Economische Ruimte (EER). Alle data (inclusief de back-ups) moet binnen de EER blijven.
10	29	(Systeem)software wordt altijd volgens de laatste stand van zaken gepatched, conform https://www.informatiebeveiligingsdienst.nl/product/patch-management-voor-gemeenten. Inschrijver committeert zich aan het patch managementbeleid van de leveranciers van Operating Systems, DBMS'en en ondersteunende softwarefunctionaliteit aanwezig in de infrastructuur en volgt de adviezen op van patchmanagement eisen gesteld door het NCSC.
10	30	Inschrijver slaat gegevens van Burgers in aparte databases op, gescheiden van de gegevens van andere klanten.
10	31	Inschrijver past pseudonimisering of anonimisering toe. Alleen de KWP-productieomgeving bevat productiedata. Data in alle andere KWP-omgevingen is geanonimiseerd of gepseudonimiseerd. De enige uitzonderingen zijn (tijdelijke) testomgevingen die gebruikt worden voor controle van de *Conversie* van productiegegevens. Schaduwdraaien voor de controle van de *Conversie* en/ of de inrichting/ configuratie van de applicatie. Deze omgevingen worden direct na het voltooien van deze testen verwijderd.
10	32	Inschrijver en KWP voldoen aan de *Gemeentelijke ICT-kwaliteitsnormen* van de VNG.
10	33	Door Inschrijver gebruikte software en infrastructuur [incl. datacentra (incl. back-up)] zijn adequaat beveiligd volgens ISO/IEC 27001.
10	34	Inschrijver sluit met GDH een Verwerkersovereenkomst (zie bijlage ’08. Concept Verwerkersovereenkomst’).
11		**Archivering**
11	1	KWP moet Documenten kunnen converteren naar het (duurzame) bestandsformaat PDF/A wanneer de definitieve versie wordt opgeslagen.
11	2	Aan een Zaak moet metadata over de achtergronden van de waardering (bewaren of vernietigen) en/of hoogte van de bewaartermijn automatisch kunnen worden toegevoegd.
11	3	Het moet mogelijk zijn om een Zaak te voorzien van een speciaal kenmerk en van een afwijkende, langere, bewaartermijn. Dit is bijvoorbeeld nodig bij het aanvragen van subsidie ui:t het Europese Subsidie Fonds.
11	4	Inschrijver verwijdert geen gegevens uit het systeem zonder de voorafgaande goedkeuring van GDH.
11	5	KWP beschikt tenminste over de Haagse Minimale Metadataset (MMS). Deze door GDH vastgestelde metadataset is compatible met het TMLO van het Nationaal Archief. De minimale metadata worden niet alleen gebruikt in KWP zelf, maar worden ook meegegeven aan de Documenten/ informatieobjecten die in DMS/Plato worden opgeslagen. Zie voor de metadata-velden de bijlage ‘28. Informatiebeheer - Haagse MMS (minimale dataset)’ en voor de achterliggende stamtabellen bijlage ‘29. Informatiebeheer – Stamtabellen’.

Par.	Nr.	Eis
11	6	De bewaartermijnen van zaken/dossiers in KWP, plus onderliggende registraties en bijbehorende metadata, worden ingesteld aan de hand van het type werkproces, de waardering van het werkproces (bewaren of vernietigen) en het resultaattype van de Zaak en de einddatum van de behandeling van de Zaak. Zie ook bijlage '28. Informatiebeheer - Haagse MMS (minimale dataset)' en bijlage '29. Informatiebeheer – Stamtabellen'.
11	7	Het moet in KWP mogelijk zijn om een overzicht te maken van alle zaken/dossiers plus onderliggende registraties en bijbehorende metadata die voor vernietiging of overbrenging in aanmerking komen in een gegeven tijdvak (begin- en einddatum).
11	8	Zaken/dossiers plus onderliggende registraties en bijbehorende (meta-) data moeten in KWP onherstelbaar kunnen worden vernietigd op basis van de waardering (bewaren of vernietigen) en de ingestelde vernietigingstermijn. Documenten/informatieobjecten plus bijbehorende metadata worden niet vanuit KWP maar vanuit DMS/Plato vernietigd.
11	9	Van de vernietiging in KWP moet een rapportage kunnen worden opgeleverd waarin minimaal wordt aangegeven om welke zaken/dossiers het gaat en dat de vernietiging volledig is uitgevoerd.
11	10	KWP biedt een zoekfunctie op ingevoerde en automatisch gegenereerde metadata en combinaties hiervan.
12		**Koppelvlakken BI-systeem**
12	1	KWP moet in staat zijn de data, incrementeel of eenmalig, beschikbaar te stellen aan een dataplatform ten behoeve van het BI-systeem.
12	2	In een incrementele levering van data moeten alle relevante wijzigingen in het bronsysteem sinds de laatste levering geleverd worden. Een verwijdering van data uit het bronsysteem is een relevante wijziging.
12	3	Bij de realisatie van de incrementele levering van data moet gegarandeerd worden dat alle wijzigingen ook daadwerkelijk geleverd worden, ook in geval van onvoorziene omstandigheden.
12	4	Het bron- en doelsysteem moeten beide beschikbaar zijn op het moment van uitwisselen van de levering; dit moment wordt zo kort mogelijk gehouden. NB. Door het beschikbaar stellen van de levering van de data door het bronsysteem los te koppelen van de verwerking van deze levering, hoeven geen afspraken gemaakt te worden over het tijdstip van het klaarmaken en het opnemen van de levering. Beide kunnen gepland worden op het meest geschikte moment vanuit het eigen perspectief bekeken.
12	5	Wijzigingen van de datastructuur binnen het bron-systeem mogen geen invloed hebben op het formaat (de lay-out) van de data levering. Het afgesproken formaat blijft van kracht totdat de gewenste inhoud van de levering verandert.
12	6	Voor het interpreteren van de Datalevering hoeft geen applicatie logica toegepast te worden.

Par.	Nr.	Eis
12	7	Een Datalevering is voorzien van metadata, waarmee de volledigheid van de levering getoetst kan worden en de interpretatie van de levering eenduidig is. De volgende groepen van metadata zijn minimaal benodigd: Minimale BI-metadataset: Betekenis: •Naam •Definitie •Relaties tussen de gegevenselementen Vertrouwelijkheid: •Vertrouwelijkheid niveau Privacy: •Aanduiding of het een persoonsgegeven betreft Technische eigenschappen: •Datatype •Lengte •Indicatie verplicht Verwerking: •Datum van levering •Contactpersoon Toegelicht: Betekenis: een ondubbelzinnige definitie is nodig om de gegevens correct te gebruiken. Vertrouwelijkheid: het is mogelijk de gegevens te verwerken voor een gedefinieerde groep van gerechtigden. Privacy: om te kunnen voldoen aan de AVG-eisen dient te worden aangegeven of het om persoonsgegevens gaat. Technische eigenschappen: voor correcte en efficiënte transformatie en presentatie worden technische eigenschappen van data vermeld. Verwerking: informatie betreffende de data levering is nodig om de levering te identificeren.
13		**Implementatie**
13	1	Tijdens de Implementatie wordt de *Conversie* uitgevoerd, in lijn met de beschrijving in bijlage '19. Datamigratie en Initiële vulling'. Het inlezen van de data in KWP wordt geautomatiseerd uitgevoerd.
13	2	Alle implementatiewerkzaamheden die storend (kunnen) zijn voor de bedrijfsvoering van GDH dienen te worden uitgevoerd tussen 22.00 uur en 07.00 uur. Uitzondering hierop is alleen mogelijk met instemming van GDH.
13	3	Gedurende de *Implementatie* beschikt Inschrijver over voldoende resources om inrichting, migratie en nazorg volgens het *Implementatieplan* te begeleiden.
13	4	Inschrijver dient zorg te dragen voor adequate Gebruikersondersteuning gedurende ten minste de eerste vier weken na in productie name van de applicatie.
14		**Facturatie**

Par.	Nr.	Eis
14	1	Het facturatieschema van inschrijfsom van de *Implementatie* is als volgt: • 25% bij aanvang van de *Implementatie;* • 25% bij een gezamenlijk (in het *Implementatieplan*) te bepalen mijlpaal; • 25% bij livegang; • 25% na livegang, op voorwaarde dat alle restpunten/kleine gebreken die geen belemmering waren om live te gaan, zijn opgelost.
14	2	De dienstverlening voor KWP kan gefactureerd worden vanaf het moment van livegang.
14	3	Inschrijver factureert de KWP-dienstverlening per kwartaal achteraf. Inschrijver vermeldt op de factuur de volgende elementen: • inkooporder nummer; • uw btw-identificatienummer; • factuurnummer; • factuurdatum; • naam en adres; • KvK nummer; • IBAN-bankrekeningnummer; • naam contactpersoon van GDH; • postadres van GDH. Ten aanzien van de uitgevoerde dienstverlening dient in ieder geval het volgende te worden opgenomen: • het kwartaal van de geleverde dienst; • het toegepaste btw-tarief; • de totale vergoeding.
14	4	De facturen voor KWP worden digitaal als pdf-bijlage verstuurd naar e-mailadres: facturen.szw@denhaag.nl ter attentie van de in de SLA vermelde contactpersoon.
14	5	Facturatie van aanvullende consultancy vindt plaats op basis van het dagtarief zoals door Inschrijver opgegeven op het prijzenblad zoals ingediend bij Inschrijving op de Aanbesteding.
14	6	Inschrijver is akkoord met een betalingstermijn van 30 dagen na ontvangst factuur.

2.2 BIO maatregelen BBN2+

De Baseline voor Informatiebeveiliging Overheid (BIO) beschrijft de aanpak en kaders ten aanzien van Informatiebeveiliging voor Overheidsorganen. Deze gelden in principe ook voor externe dienstverleners.

De set van maatregelen die vanuit de VNG beschikbaar gesteld worden is van toepassing op KWP en Inschrijver.

Uiteraard gelden alleen de maatregelen aan de externe dienstverlener (Inschrijver) en de aangeboden oplossing (KWP).

Onderstaande eisen zijn conform https://www.informatiebeveiligingsdienst.nl/product/maatregelenset-bbn2/ voor zover van toepassing op de dienstenleverancier (kolom H).

Voor dienstenleverancier dient te worden gelezen Inschrijver.

Voor ICT-oplossing dient te worden gelezen KWP.

Nr.	BBN2+ Maatregel
6.1.1.9	De Chief Information Security Officer (CISO) draagt zorg voor het geven van aanwijzingen aan lijnmanagement, systeemontwikkelaars en dienstenleveranciers en/of de ICT-afdeling bij het onderzoeken van incidenten of vermoedens van incidenten.
6.1.1.10	De dienstenleverancier en/of de ICT-afdeling draagt zorg voor het opstellen en onderhouden van beveiligingsdocumentatie die door de CISO verlangd en gecontroleerd wordt ten behoeve van de toestemmingsverlening.
6.1.1.15	De lijnmanager, dienstverlener en de CISO draagt zorg voor rapporteren over gevonden zwakten aan de Gemeentesecretaris (GS) of degene die in de SLA vermeld staat.
6.1.1.16	Er is functiescheiding tussen systeembeheerderstaken en de beveiligingsrollen.
6.1.1.17	De lijnmanager zal, in samenspraak met de CISO-systeemontwikkelaar en de dienstenleverancier en/of de ICT-afdeling, de eisen aan de beoordeling van de beveiliging vaststellen.
6.1.1.18	De lijnmanager, de dienstenleverancier en/of de ICT-afdeling en/of de systeemontwikkelaar houden de CISO tijdig op de hoogte van ontwikkelingen, zoals voorgenomen wijzigingen van het systeem, van de wijze waarop het systeem wordt ingezet en van wijzigingen in de belangen waarop het systeem betrekking heeft.
7.1.1.2	Medewerkers met bijzondere bevoegdheden (bijvoorbeeld auditors en systeembeheerders) in een infrastructuur die bedoeld is voor de verwerking van BBN2+ informatie, beschikken over een Verklaring omtrent gedrag (VOG).

Nr.	BBN2+ Maatregel
8.3.3.3	Fysieke verzending van BBN2+ informatie dient te geschieden met goedgekeurde middelen, waardoor de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is.
9.2.1.3	Er zijn alleen accounts toegestaan die te herleiden zijn naar natuurlijke personen. Systeemprocessen draaien onder een eigen Gebruikersnaam (een functioneel account), voor zover deze processen handelingen verrichten voor andere systemen of Gebruikers.
9.2.3.2	Het raadplegen van logbestanden is voorbehouden aan geautoriseerde Gebruikers. Hierbij is de toegang beperkt tot leesrechten.
9.2.3.3	Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.
9.2.3.4	De instellingen van logmechanismen worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden. Indien de instellingenaangepast moeten worden zal daarbij altijd het vier ogen principe toegepast worden.
9.2.3.5	Standaard Gebruikers hebben een Gebruikersaccounts (Tier 2), zonder beheerdersrechten
9.3.1.3	Uitsluitend door de CISO geadviseerde wachtwoordkluizen zijn toegestaan.
9.3.1.4	Voorafgaand aan het aanmelden wordt aan de Gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden en de verantwoordelijkheid die de Gebruiker als gevolg daarvan heeft.
9.4.1.3	Er wordt tijdens het inloggen geen extra informatie vrijgegeven die misbruikt kan worden door derden (bijv. geen aantal telbare sterretjes, leidend tot de lengte van het wachtwoord). Indien een fout tijdens het inloggen optreedt, zal het systeem niet aangeven welke gegevens juist of onjuist zijn (bijv. geen bevestiging Gebruikersnaam, geen wachtwoordhints).
9.4.1.4	Het aantal sessies dat één Gebruiker gelijktijdig kan hebben, is beperkt en wordt gemonitord op misbruik. Maak bij het aanmelden een nieuwe sessie aan en verbreek een eventueel al bestaande sessie van die Gebruiker. Maak de oude sessie-identifier ongeldig.
9.4.1.5	Stel vast welke functies nodig zijn en schakel alle andere functies uit (minste functionaliteit). Deactiveer of verwijder (de-installatie) alle functies, protocollen, services en accounts op het ICT-component als die niet noodzakelijk zijn. Toets periodiek (eventueel automatisch) of de in productie zijnde ICT-componenten niet meer dan de vastgestelde noodzakelijke functies bieden (statusopname) en de geconstateerde afwijkingen worden hersteld.

Nr.	BBN2+ Maatregel
9.4.3.6	De dienstenleverancier en/of de ICT-afdeling staat uitsluitend het gebruik van tijdelijke wachtwoorden toe voor de eerste keer inloggen en het resetten van een wachtwoord. Het ICT-systeem vereist dat het tijdelijke wachtwoord bij het eerste gebruik worden gewijzigd in een permanent wachtwoord wordt gewijzigd. Een tijdelijk wachtwoord heeft een zeer korte geldigheidsduur. Een tijdelijk wachtwoord is voor eenmalig gebruik. Initiële wachtwoorden worden alleen verstrekt als de identiteit van de Gebruiker is vastgesteld.
9.4.3.7	De dienstenleverancier en/of de ICT-afdeling past hardening toe ter beveiliging van credential stores en -mechanismen.
9.4.3.8	Replay aanval op authenticatie en binnen een sessie wordt voorkomen.
9.4.3.9	Inactieve accounts worden na 90 dagen geblokkeerd.
9.4.4.3	Basic Input Output System (BIOS)/Unified Extensible Firmware Interface (UEFI) instellingen zijn niet toegankelijk voor eindGebruikers. Uitsluitend de noodzakelijke BIOS/UEFI features zijn geactiveerd. Het BIOS/UEFI systeem wordt gepatcht in overeenstemming met het patchbeleid. UEFI Secure Boot is geactiveerd, waar mogelijk.
10.1.1.3	Voor PKI-gebaseerde authenticatie zorgt de dienstenleverancier en/of de ICT-afdeling ervoor dat het ICT-systeem certificaten valideert door een certificaatpad naar een trust anchor op te zetten en te verifiëren, en dat het daarbij ook informatie over de certificaatstatus controleert.
10.1.1.4	Een token (bijvoorbeeld smartcard) wordt geblokkeerd indien de pincode of het wachtwoord vijf keer verkeerd wordt ingevoerd.
10.1.1.5	De dienstenleverancier en/of de ICT-afdeling voert voor natuurlijke personen het eerste PKI aanvraag- en uitgifteproces persoonlijk (d.w.z.: face to face) uit.
11.1.2.2	Fysieke beveiligingsmaatregelen moeten zo zijn ingericht dat ze: (a) heimelijke of geforceerde toegang van een indringer buitenhouden; (b) acties van wraakzuchtige en onbetrouwbare medewerkers ontmoedigen, belemmeren en detecteren; (c) het mogelijk maken dat ruimtes zodanig beschermd worden dat uitsluitend tot die gegevens geautoriseerde medewerkers toegang kunnen krijgen. (d) beveiligingsinbreuken zo snel mogelijk detecteren en erop reageren.
11.1.2.3	Fysieke toegang tot serverruimtes of datacenters waar BBN2+ informatie wordt opgeslagen of verwerkt, wordt gecontroleerd.
11.1.2.4	Toegang tot ruimtes/locaties/zones waarbinnen transport van onversleutelde BBN2+ informatie plaatsvindt, is beperkt en gecontroleerd.
11.1.2.5	Toegang tot ruimtes/locaties/zones waarbinnen zich voor het systeem noodzakelijke faciliteiten bevinden, is beperkt, geregistreerd en gecontroleerd.
11.1.2.6	Toegang tot ruimtes/locaties/zones waarbinnen zich centrale BBN2+ apparatuur bevindt, is uitsluitend toegankelijk voor medewerkers die beschikken over minimaal een VOG en op een autorisatielijst staan.

Nr.	BBN2+ Maatregel
11.1.2.7	Het moet voorkomen worden dat bezoekers kennis kunnen nemen van BBN2+ informatie.
11.2.1.4	ICT-middelen (ook kopieerapparaten, faxapparatuur) die toegang kunnen geven tot BBN2+ informatie worden op ten minste BBN2+ niveau beschermd.
11.2.1.6	Uitsluitend door de CISO goedgekeurde Keyboard-Video-Mouse- (KVM-) switches en andere randapparatuur die gedeeld worden onder verschillende omgevingen zijn toegestaan.
11.2.1.7	Apparatuur die ooit is gebruikt voor de opslag of verwerking van BBN2+ informatie (eigen apparatuur, apparatuur van dienstenleveranciers maar ook laptops van consultant of gehuurde ICT-middelen (waaronder kopieerapparaten en faxapparatuur) blijven binnen de organisatie. Uitsluitend als BBN2+ informatie is verwijderd met een door de CISO goedgekeurde methode is hergebruik van apparatuur buiten de organisatie toegestaan
11.2.1.8	Externe medewerkers en ingehuurd *Personeel* werken met BBN2+ informatie uitsluitend op door de gemeente verstrekte apparatuur. Indien dit niet mogelijk is dan kan er na overleg met de CISO van worden afgeweken.
11.2.9.6	Na een bepaalde periode van inactiviteit (zoals met de CISO overeengekomen) wordt een sessie vergrendeld waarbij alle informatie op het beeldscherm onleesbaar en ontoegankelijk wordt.
12.1.2.2	De dienstenleverancier en/of ICT-afdeling past softwarebescherming toe overeenkomstig vastgestelde en gedocumenteerde procedures van de organisatie.
12.1.2.3	De dienstenleverancier en/of ICT-afdeling past (veilig) *Onderhoud* toe overeenkomstig vastgestelde en gedocumenteerde procedures van de organisatie.
12.2.1.6	De authenticiteit en integriteit van software, firmware, patches en security-*Update(s)* is, bij installatie, technisch geborgd.
12.3.1.7	Back-upstrategieën zijn vastgesteld op basis van de soort gegevens ((log)bestanden, databases, software, standaardconfiguraties, VM-templates, et cetera), de maximaal toegestane periode waarover gegevens verloren mogen raken, en de maximaal toelaatbare back-up- en hersteltijd.
12.3.1.8	Het back-up- en herstelproces wordt op basis van vastgestelde en gedocumenteerde procedures regelmatig getest op doelmatigheid. De frequentie wordt door de lijnmanager in overleg met de CISO, op basis van het risicoprofiel, bepaald en is in lijn met de back-upstrategie.
12.3.1.9	Back-ups worden zodanig opgeslagen dat bij een incident niet zowel het ICT-systeem als de back-ups worden getroffen
12.4.1.7	Er zijn maatregelen getroffen die zeker stellen dat voldoende, complete en juiste (log)informatie beschikbaar is om gebeurtenissen zorgvuldig te analyseren (onderzoeken).

Nr.	BBN2+ Maatregel
12.4.1.8	Onderstaande voorwaarden om onderzoek uit te kunnen voeren naar Gebruikershandelingen en systeemactiviteiten zijn ingevuld: 1) Er is bepaald welke Gebruikershandelingen, systeemactiviteiten, gebeurtenissen en/of beheeractiviteiten vastgelegd moeten worden. 2) Er is vastgelegd waar en hoe centralisering van logging is ingericht (inclusief configuratie-instellingen). 3) Er is een plan met daarin activiteiten die worden uitgevoerd (wie, wat en wanneer) indien logrecords op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd. 4) De systemen zijn zodanig geconfigureerd dat interne systeemklokken automatisch gesynchroniseerd worden. 5) Er is bepaald wat te doen bij het uitvallen van loggingmechanismen (alternatieve paden). 6) Er zijn bewaartermijnen vastgesteld voor de loginformatie. 7) De loggegevens zijn beveiligd tegen achteraf wijzigen/verwijderen door onbevoegden.
12.4.1.9	ICT-systemen leggen ten minste het volgende vast: • authenticatiegebeurtenissen; • bestands- en objectgebeurtenissen; • export- (bijv. uploads) en importgebeurtenissen (bijv. downloads); • gebeurtenissen betreffende Gebruikersaccounts; • gebeurtenissen betreffende accounts met speciale bevoegdheden.
12.4.1.10	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en over de bevindingen gerapporteerd. Om dit uit te kunnen voeren zijn onderstaande voorwaarde ingevuld: 1) De verschillende gelogde informatie wordt samengebracht voor analysedoeleinden. 2) De signaleringssystemen (detectie) maken tijdig melding van ongewenste gebeurtenissen (alarmeringen). 3) Er zijn procedures vastgelegd met daarin beschreven hoe en wanneer controles op logging moeten plaatsvinden en hoe taken op dit gebied belegd zijn. 4) Er is vastgelegd waar en hoe correlaties worden aangebracht (analyseren/ auditing). 5) De geregistreerde menselijke en systeemacties worden periodiek geanalyseerd. 6) De ongebruikelijke situaties (incidenten) worden periodiek geanalyseerd. 7) De geanalyseerde en beoordeelde gelogde gegevens worden geconsolideerd en gerapporteerd naar het hoogste management.
12.4.2.7	Offline gearchiveerde logbestanden zijn niet benaderbaar vanaf het ICT-systeem waarop ze gegenereerd zijn.

Nr.	BBN2+ Maatregel
12.6.1.2	*Update(s)*/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is (kritieke beveiligings-*Update(s)*/patches) worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiligings-*Update(s)*/patches moeten binnen vier weken na beschikbaar komen worden doorgevoerd. Als de inschatting is dat overige applicaties niet meer kunnen werken mag hiervan afgeweken worden, er moet dan wel een workaround bedacht worden. Indien nog geen patch beschikbaar is dient gehandeld te worden volgens het advies van de Informatiebeveiligingsdienst voor gemeenten (IBD).
12.6.1.3	Er mag alleen gebruik worden gemaakt van ICT-systemen (zowel soft- als hardware) die door de leverancier actief worden ondersteund, door het aanbieden van beveiligings-*Update(s)*/patches, het gaat hier om ICT-systemen die niet het einde van hun levenscyclus (End-of-life) hebben bereikt. Deze ICT-systemen dienen voordat de ondersteuning stopt te worden vervangen.
12.6.1.4	De CISO stelt, na overleg met de lijnmanager, systeemontwikkelaars en dienstenleveranciers en/of de ICT-afdeling, de eisen vast met betrekking tot: 1) Toegang tot hulpmiddelen voor audits van informatiesystemen om mogelijk misbruik of compromitteren te voorkomen. 2) Het gebruik van hulp*Programmatuur* waarmee systeem- en toepassingsbeheersmaatregelen zouden kunnen worden gepasseerd. 3) Het gebruik van technische hulpmiddelen waarbij wordt nagegaan in hoeverre in de ICT-componenten kwetsbaarheden voorkomen (kwetsbaarheidsanalyse). 4) Het gebruik van technische hulpmiddelen waarbij specifieke componenten of specifieke delen van de ICT-infrastructuur op zwakheden gecontroleerd worden (penetratietest). 5) Het gebruik van technische hulpmiddelen om te toetsen of de in productie zijnde ICT-componenten niet meer dan de vastgestelde noodzakelijke functies bieden (policycompliancychecks).
13.1.2.6	Het interne netwerk van Storage Area Networks (SANs) is van buitenaf niet toegankelijk, tenzij een Virtual Private Networks (VPN) gebruikt wordt.
13.1.2.7	Uitsluitend na advies van de CISO wordt SAN technologie en Network Attached Storage (NAS) technologie toegepast.
13.1.2.8	Scheid netwerkzones fysiek of logisch van elkaar, zet een minimale hoeveelheid netwerkcomponenten in op koppelvlakken (extern en indien noodzakelijk ook intern) die deze scheiding handhaven. Koppeling van netwerkzones kan plaatsvinden door een firewall of (reverse) proxies.
13.1.2.9	Het aantal externe koppelvlakken wordt beperkt tot het minimum dat vanuit *Beschikbaarheid* noodzakelijk is.
13.1.2.10	De beveiligingsarchitectuur van ICT-netwerken volgt het principe van minimalisatie: “deny by default and allow by necessity".
13.1.2.11	Ongeautoriseerde distributie van (vertrouwelijke) informatie binnen en buiten uw netwerken wordt voorkomen (geblokkeerd).
13.1.2.12	Uitsluitend door de CISO geadviseerde firewall componenten worden toegepast.

Nr.	BBN2+ Maatregel
13.1.2.13	De toegepaste firewalls beschermen maximaal de interne netwerkeigenschappen zoals IP-adressen zodat het (onnodig) vrijgeven van informatie tot een minimum wordt beperkt.
13.1.2.14	Verstoringen in de firewall functionaliteit leiden niet tot verlies van vertrouwelijkheid of integriteit, maar tot verlies van *Beschikbaarheid*. De failsave mode van de firewall mag niet leiden tot het verlies van integriteit of vertrouwelijkheid van informatie.
13.1.2.15	Domain Name System (DNS) Zone transfers worden beperkt.
13.1.2.16	Alleen geautoriseerde systemen kunnen een DNS zonetransfer uitvoeren van authoritative nameservers.
13.1.2.17	De DNS services beschikken niet over privileges.
13.1.2.18	Alleen noodzakelijke beheerders hebben toegang tot de DNS nameservers.
13.1.2.19	Wifi-apparatuur gebruikt IEEE 802.11 Wifi Protected Access 2 (WPA2) Enterprise (of nieuwer) en Extensible Authentication Protocol (EAP), in overeenstemming met de standaarden van het Forum.
13.1.2.20	Uitwisseling van informatie via netwerken die niet onder eigen beheer vallen (zoals het intranet/extranet) is uitsluitend toegestaan via toegang op afstand via de firewalls van de organisatie en mag niet onderschept of gemanipuleerd kunnen worden.
13.1.2.21	Accounts met verhoogde (of bijzondere) rechten worden continu gemonitord zodat misbruik of afwijkend gebruik van rechten wordt gedetecteerd.
13.1.2.22	Het beheer van accounts met verhoogde (of bijzondere) rechten worden continue gemonitord zodat ongeautoriseerde wijzigingen worden gedetecteerd,
13.2.3.6	De CISO beoordeeld ook de Voice over IP (VoIP) technologie dat onderdeel is van een ICT-systeem, met inbegrip van de IP-telefoons.
13.2.3.7	VoIP-apparaten authentiseren aan een VoIP-server.
13.2.3.8	VoIP-verkeer verloopt via een eigen netwerk, dat fysiek of logisch (Virtual LAN) is gescheiden van de overige netwerken.
13.2.3.9	VoIP toepassingen maken standaard gebruik van een versleutelde gegevensoverdracht
14.1.1.2	Er is *Documentatie* opgesteld voor de veilige configuratie en beheer van ICT-componenten, deze *Documentatie* dient ook aandacht te geven aan alle beveiligingsrelevante keuzes inclusief hardening. - Maak gebruik van bestaande richtlijnen van leveranciers en erkende kennisinstituten als NIST, SANS, et cetera.

Nr.	BBN2+ Maatregel
	- De ICT-componenten worden conform deze *Documentatie* ingericht en wijzigingen worden gedurende de gehele levenscyclus in de *Documentatie* bijgehouden (maak dit onderdeel van wijzigingsbeheer). - De *Documentatie* geldt tevens als uitgangspunt bij toezichtshandelingen.
14.1.1.3	De hardening van ICT-componenten wordt actueel gehouden (maak dit onderdeel van wijzigingsbeheer).
14.1.1.4	ICT-componenten die niet langer noodzakelijk zijn en/of niet meer wordt gebruikt, wordt verwijderd (maak dit onderdeel van wijzigingsbeheer).
14.1.1.5	De dienstenleverancier en/of ICT-afdeling past gedocumenteerde procedures toe voor de bescherming van alle ICT-componenten.
14.1.1.6	Op Virtuele Machines (VM) zijn alle maatregelen onverkort van toepassing, inclusief de volgende maatregelen die specifiek op VM zijn gericht: - Type 2 hypervisors zijn niet toegestaan (de CISO kan uitzonderingen maken); - Een fysieke server host uitsluitend VM's binnen hetzelfde domein; Voor VM's gelden dezelfde documentatie eisen als voor fysieke machines; - Toegang tot informatie over de inrichting van beschikbare VM wordt beperkt; - VM's die niet langer noodzakelijk zijn, worden buiten gebruik gesteld; - Gegevensoverdracht van een VM naar een ander VM, een ander systeem of de omgeving van de Gebruikersclient wordt voorkomen (bijvoorbeeld door het blokkeren van toegang vanaf beiden tot het clipboard en gedeelde gegevensopslag), tenzij expliciet toegestaan. - Firewalls e.d. worden niet gehost op dezelfde fysieke server als de VM's die zij beschermen;
14.1.1.7	De dienstenleverancier en/of ICT-afdeling ontwikkelt, onderhoudt en hanteert standaardconfiguraties voor gebruikte ICT-componenten waarbij hardening expliciet is uitgewerkt.
14.1.1.8	De dienstenleverancier en/of ICT-afdeling blijft controleren of ICT-componenten nog steeds ingericht zijn volgens de standaardconfiguratie.
14.1.1.9	De dienstenleverancier en/of de ICT-afdeling zoekt continu naar nieuwe kwetsbaarheden en dreigingen en rapporteert deze aan de lijnmanager en initieert het wijzigingsproces.
14.1.1.10	Het ICT-systeem is gebaseerd op een door de CISO geadviseerde beveiligingsarchitectuur.
14.2.2.2	Elke soort onderhoud en reparaties worden in overeenstemming met procedures voor configuratiebeheer goedgekeurd en gedocumenteerd.

Nr.	BBN2+ Maatregel
14.2.2.3	*Onderhoud* wordt uitsluitend door adequaat gescreend en gemachtigd *Personeel*, of door *Personeel* onder toezicht en op locatie uitgevoerd, tenzij er geen data op het ICT-component aanwezig of toegankelijk is
14.2.2.4	De dienstenleverancier en/of ICT-afdeling heeft configuratie management/ configuratiebeheer ingericht en hanteert hierbij vastgestelde procedures. Documentatie van wijzigingen en herbeoordeling door de CISO (of binnen het mandaat dat de ICT-afdeling van de CISO heeft gekregen) maakt deel uit van deze procedures.
14.2.3.3	Voordat nieuwe (versies van) ICT (hard- en software) in een omgeving wordt geïntroduceerd, vindt een beoordeling plaats van de impact op de veiligheid van die bestaande omgeving door middel van testen in een testomgeving (integriteit, afwezigheid van malware).
14.2.7.2	De organisatie controleert (log)bestanden met diagnostische gegevens op de gevoeligheid van deze gegevens alvorens deze naar externe partijen te sturen.
14.2.9.3	De dienstenleverancier en/of ICT-afdeling test software en firmware *Update(s)* voorafgaand aan installatie volgens vastgestelde (test)procedures als onderdeel van patchmanagement, releasemanagement en/of lifecycle management.
15.1.2.9	Op basis van de informatiebeveiligingseisen uit de offerteaanvraag/ Programma van Eisen (PvE) worden maatregelen expliciet opgenomen in de (inkoop-)contracten.
15.1.2.10	De BBN2+ infrastructuur maakt uitsluitend gebruik van geëvalueerde en goedgekeurde producten die de beveiliging waarborgen.
15.1.3.3	Er zijn voldoende middelen toegewezen om de BBN2+ infrastructuur te adequaat beschermen.
16.1.1.2	Er zijn vastgestelde procedures voor incident respons.
16.1.2.9	Bij vermoeden van opzet bij compromittering van BBN2+ informatie, wordt onverwijld melding gedaan door de CISO bij de portefeuillehouder voor informatiebeveiliging.
16.1.2.11	Systemen voor continue bewaking (Intrusion Dection System/ Intrusion Prevention System) geven automatisch een veiligheidswaarschuwing af om het beveiligings*Personeel* te waarschuwen.
16.1.5.3	Na een incident worden ICT-systemen in overeenstemming met een vooraf vastgestelde prioritering hersteld. Dit is in lijn met vastgestelde bedrijfscontinuïteitsplannen (BCM).

Nr.	BBN2+ Maatregel
16.1.6.3	De dienstenleverancier en/of de ICT-afdeling stelt na evaluatie van het incident een verbeterplan op en voert dit uit.
17.2.1.3	Voor cruciale ICT-systeemcomponenten binnen de BBN2+ infrastructuur is automatische failover/load balancing geïmplementeerd.
18.2.2.2	Tijdens de gehele levenscyclus van een ICT-dienst wordt beveiligingsdocumentatie opgesteld en actueel gehouden.
18.2.2.4	Periodiek (minimaal eens per drie jaar) en indien de omstandigheden daar aanleiding toe geven, vindt onafhankelijk toezicht door bijvoorbeeld de interne auditafdeling plaats om vast te stellen of de ICT-dienst nog steeds aan de eisen voldoet en de belangen voldoende bescherming krijgen. Diepgang en de borging van onafhankelijkheid van het toezicht hangt af van de omstandigheden. De onafhankelijkheid van de auditor kan bijvoorbeeld gerealiseerd worden door gebruik te maken van interne auditors van andere gemeenten en samenwerkingsverbanden of externe inhuur.
18.2.2.5	Technische beveiligingsmaatregelen zijn door een vertrouwde, onafhankelijke en deskundige partij afdoende bevonden, of in overleg met de CISO anderszins vastgesteld.
18.2.2.6	Noodzakelijke afwijkingen van de BIO (O-maatregelen) zijn uitsluitend toegestaan indien de GS hiervoor toestemming heeft verleend. (GS kan deze taak uiteraard mandateren.) Deze toestemming wordt verleend uitsluitend nadat een formele risicoafweging heeft aangetoond dat (bijvoorbeeld met vervangende maatregelen) het beveiligingsrisico als gevolg van de niet-naleving niet is toegenomen. Deze afwijking wordt gedocumenteerd en wordt periodiek gereviewd of het nog nodig is en of er aanvullende maatregelen nodig zijn om de risico's te verminderen.
18.2.3.3	BBN2+ informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen, de fysieke toegang en risico’s ten aanzien van de feitelijke veiligheid. Dit kan bijv. door (geautomatiseerde) kwetsbaarheidsanalyses of pentesten.