



Zeker-OnLine is een onafhankelijk en transparant keurmerk voor online dienstverlening (cloud services)

Versienummer 1.4 Ingangsdatum: 04 maart 2019 Publicatiedatum: 04 maart 2019

# doelstelling	Onderwerp	Toelichting beheersdoelstelling	Beheersdoelstelling	# beheersmaatregel	Deze beheersmaatregelen zijn een baseline of eerste invulling.	Deze handreiking probeert de doelstellingen en maatregelen te verduidelijken nergens zijn opsommingen limitatief tenzij anders vermeld.
1.1	Wet en regelgeving	De dienstaanbieder waarborgt dat de Nederlandse wet- en regelgeving worden toegepast.	De maatregelen bieden een redelijke mate van zekerheid dat de dienstaanbieder de Nederlandse wet- en regelgeving waarborgt in haar aangeboden dienst.	1.1.1	De dienstaanbieder verklaart het Nederlands recht van toepassing op zijn diensten en op eventuele conflicten met ondernemers die verband houden met die diensten.	Hier valt ook de Algemene verordening Gegevensverwerking vanaf 25 mei 2018 onder. Deze artikelen zien toe op het tot stand komen van een overeenkomst.
				1.1.2	De dienstaanbieder voldoet aan de wettelijke verplichtingen, waaronder de informatieverplichtingen van artikel 3:15d BW, 6:227b BW en 6:227c BW.	
				1.1.3	De dienstaanbieder biedt zijn diensten op een zodanige wijze aan dat ondernemers kunnen voldoen aan artikelen 47 t/m 53 van de Algemene wet inzake rijksbelastingen.	
1.2	Voorwaarden	De dienstaanbieder draagt er zorg voor dat zijn klant kennis kan nemen van de voorwaarden die hij hanteert.	De maatregelen bieden een redelijke mate van zekerheid dat de klant kennis kan nemen van de voorwaarden die dienstaanbieder hanteert.	1.2.1	De dienstaanbieder publiceert de voorwaarden die op zijn diensten betrekking hebben op zijn website en verstrekt deze voorwaarden tijdig en op een juiste wijze aan de ondernemer.	Deze maatregel beoogt te bewerkstelligen dat een afnemer inzicht krijgt in de wijzigingen tussen de verschillende voorwaarden. Op de juiste wijze duidt op de verplichting om de afnemer juist en volledig te informeren over wijzigingen. Een voorbeeld van juist en volledig informeren is een vereenvoudigde samenvatting van de wijzigingen met impact voor de afnemer. Het kan nimmer zo zijn dat verzwarende voorwaarden voor de gebruiker alleen via het plaatsen van nieuwe voorwaarden op de site worden doorgevoerd. Als een dienstaanbieder meerdere versies wil hanteren voor zijn afnemers, dan moeten al deze versies op de website worden opgenomen, dit geldt ook als er sprake is van een overgangperiode. Zeker-OnLine onderschrijft de code van het platform Internetveiligheid. Zie voor meer informatie: https://ecp.nl/activiteiten/werkgroep-notice-and-takedown .
				1.2.2	De dienstaanbieder past een adequaat versiebeheer toe op de voorwaarden die op zijn diensten betrekking hebben. De dienstaanbieder publiceert alle verschillende van toepassing zijnde versies, met een vermelding van versienummer en -datum, op zijn website.	
				1.2.3	De dienstaanbieder hanteert een notice- en takedownbeleid volgens de gedragscode Notice-and-Take-Down van ECP voor de omgang met onrechtmatige content en content die anderszins inbreuk maakt op rechten van derden.	
				1.2.4	De dienstaanbieder neemt in de voorwaarden die op zijn diensten betrekking hebben een deugdelijke geheimhoudingsclausule op.	
1.3	AVG	De dienstaanbieder respecteert en waarborgt de privacyrechten van zijn klanten.	De maatregelen bieden een redelijke mate van zekerheid dat de dienstaanbieder de privacyrechten van zijn klanten respecteert en waarborgt deze rechten overeenkomstig de Algemene Verordening Gegevensbescherming.	1.3.1	De organisatie heeft een overzicht van de gegevensverwerkingen en op basis daarvan is DPIA uitgevoerd.	De dienstaanbieder heeft een proces voor de nieuwe ontwikkelingen waarbij wordt vastgesteld dat de belangen van de betrokkenen zijn meegenomen. Bij nieuwe verwerkingen wordt vastgesteld dat er niet meer data wordt verzameld dan noodzakelijk in samenhang met doel van verantwoordelijke (dataminimalisatie). Bij een grotere organisatie is een privacy officer beschikbaar en bereikbaar voor klanten. Kleinere dienstverleners kunnen volstaan met het beleggen van deze privacy functie bij een medewerker. De dienstaanbieder heeft een (calamiteiten)plan opgesteld waarin de omgang met beveiligingslek wordt beschreven met betrekking tot het bepalen van een datalek. In dit plan is nader uitgewerkt wat een datalek is en een procedure inclusief beslisboom ter ondersteuning inzake wie, wat, wanneer, waar en hoe moet melden. Wie er verantwoordelijk is voor het doen van een melding van een datalek bij de relevante toezichthouder dan wel de verantwoordelijke van de gegevens. Op de website van www.ICTRecht.nl of van de autoriteit Persoonsgegevens zijn voorbeelden te downloaden Verwerker heeft een proces waarbij vastgesteld wordt dat met alle toeleveranciers een verwerkersovereenkomst is gesloten.
				1.3.2	De dienstaanbieder analyseert jaarlijks of haar Functionaris Gegevensbescherming (hierna FG) voldoet aan de eisen van de AVG en of het voor haar wettelijk verplicht is een FG aan te stellen. Indien er geen FG is aangesteld is de functie van een privacy officer belegd.	
				1.3.3	De dienstaanbieder heeft een proces met betrekking tot datalekken.	
				1.3.4	De dienstaanbieder sluit met alle toeleveranciers een verwerkersovereenkomst die voldoet aan de bepalingen uit de AVG.	

# doelstelling	Onderwerp	Toelichting beheersdoelstelling	Beheersdoelstelling	# beheersmaatregel	Deze beheersmaatregelen zijn een baseline of eerste invulling.	Deze handreiking probeert de doelstellingen en maatregelen te verduidelijken nergens zijn opsommingen limitatief tenzij anders vermeld.
				1.3.5	Als de dienstaanbieder gebruikmaakt van een derde partij om persoonsgegevens te laten verwerken, verstrekt de dienstaanbieder deze gegevens enkel aan organisaties buiten de Europese Ruimte op basis van: adequaatsheidsbesluiten van de Europese Commissie, passende waarborgen of bindende bedrijfsvoorschriften of indien er toestemming van de betrokkenen is ontvangen. Bewaren van persoonsdata is ten alle tijde binnen de Europese Economische Ruimte.	
				1.3.6	De dienstaanbieder past Privacy by Design toe bij het mogelijk maken van nieuwe verwerkingen.	Deze maatregel moet onder andere worden toegepast bij doelstelling 2.4 zoals uitgewerkt in de infrastructurele laag.
				1.3.8	De dienstaanbieder heeft met alle gebruikende/afnemende partijen een contract afgesloten afhankelijk van zijn rol is dit een verwerkersovereenkomst of een privacy statement.	De rechten zoals genoemd in de AVG van betrokkene zijn in deze contracten verder uitgewerkt. De volgende rechten zijn uitgewerkt: recht op toegang/inzage, verbetering, verwijdering, beperking van verwerking, overdraagbaarheid en bezwaar. Een dienstaanbieder kan rechtstreeks werken met betrokkene in die situatie worden de rechten vastgelegd in een privacy statement. Dienstaanbieders die werken met intermediairs zorgen ervoor dat de rechten worden uitgewerkt in verwerkersovereenkomsten met deze intermediairs.
1.4	Gegevens	De dienstaanbieder waarborgt dat de klant eigenaar is en blijft van de gegevens die in het kader van de online dienstverlening met betrekking tot zijn organisatie worden ingevoerd en verzameld. In geval van het beëindigen van de overeenkomst tussen dienstaanbieder en klant zijn er afspraken gemaakt over het gegevensbeheer en de bewaartermijn.	De maatregelen bieden een redelijke mate van zekerheid dat: 1. dienstaanbieder waarborgt dat de klant eigenaar is en blijft van de gegevens die in het kader van de online dienstverlening met betrekking tot zijn organisatie zijn ingevoerd en verzameld en 2. in geval van het beëindigen van de overeenkomst tussen dienstaanbieder en klant er afspraken zijn gemaakt over het gegevensbeheer en de bewaartermijn.	1.4.1	De dienstaanbieder neemt in de voorwaarden die op zijn diensten betrekking hebben op, dat de afnemer van de dienst eigenaar blijft van alle voor/door hem ingevoerde gegevens.	
				1.4.2	De dienstaanbieder biedt de mogelijkheid om de gegevens in een gangbaar formaat te exporteren (dataportabiliteit). De wijze van overdracht en voorwaarden zijn helder beschreven bij het aangaan van het contract.	Een beschrijving van de structuur van de export is verplicht. Het gebruik binnen de sector waarin de dienstaanbieder opereert, bepaalt het gangbare format. Dit moet een van de meest gehanteerde standaarden zijn. Artikel 18 AVG is tevens van toepassing. De klant heeft het recht persoonsgegevens op te vragen die hij aan de dienstaanbieder heeft verstrekt. De dienstaanbieder moet deze gegevens aanleveren in een gestructureerd bestand zodat ze meegenomen kunnen worden naar een andere dienstverlener. Een voorbeeld is de meest actuele auditfile die is voorgeschreven door de Belastingdienst. Factoren die bepalend zijn de functionaliteiten van de opvolgende partijen. Uitgangspunt is alle data mee kan worden genomen.
				1.4.3	De dienstaanbieder wijst de ondernemer vóór het beëindigen van de overeenkomst expliciet op diens verplichtingen in het kader van het bewaren van de gegevens. Hij doet hem daarbij een aanbod om de gegevens te bewaren en te archiveren dan wel ze aan hem over te dragen alvorens deze te verwijderen.	Deze maatregel heeft met name betrekking op voor de bewaarplicht en het mogelijk maken van een heraanlevering.
				1.4.4	De dienstaanbieder archiveert de gegevens van de ondernemer gedurende een termijn van tenminste zes maanden als de overeenkomst door faillissement van de ondernemer wordt beëindigd. In de overeenkomst neemt de dienstaanbieder een bepaling op die dit regelt.	De zes maanden termijn start op de dag van inschrijving van de onderneming in het insolventieregister. Tijdens deze termijn hebben alleen daartoe bevoegde (opsporings-)ambtenaren en de curator toegang tot de gegevens. In de overeenkomst neemt de dienstaanbieder een bepaling op die dit regelt.
1.5	Doelbinding	De dienstaanbieder waarborgt dat betrokkene eenduidig en transparant zijn ingelicht over de doeleinden van de verwerkingen en zorgen dat de toestemming op heldere wijze per doel wordt gegeven.	De maatregelen bieden een redelijke mate van zekerheid dat de dienstaanbieder alleen persoonsdata verzamelt die noodzakelijk is voor de uitvoering van de online dienst.	1.5.1	De dienstaanbieder neemt in de voorwaarden/verwerkersovereenkomst/privacy overeenkomst het doel op waarvoor persoonsgegevens worden verzameld en welke persoonsgegevens worden verzameld.	Het specificeren van de verwerkingen die zullen plaatsvinden en het bijbehorende doel daarvan.
				1.5.2	Voor ieder doel waarvoor dienstaanbieder persoonsgegevens wil verwerken en waarvoor toestemming nodig is, dient aparte toestemming te worden gevraagd.	
				1.5.3	Het intrekken van toestemming is voor de gebruiker net zo makkelijk als het geven van de toestemming.	

# doelstelling	Onderwerp	Toelichting beheersdoelstelling	Beheersdoelstelling	# beheersmaatregel	Deze beheersmaatregelen zijn een baseline of eerste invulling.	Deze handreiking probeert de doelstellingen en maatregelen te verduidelijken nergens zijn opsommingen limitatief tenzij anders vermeld.
1.6	Continuïteit	De dienstaanbieder waarborgt een continue beschikbaarheid van de desbetreffende online dienstverlening.	De maatregelen bieden een redelijke mate van zekerheid dat de aangeboden online dienst continu beschikbaar is.	1.5.4	Alle verwerkingen van persoonsgegevens met doelbinding zijn vastgelegd in een register.	
				1.6.1	De intellectuele rechten van de applicatie zijn in eigendom van een andere entiteit dan de werkmaatschappij van de dienstaanbieder of er is een andere voorziening getroffen die de overeengekomen beschikbaarheid van de online dienstverlening waarborgt.	
				1.6.2	De dienstaanbieder draagt zorg voor het treffen van zodanige voorzieningen dat in geval van faillissement, of in geval van een andere situatie die tot gevolg heeft dat de dienstaanbieder zijn dienst niet kan continueren, de diensten gedurende zes maanden na een dergelijke gebeurtenis beschikbaar blijven. Deze voorzieningen zijn bedoeld om de ondernemer in staat te stellen om zijn gegevens over te zetten naar een andere dienstaanbieder.	
				1.6.3.	De dienstaanbieder vermeldt in de voorwaarden die op zijn diensten betrekking hebben, dat hij zijn diensten slechts eenzijdig kan beëindigen met inachtneming van een opzegtermijn van zes maanden, tenzij er sprake is van tekortkomingen van de kant van de gebruiker van de dienstverlening.	

# doelstelling	Onderwerp	Toelichting beheersdoelstelling	Beheersdoelstelling	# beheersmaatregel	Deze beheersmaatregelen zijn een baseline of eerste invulling.	Deze handreiking probeert de doelstellingen en maatregelen te verduidelijken nergens zijn opsommingen limitatief tenzij anders vermeld.
2.1	Vastleggen van het dienstverleningsproces en de afhankelijkheden.	De dienstaanbieder heeft processen, administratieve richtlijnen en procedures gedefinieerd voor alle functies. In het bijzonder heeft hij daarbij aandacht voor de beheersing, het waarborgen van het kwaliteitsniveau, risicobeheer, informatiebeveiliging, gegevensbeheer, systeembeheer en functiescheiding. Om het gewenste niveau van de dienstverlening te waarborgen is het management van de afdeling die verantwoordelijk is voor dienstverlening betrokken bij de besluitvorming hierover. De dienstaanbieder moet zorgen voor het adequaat inrichten van zijn organisatie en het formeel en eenduidig beleggen van verantwoordelijkheden. Het moet duidelijk zijn welke rechten en verantwoordelijkheden eenieder binnen de organisatie heeft.	De maatregelen bieden een redelijke mate van zekerheid dat dienstaanbieder processen, administratieve richtlijnen en procedures definieert voor alle functies die betrekking hebben op de dienstverlening.	2.1.1 2.1.2 2.1.3 2.1.4 2.1.5 2.1.6 2.1.7 2.1.8	<p>2.1.1 Het management van de dienstaanbieder is eindverantwoordelijk voor en eigenaar van de risico's die met de dienst verband houden.</p> <p>2.1.2 Binnen de organisatie zijn de verantwoordelijkheden voor het risicobeheer, informatiebeveiliging en compliance eenduidig belegd.</p> <p>2.1.3 De organisatie kent een beleid voor risicobeheer, informatiebeveiliging en compliance. Het beleid is gedocumenteerd en wordt door het management actief uitgedragen.</p> <p>2.1.4 De dienstaanbieder legt rollen en verantwoordelijkheden die met de dienst verband houden eenduidig vast en communiceert hierover binnen de organisatie.</p> <p>2.1.5 Taken en bevoegdheden zijn duidelijk omschreven, zodat medewerkers ongehinderd hun functie kunnen uitvoeren.</p> <p>2.1.6 Wijzigingen in de organisatie leiden tot het overeenkomstig aanpassen van rollen, verantwoordelijkheden, taken en bevoegdheden. Ten minste eenmaal per jaar wordt vastgesteld dat de formele vastlegging overeenkomt met de praktische gang van zaken.</p> <p>2.1.7 De taken en bevoegdheden zijn zo verdeeld, dat de kans op verstoring of misbruik door een individuele medewerker van een kritiek proces minimaal is. Het management stelt periodiek voor de kritieke processen vast, dat de medewerkers handelen binnen hun bevoegdheden.</p> <p>2.1.8 Sleutelfunctionarissen voor de dienstverlening zijn geïdentificeerd. De afhankelijkheid van individuen is zo gering mogelijk.</p>	Deze maatregelen hebben betrekking op de interne formele vastlegging.
2.2	risicobeheer	De dienstaanbieder hanteert risicobeheer om adequaat op gebeurtenissen in de dienstverlening te kunnen reageren. Het risicobeheer is er op gericht om de klanten zo ongehinderd mogelijk de dienst te laten gebruiken. De aard en omvang van de risico's die de klanten kunnen lopen zijn duidelijk, met maatregelen ingeperkt tot een acceptabel niveau en goed begrepen door het management. Iedere potentiële inbreuk op de dienstverlening is vastgesteld, geanalyseerd en beoordeeld. Om dit te bereiken moet de dienstaanbieder het risicobeheer volledig integreren binnen alle lagen van zijn organisatie en dat constant toepassen. Hij moet de risico's periodiek beoordelen en zijn calamiteitenplan voortdurend verbeteren en daarover communiceren.	De maatregelen bieden een redelijke mate van zekerheid dat het risicobeheer op alle niveaus inclusief management geïntegreerd is. Risicobeheer is gericht op het waarborgen van een continue en betrouwbare dienst door middel van een proces van evaluatie van risico's van de dienst en de uitvoering van controles om de risico's tot een aanvaardbaar niveau terug te brengen.	2.2.1 2.2.2 2.2.3 2.2.4 2.2.5	<p>2.2.1 Risicomanagement waarborgt een redelijke mate van zekerheid dat interne en externe bedreigingen op de dienstverlening worden vastgesteld en beoordeeld.</p> <p>2.2.2 Significante gebeurtenissen die de dienstverlening bedreigen worden geïdentificeerd, geregistreerd en geëvalueerd.</p> <p>2.2.3 De kans op het ontstaan en de impact van een risico worden kwalitatief en kwantitatief gewogen.</p> <p>2.2.4 De dienstaanbieder kent een methode waarbij maatregelen worden genomen om de gevolgen van een actueel risico te verminderen tot een aanvaardbaar niveau.</p> <p>2.2.5 Het risicobeheersysteem is in alle lagen van de organisatie geïmplementeerd, wordt periodiek beoordeeld op werking en geschiktheid en wordt voortdurend onderhouden.</p>	Op regelmatige basis wordt het risicobeheersysteem geëvalueerd, tenminste jaarlijks of indien noodzakelijk vaker. Van alle risico's die zijn vastgesteld en beoordeeld zijn maatregelen voor genomen of indien dit niet gebeurt dient de directie (rest)risico's bewust en formeel te accepteren. Risico beheer is een continue proces waarbij periodiek formeel stil gestaan wordt. Significante wijzigingen zijn wijzigingen waarvan waarschijnlijk is dat de gebruikende partij impact ervaart of wijzigingen waardoor de kans bestaat dat doelstellingen met betrekking tot dit normenkader niet behaald zouden kunnen worden. Elementen in deze afweging die duidelijk naar voren moeten komen: de kans van een bedreiging, de mogelijke impact en op de wijze waarop de leverancier heeft vastgesteld.
2.3	kennisoverdracht	Het management van de dienstverlener is verantwoordelijk voor de aard, de omvang en de kwaliteit van de geleverde diensten, voor de wijze waarop de dienstverlening plaatsvindt en voor de interne beheersing. Hiervoor is het nodig dat de IT-organisatie voldoende kennis overdraagt aan het management, zodat het in staat is om het eigenaarschap van de systemen op zich te nemen. Medewerkers moeten voldoende getraind zijn en voldoende kennis hebben om de dienstverlening op het vereiste niveau te leveren. Daarom moeten de medewerkers beschikken over competenties om het systeem en de daaraan gerelateerde infrastructuur efficiënt en effectief te leveren, te ondersteunen en te onderhouden.	De maatregelen bieden een redelijke mate van zekerheid dat het management van de dienstverlener in staat is om de verantwoordelijkheid voor de aard, de omvang en de kwaliteit van de aangeboden dienst en de wijze waarop de dienstverlening plaatsvindt op zich te nemen en dat alle werknemers voldoende training en kennis krijgen om de dienst op het vereiste niveau uit te voeren.	2.3.1 2.3.2 2.3.3 2.3.4 2.3.5	<p>2.3.1 Het management is eigenaar van de systemen.</p> <p>2.3.2 Het management heeft kennis van de systemen en geleverde diensten.</p> <p>2.3.3 Voor de kennisoverdracht aan medewerkers zijn trainingsmateriaal en/of proces- en procedurebeschrijvingen, technische documentatie en functie- en taakomschrijvingen aanwezig.</p> <p>2.3.4 Medewerkers zijn voldoende getraind om de functies op het vereiste niveau uit te voeren.</p> <p>2.3.5 Management en medewerkers communiceren regelmatig over de geleverde diensten en veranderende omstandigheden. Enkele voorbeelden van deze communicatie zijn notulen, e-mails en notities.</p>	

# doelstelling	Onderwerp	Toelichting beheersdoelstelling	Beheersdoelstelling	# beheersmaatregel	Deze beheersmaatregelen zijn een baseline of eerste invulling.	Deze handreiking probeert de doelstellingen en maatregelen te verduidelijken nergens zijn opsommingen limitatief tenzij anders vermeld.
2.4	Beheer van wijzigingen (i) acceptatie	Het beheer van wijzigingen is een cruciaal proces voor een ongehinderde dienstverlening. Voor het doorvoeren van wijzigingen moet sprake zijn van een formele procedure voor wat betreft de (i) acceptatie, (ii) de planning, (iii) de uitvoering en (iv) de bewaking. Wijzigingen moeten worden geautoriseerd met inachtneming van de "impact" op de dienstverlening om de kans op ongewenste (neven)effecten op de dienstverlening tot een acceptabel niveau te verminderen.	De maatregelen bieden een redelijke mate van zekerheid dat dienstverlening ongehinderd doorgaat bij het implementeren van wijzigingen; hiervoor moeten wijzigingen via een formele procedure voor wat betreft (i) acceptatie, (ii) de planning, (iii) de uitvoering en (iv) de bewaking worden doorgevoerd.	2.4.1	Voorgestelde wijzigingen worden systematisch geïnclassificeerd op impact.	
				2.4.2	Voorgestelde wijzigingen worden geautoriseerd met inachtneming van de impactanalyse.	Procedure impactanalyse kan beschreven staan in het handboek.
				2.4.3	Voorgestelde technische wijzigingen worden geprioriteerd. De voorgestelde wijzigingen worden adequaat gecommuniceerd indien er impact is voor het gebruik.	
				2.4.4	De organisatie voorziet in een procedure waarbij wijzigingen in de functionaliteit worden geprioriteerd en gepland in overleg met de betrokken medewerkers.	
				2.4.5	De organisatie voorziet in een procedure waarbij achteraf kan worden vastgesteld of een change niet van invloed is op overige functionaliteiten indien een urgente wijziging niet volgens de reguliere procedure is afgehandeld. In dit geval moeten overgeslagen controlestappen achteraf worden doorlopen.	Doel vaststellen dat change niet van negatieve invloed is op overige functionaliteiten.
				2.4.6	Er is een beveiligde testomgeving beschikbaar die representatief is voor de productieomgeving.	
	Beheer van wijzigingen (ii) de planning	Het beheer van wijzigingen is een cruciaal proces voor een ongehinderde dienstverlening. Voor het doorvoeren van wijzigingen moet sprake zijn van een formele procedure voor wat betreft de (i) acceptatie, (ii) de planning, (iii) de uitvoering en (iv) de bewaking. Wijzigingen moeten worden gepland op deze juist, tijdig en volledig door te voeren en zodoende de noodzakelijke verbeteringen te realiseren of de instandhouding van de dienstverlening te waarborgen.	De maatregelen bieden een redelijke mate van zekerheid dat dienstverlening ongehinderd doorgaat bij het implementeren van wijzigingen; hiervoor moeten wijzigingen via een formele procedure voor wat betreft (i) acceptatie, (ii) de planning, (iii) de uitvoering en (iv) de bewaking worden doorgevoerd.	2.4.7	Voor elke significante wijziging is een testplan opgesteld en goedgekeurd door management en medewerkers.	Significante wijziging, of een wijziging significant is moet door de dienstverlener worden ingeschat. Tijdens de audit vindt afstemming hierover met de auditor plaats.
				2.4.8	Het testplan is gebaseerd op organisatiebrede standaarden, waarbij aandacht is voor de verschillende rollen, verantwoordelijkheden en acceptatiecriteria.	
				2.4.9	Voorafgaand aan die wijziging wordt een back out/fall back -scenario opgesteld als onderdeel van het implementatieplan. Het scenario is afgestemd met de medewerkers en is goedgekeurd door het management.	
				2.4.10	Alle significante wijzigingen worden voorafgaand aan de migratie naar de productieomgeving onafhankelijk getest in overeenstemming met het gedefinieerde testplan, waarna de testresultaten worden geaccordeerd door het management.	Significante wijzigingen zijn wijzigingen waarvan waarschijnlijk is dat de gebruikende partij impact ervaart of wijzigingen waardoor de kans bestaat dat doelstellingen met betrekking tot dit normenkader niet behaald zouden kunnen worden.
				2.4.11	Wijzigingen die een conversie van gegevens en/of een migratie van infrastructuur omvatten, worden gepland op dezelfde wijze als significante wijzigingen voortkomend uit het ontwikkelproces van de dienst, inclusief audit trails en back out/fall back -scenario.	
				2.4.12	De functionaris verantwoordelijk voor de technische controlefunctie van de webapplicaties voert periodiek (technische) evaluaties (codereview) van de beveiligingsfunctionaliteit van de webapplicaties uit.	Essentie is dat reviewer en de schrijver in de code gescheiden rollen zijn maar dat deze rollen kunnen verschillen per situatie. Dit moet de duidelijk uitgewerkt zijn in de procesbeschrijving.
Beheer van wijzigingen (iii) de uitvoering	Het beheer van wijzigingen is een cruciaal proces voor een ongehinderde dienstverlening. Voor het doorvoeren van wijzigingen moet sprake zijn van een formele procedure voor wat betreft de (i) acceptatie, (ii) de planning, (iii) de uitvoering en (iv) de bewaking. Wijzigingen moeten worden beoordeeld op doeltreffendheid om het risico te verminderen dat ze niet, of slechts gedeeltelijk, bijdragen aan verbetering van de dienstverlening of zelfs storend zijn voor de dienstverlening.	De maatregelen bieden een redelijke mate van zekerheid dat dienstverlening ongehinderd doorgaat bij het implementeren van wijzigingen; hiervoor moeten wijzigingen via een formele procedure voor wat betreft (i) acceptatie, (ii) de planning, (iii) de uitvoering en (iv) de bewaking worden doorgevoerd.	2.4.13	Een wijziging wordt pas afgesloten nadat is gecontroleerd of alle activiteiten zijn afgerond en alle wijzigingen zijn geregistreerd.	In deze fase moet geëvalueerd worden of het doel bereikt (of moeten we terug naar de oude situatie) en is iedereen geïnformeerd t.a.v. situatie ingeval van incrementeel uitrollen.	
			2.4.14	Er wordt voortgangsbewaking uitgevoerd op de tijdige afhandeling van voorgestelde wijzigingen.		
			2.4.15	De organisatie voorziet in een procedure waarbij achteraf kan worden vastgesteld of een change niet van invloed is op overige functionaliteiten indien een urgente wijziging niet volgens de reguliere procedure is afgehandeld. In dit geval moeten overgeslagen controlestappen achteraf worden doorlopen.		
			2.4.16	Er is een beveiligde testomgeving beschikbaar die representatief is voor de productieomgeving.		
			2.4.17	Voor elke significante wijziging is een testplan opgesteld en goedgekeurd door management en medewerkers.		
			2.4.18	Het testplan is gebaseerd op organisatiebrede standaarden, waarbij aandacht is voor de verschillende rollen, verantwoordelijkheden en acceptatiecriteria.		
2.5	Definitie en management van de dienstverlening	De klanten moeten in staat zijn om de karakteristieken en voorwaarden van de dienstverlening, zoals die zijn opgenomen in de	De maatregelen bieden een redelijke mate van zekerheid dat de klant in staat is om de karakteristieken en	2.5.1	Management en medewerkers zijn betrokken bij de definitie van de dienst en de bijbehorende voorwaarden.	

# doelstelling	Onderwerp	Toelichting beheersdoelstelling	Beheersdoelstelling	# beheersmaatregel	Deze beheersmaatregelen zijn een baseline of eerste invulling.	Deze handreiking probeert de doelstellingen en maatregelen te verduidelijken nergens zijn opsommingen limitatief tenzij anders vermeld.
		overeenkomst tussen de dienstverlener en de klant, te begrijpen. Hierdoor moet het voor de klanten duidelijk zijn hoe de dienstverlening het eigen bedrijfsproces raakt en waarvoor de dienstaanbieder aansprakelijk is. De dienstaanbieder stelt voortdurend vast of de dienstverlening in overeenstemming is met de overeenkomst. Hij rapporteert hierover periodiek naar de klanten in een begrijpelijke vorm. Periodiek wordt ook beoordeeld of de overeenkomst nog past bij de huidige dienstverlening en (toekomstige) ontwikkelingen	voorwaarden van de dienstverlening, zoals die zijn opgenomen in de overeenkomst tussen de dienstverlener en de klant, te begrijpen en vastbieden dat de dienst conform deze voorwaarden wordt uitgevoerd.	2.5.2	Het management accordeert de diensten en voorwaarden. Ze zijn beschreven in een vorm die voor de klanten begrijpelijk en eenvoudig toegankelijk is.	
				2.5.3	De diensten en voorwaarden zijn in overeenstemming met de overeenkomst. Management en medewerkers zijn bekend met en onderschrijven de overeenkomst.	
				2.5.4	In de overeenkomst zijn tenminste de volgende onderdelen van de dienst beschreven: beschikbaarheid, prestatie, betrouwbaarheid, beveiliging, mate van ondersteuning en continuïteit.	
				2.5.5	De dienstaanbieder sluit met de klant voor elke te leveren dienst een overeenkomst.	Mantelovereenkomst met daarin de diensten uitgesplitst en gedefinieerd kan voorkomen dat voor elke extra dienst een overeenkomst opgesteld moet worden, uitgangspunt blijft dat er met alle klanten bindende afspraken gemaakt moeten worden. Bij kleine aanvullende diensten kan een e-mail invulling geven aan deze maatregel. In de overeenkomst moet duidelijk zijn wie geautoriseerd is van de klant om een opdracht mag geven. Een panel kan ook een wijze zijn van een invulling.
				2.5.6	De dienstaanbieder zorgt ervoor dat de geleverde prestaties continu worden gemeten en geregistreerd.	Continu is in principe 24*7. De meting van de prestaties vindt ook buiten het datacenter plaats.
				2.5.7	De dienstaanbieder analyseert de metingen en eventuele signalen over afgesproken prestaties die niet werden gerealiseerd. Zo nodig ondernemt hij passende acties.	
				2.5.8	Periodiek rapporteert de dienstaanbieder aan de klanten over de gerealiseerde dienstenniveaus, de geplande en uitgevoerde wijzigingen en de incidenten die zich hebben voorgedaan. Het rapport is helder en eenvoudig toegankelijk voor klanten en bevat analyses om positieve en negatieve trends vast te stellen.	
2.6	Beheer leveranciers	De dienstverlening vraagt om een goede beheersing van de leveranciers waarvan de dienstverlening afhankelijk is. Daarom registreert de dienstaanbieder wat de relevante uitbestede diensten zijn en welke leveranciers hierbij zijn betrokken. Hij onderkent de risico's die kleven aan het afnemen van diensten bij leveranciers en beperkt deze tot een aanvaardbaar niveau. De dienstaanbieder stelt vast of de leverancier de uitbestede diensten levert conform de overeenkomst om er zeker van te zijn dat de dienstverlening naar klanten voldoet aan het afgesproken niveau. De dienstaanbieder maakt een inschatting of de leverancier blijft voldoen aan de vraag en concurrerend is met alternatieve leveranciers en marktomstandigheden, om zodoende ook de eigen dienst in de nabije toekomst met voldoende kwaliteit te kunnen realiseren.	De maatregelen bieden zeker dat de uitbestede dienstverlening op het vereiste niveau van de dienstverlener en Zeker-Online worden uitgevoerd zodat de dienstverlener de beheersdoelstellingen kan halen voor zijn aangeboden dienst.	2.6.1	Het management en de medewerkers zijn betrokken bij het identificeren van de relaties met externe leveranciers.	
				2.6.2	De relevante relaties met leveranciers zijn geïdentificeerd. Het is helder in welke mate de leverancier kritiek is voor de dienstverlening, welke rollen en verantwoordelijkheden er in de relatie met de leverancier bestaan en welke doelen voor de samenwerking zijn geformuleerd. Ook zijn de afspraken duidelijk die over (het niveau van) de dienstverlening zijn overeengekomen.	
				2.6.3	In een contract met een derde partij voor de uitbestede levering of beheer van een webapplicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.	
				2.6.4	Periodiek worden de risico's ten aanzien van uitbestede diensten geïdentificeerd en geëvalueerd.	
				2.6.5	Prestaties in het kader van relevante uitbestede diensten worden continu gemeten en geregistreerd. Enkele voorbeelden van dergelijke uitbestede diensten zijn serverdiensten, web services en diverse koppelingen met partijen.	Voorbeelden van continue meting en registratie kunnen zijn een combinatie van de volgende maatregelen: 3402 type II en overige rapportages ontvangen van de leverancier, notulen van overleg.
				2.6.6	De metingen van de prestaties en eventuele signalen voor het overschrijden van kritische kwaliteitsgrenzen worden geanalyseerd en vergeleken met de gemaakte afspraken.	
				2.6.7	Rapportages over het niveau van de geleverde diensten, al of niet gerealiseerde doelstellingen en verwachtingen over prestaties in de nabije toekomst, worden beoordeeld.	De prestaties van uitbestede diensten als hosting-, en housing services worden door een externe auditor beoordeeld, de uitkomsten worden gecommuniceerd middels een assurance-rapport.
2.7	Prestatie en capaciteitsplanning	Een goede dienstverlening vraagt om een periodieke beoordeling van de prestaties en de capaciteit om zodoende de beschikbaarheid voor nu en in de nabije toekomst te waarborgen. De	De maatregelen bieden een redelijke mate van zekerheid dat er te allen tijde voldoende capaciteit beschikbaar is - nu en in de nabije toekomst - voor het uitvoeren van de	2.7.1	De dienstaanbieder heeft een actueel, gedocumenteerd en door het management geaccordeerd beschikbaarheids- en capaciteitsplanning voor de dienstverlening.	

# doelstelling	Onderwerp	Toelichting beheersdoelstelling	Beheersdoelstelling	# beheersmaatregel	Deze beheersmaatregelen zijn een baseline of eerste invulling.	Deze handreiking probeert de doelstellingen en maatregelen te verduidelijken nergens zijn opsommingen limitatief tenzij anders vermeld.
		dienstaanbieder stelt vast of er voldoende capaciteit aan IT-hulpmiddelen aanwezig is om de geplande dienstverlening te realiseren. De daadwerkelijke prestaties en de beschikbare capaciteit worden voortdurend gemeten, geregistreerd en periodiek beoordeeld. De dienaarbieder zet tijdig, additionele IT-hulpmiddelen in als de planning of realisatie hierom vraagt.	dienst.	2.7.2	De dienaarbieder zorgt ervoor dat beschikbaarheid en capaciteitsverbruik van de dienstverlening en de IT-hulpmiddelen continu worden gemeten en geregistreerd.	
				2.7.3	Capaciteitsmetingen en beschikbaarheidsmetingen worden periodiek geanalyseerd en afgezet ten opzichte van de gestelde eisen en de verwachte werklast.	
				2.7.4	Periodiek voert de dienaarbieder ten aanzien van de werklast en eventuele incidenten trendanalyses en voorspellingen uit die als input dienen voor het beschikbaarheids- en capaciteitsplanning.	
				2.7.5	De dienaarbieder rapporteert aan de klanten over beschikbaarheid en capaciteit zoals afgesproken in de overeenkomst.	
				2.7.6	Periodiek wordt het beschikbaarheids- en capaciteitsplanning geëvalueerd, zo nodig geactualiseerd en door het management geaccordeerd.	
2.8	Beheersing continue dienstverlening	Om de dienstverlening continu overeenkomstig de overeenkomst te kunnen realiseren is het nodig om een IT-continuïteitsplan te ontwerpen, te testen en te onderhouden. Het doel daarvan is om de impact op de dienstverlening in het geval van een grote storing te minimaliseren. Het continuïteitsplan prioriteert het belang van de onderdelen van de dienst, zodat de meest kritieke als eerste kunnen worden hersteld wanneer zich een calamiteit voordoet. Door het continuïteitsplan regelmatig te testen weet de dienaarbieder dat de dienstverlening effectief kan worden hersteld, komen eventuele tekortkomingen aan het licht en blijft het plan relevant. De dienaarbieder zorgt voor de beschikbaarheid van apparatuur, programmatuur en gegevens op een alternatieve locatie, zodat de dienstverlening bij een calamiteit snel kan worden hersteld. Als zich een calamiteit voordoet wordt dit geregistreerd, geanalyseerd en met de klant gecommuniceerd.	De maatregelen rondom en in het IT-continuïteitsplan waarborgen een redelijke mate van zekerheid dat de impact van zeer grote storingen minimaal is op dienstverlening.	2.8.1	Er is een actueel, gedocumenteerd en door het management geaccordeerd continuïteitsplan voor de dienstverlening. Periodiek evalueert het management het continuïteitsplan.	
				2.8.2	Het continuïteitsplan beschrijft helder de richtlijnen, rollen en verantwoordelijkheden, procedures, communicatieprocessen en testbenaderingen voor de situaties waarin zich een calamiteit voordoet die de continuïteit van de dienstverlening bedreigt.	
				2.8.3	Het continuïteitsplan bevat een aantal alternatieve scenario's die in lijn zijn met de ernst van het incident en de impact daarvan.	
				2.8.4	Het continuïteitsplan beschrijft eenduidig de volgorde waarin onderdelen van de dienst worden hersteld alsmede alternatieve scenario's.	
				2.8.5	Er zijn testplannen opgesteld voor het testen van (onderdelen van) het continuïteitsplan. De testplannen zijn gericht op de afgesproken dienstenniveaus.	
				2.8.6	Periodiek wordt het continuïteitsplan getest in overeenstemming met de testplannen.	
				2.8.7	Testresultaten worden gedocumenteerd en gerapporteerd aan het management en alle belanghebbenden. Ze leiden als dit nodig is tot een actieplan.	
				2.8.8	Over het optreden van een calamiteit en het herstarten van de dienstverlening wordt met de klanten, die hierdoor worden geraakt, helder en tijdig gecommuniceerd.	
				2.8.9	Er zijn eenduidige richtlijnen voor de klanten hoe zij moeten handelen tijdens uitval van de dienstverlening.	
				2.8.10	Kritieke back-upmedia, documentatie en andere essentiële IT-hulpmiddelen zijn op een externe locatie opgeslagen.	
				2.8.11	Externe opslag van back-ups en overige gegevens vindt plaats conform het dataclassificatiebeleid (informatiebeveiligingsbeleid), alsmede de wet- en regelgeving die daarvoor van toepassing is.	
				2.8.12	De gegevens die extern zijn opgeslagen worden periodiek geïnventariseerd op actualiteit en beveiliging en er wordt vastgesteld of het herstel van gearchiveerde data mogelijk is met behulp van de aanwezige faciliteiten.	
				2.8.13	Iedere uitval van de dienstverlening wordt geregistreerd, geanalyseerd en door het management geëvalueerd.	
				2.8.14	Bij een calamiteit worden activiteiten conform het continuïteitsplan uitgevoerd of er wordt in overleg met en na akkoord van het management voor een alternatief scenario gekozen.	
2.9	Beheersing informatiebeveiliging (I) proces	Het management is verantwoordelijk voor de informatiebeveiliging. Het vertaalt de functionaliteitseisen uit de overeenkomst, de risico's en de relevante wet- en regelgeving in een informatiebeveiligingsplan. Kerndoel daarvan is het beschermen	De maatregelen bieden een redelijke mate van zekerheid dat de functionaliteitseisen uit de overeenkomst, de risico's en relevante wet- en regelgeving worden vertaald in een informatiebeveiligingsplan met als kerndoel het	2.9.1	De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatie gerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.	
				2.9.2	Het management is verantwoordelijk voor de informatiebeveiliging.	

# doelstelling	Onderwerp	Toelichting beheersdoelstelling	Beheersdoelstelling	# beheersmaatregel	Deze beheersmaatregelen zijn een baseline of eerste invulling.	Deze handreiking probeert de doelstellingen en maatregelen te verduidelijken nergens zijn opsommingen limitatief tenzij anders vermeld.
		aanpassen, inzien of verwijderen van gegevens. Dit vereist een voortdurend testen, monitoren en aanpassen van beveiligingsmaatregelen. Het beleid wordt ondersteund c.q. afgedwongen door de juiste beveiligingstechnieken te gebruiken. Tav (i) proces, (ii) Toegang, (iii) Generieke eisen voor ICT-Middelen, (iv) Monitoring.	van het ongeautoriseerd aanpassen, inzien of verwijderen van gegevens.	2.9.16	Afwijkingen en veiligheidslekken worden gesignaleerd en gerapporteerd aan het management.	
				2.9.17	Het niveau van informatiebeveiliging wordt periodiek getest op veiligheidslekken. De resultaten hiervan worden gerapporteerd aan het management.	
				2.9.18	Periodiek worden testen uitgevoerd om beveiliging tegen ongeautoriseerde toegang te voorkomen, onderdeel van deze procedure zijn extern uitgevoerde penetratietesten.	
				2.9.19	Vulnerability assessments (security scans) worden procesmatig en procedureel minimaal dagelijks uitgevoerd op de ICT-componenten van de webapplicatie (scope).	De vulnerabilitycheck moet een minimale frequentie van 24 uur worden uitgevoerd. Met name het oppakken van nieuwe vulnerability is relevant. Dit is een van de belangrijke speerpunten van het keurmerk. De aard en impact van de vulnerability bepalen de snelheid waarmee een oplossing moet zijn geïmplementeerd. Streven moet zijn om deze binnen 24 uur gesignaleerd te hebben en hiervoor een oplossing aan te bieden.
				2.9.20	Karakteristieken van potentiële veiligheidsincidenten zijn gedefinieerd en gecommuniceerd naar de medewerkers.	
				2.9.21	Een gesignaleerd potentieel veiligheidsincident wordt geclassificeerd en op het juiste niveau binnen de organisatie afgehandeld.	Voorbeeld is een incidentenrapportage.
				2.9.22	Fysieke toegang tot de faciliteiten waar het geautomatiseerde systeem en de vertrouwelijke gegevens zich bevinden, is slechts voorbehouden tot geautoriseerde personen om aan de verplichtingen te voldoen en afspraken na te komen voor zover deze betrekking hebben op beveiliging, beschikbaarheid, integriteit, privacy of vertrouwelijkheid.	
2.10	Service desk	Een goed functionerende service desk is essentieel voor de dienstverlening. De service desk is het aanspreekpunt voor de gebruiker en zorgt voor de registratie, bewaking van de voortgang en terugkoppeling aan de gebruiker van de meldingen, incidenten, verzoeken en informatievragen. Het service desk proces moet worden ondersteund door een adequaat systeem met bijbehorende procedures. Escalatie en het aanbieden van workarounds vindt plaats volgens de overeenkomst. Het afsluiten van een 'incident', om er zeker van te zijn dat de gebruiker is geïnformeerd en oplossingen zijn geregistreerd, is een integraal onderdeel van het service desk proces. Het management moet periodiek worden geïnformeerd over de kwaliteit van het service desk proces en de gerapporteerde incidenten.	De maatregelen bieden een redelijke mate van zekerheid dat de dienst aanbieder zorgt voor de registratie, bewaking van de voortgang en terugkoppeling aan de gebruiker van de meldingen, incidenten, verzoeken en informatieaanvragen.	2.10.1	De leverancier zorgt er voor tenminste 95% van de meldingen, incidenten, verzoeken en informatievragen binnen voorwaarden en op de website vermelde termijn in behandeling zijn genomen.	De leverancier moet op eigen wijze invulling geven aan deze doelstelling. Het gaat erom dat klanten een passend antwoord krijgen op de gestelde vragen binnen een redelijke termijn bij een grote leverancier betekent dit een volledig ingericht service desk proces zoals beschreven in de toelichting op de controle doelstelling. Bij een kleinere leverancier kan worden volstaan met het aanwijzen van verantwoordelijke personen.
				2.10.2	Klanten hebben de mogelijkheid om feedback te geven over de kwaliteit van het ontvangen antwoord.	Deze kwaliteit kan op diverse wijze worden gemeten en moet passen bij de organisatiestructuur. Dit kan middels rechtstreeks de klant te vragen naar feedback over het afhandelen van een vraag of klacht tot klanttevredenheidsverzoeken. De nadruk moet liggen op de opvolging van de uitkomsten.
				2.10.3	Er zijn monitoring- en escalatieprocedures opgezet, gebaseerd op het in de overeenkomst afgesproken dienstniveau, die classificatie en prioritering van elk gerapporteerd incident mogelijk maken.	
				2.10.4	Incidenten worden systematisch geanalyseerd om zodoende eventuele problemen te kunnen signaleren.	
				2.10.5	Problemen worden geprioriteerd en toegewezen aan verantwoordelijke functionarissen op basis van vastgelegde procedures.	
				2.10.6	Incidenten worden pas afgesloten nadat de stappen die tot een oplossing leiden zijn geregistreerd en belanghebbenden akkoord zijn met de voorgestelde oplossing.	
				2.10.7	De oplossing van incidenten wordt geregistreerd en is toegankelijk voor iedereen die verantwoordelijk is voor het opvolgen van meldingen, incidenten, verzoeken en informatievragen.	Zie toelichting 2.10.2
				2.10.8	Periodiek wordt vastgesteld of binnen gestelde tijd opvolging wordt gegeven aan meldingen, incidenten, verzoeken en informatievragen.	

# doelstelling	Onderwerp	Toelichting beheersdoelstelling	Beheersdoelstelling	# beheersmaatregel	Deze beheersmaatregelen zijn een baseline of eerste invulling.	Deze handreiking probeert de doelstellingen en maatregelen te verduidelijken nergens zijn opsommingen limitatief tenzij anders vermeld.
2.11	Configuratiebeheer	Voor het beheersen van de configuratie van de hardware en de software moet de dienstaanbieder voortdurend beschikken over een bijgewerkte bibliotheek (repository). Het configuratiebeheer omvat het initieel verzamelen en onderhouden van configuratiegegevens, het implementeren van baselines[1] en het controleren van de toereikendheid van de repository. Effectief configuratiebeheer leidt tot hogere beschikbaarheid, vermindert verstoringen in het werkproces en maakt het herstel eenvoudiger.	De maatregelen bieden een redelijke mate van zekerheid dat effectief configuratiebeheer leidt tot hogere beschikbaarheid en vermindering van storingen in het werkproces en in geval storingen optreden voor een optimaal en kort herstel.	2.11.1 2.11.2 2.11.3 2.11.4	De dienstaanbieder beschikt, in de vorm van een repository, over een gestructureerde vastlegging van configuratie-items, hun kenmerken en onderlinge relaties en de daaraan gerelateerde documentatie. Voor ieder systeem of dienst is een baseline ingesteld. Het configuratiebeheer wordt ondersteund door daartoe opgestelde procedures. Het configuratiebeheer is onderdeel van het beheer van de wijzigingen en het beheer van de incidenten en problemen. Periodiek wordt de toereikendheid van gegevens in de repository vastgesteld.	Opname in het beveiligingsplan.
2.12	Gegevensbeheer	Er moeten effectieve procedures in werking zijn voor het beheer over de mediabibliotheek, voor backup en recovery van gegevens en voor het veilig vernietigen van gegevens	De maatregelen bieden een redelijke mate van zekerheid dat effectieve procedures in werking zijn voor het beheer over de mediabibliotheek, voor backup en recovery van gegevens en voor het veilig vernietigen van gegevens.	2.12.1 2.12.2 2.12.3 2.12.4 2.12.5 2.12.6 2.12.7 2.12.8 2.12.9	De dienstaanbieder heeft voor het bewaren, ter beschikking stellen en archiveren van gegevens richtlijnen opgesteld die passen binnen de overeenkomst. De dienstaanbieder onderhoudt een systeem waaruit de opslagplaats van de bewaarde en gearhiveerde gegevens van klanten eenduidig blijkt. De dienstaanbieder implementeert en onderhoudt organisatorische en technologische maatregelen om te garanderen dat de voortdurende integriteit en toegankelijkheid van de data zijn gewaarborgd en waarmee hij ook voldoet aan de eisen uit de overeenkomst en de relevante wet- en regelgeving. De dienstaanbieder treft maatregelen die de gegevens van klanten beschermen als zij worden getransporteerd via datacommunicatie alsmede bij het buiten werking stellen of vernietigen van hardware en media. Deze maatregelen, die door het management zijn geaccordeerd, worden regelmatig getest. In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.	Hier moet gebruik worden gemaakt van SSL- certificaten of gelijkwaardige beveiligingsmechanisme. " Aanbevolen wordt ook het gebruik van SPF en DKIM technieken ter voorkomen van valse e-mails. Het configuratiebeheer is procesmatig ingericht en zorgt ervoor dat slechts operationele websites in gebruik zijn. Neem websites conform wijzigingsbeheerprocessen in productie. Voer periodiek controles uit of de operationele websites nog worden gebruikt of informatie bevat en die kan worden verwijderd. Houd een overzichtslijst bij van de websites die operationeel zijn inclusief de daarbij vermelde eigenaren.
2.13	Monitoren van de dienstverlening	Het monitoren is gericht op de dienstverlening aan de klanten, de interne beheersing van het dienstverleningsproces door de medewerkers, de informatiebeveiliging en het voldoen aan relevante wet- en regelgeving. Bij de keuze van de relevante indicatoren wordt met deze vier aandachtsgebieden rekening gehouden. Self assessment en de review of audit door derden zijn onderdeel van het monitoren.	Maatregelen bieden een redelijke mate van zekerheid dat het monitoren is gericht op de dienstverlening aan de klanten, de interne beheersing van het dienstverleningsproces door de medewerkers, de informatiebeveiliging en het voldoen aan relevante wet- en regelgeving.	2.13.1 2.13.2 2.13.3	De dienstaanbieder heeft een passende methode opgesteld en ingevoerd voor het monitoren van de dienstverlening, de interne beheersing van het dienstverleningsproces, de informatiebeveiliging en het voldoen aan wet- en regelgeving. De prestatie-indicatoren zijn gebaseerd op de overeenkomst en zo gekozen dat zij een goed beeld geven van de dienstverlening. De dienstaanbieder onderzoekt periodiek de klantwensen en de ontwikkelingen in de technologie en stelt vast of aanpassing van de dienstverlening nodig is.	

# doelstelling	Onderwerp	Toelichting beheersdoelstelling	Beheersdoelstelling	# beheersmaatregel	Deze beheersmaatregelen zijn een baseline of eerste invulling.	Deze handreiking probeert de doelstellingen en maatregelen te verduidelijken nergens zijn opsommingen limitatief tenzij anders vermeld.
				2.13.4	Het management heeft een actieve opstelling als het gaat om het volgen van de ontwikkelingen in relevante wet- en regelgeving. Het management zorgt voor het integreren van de relevante wet- en regelgeving in het dienstverleningsproces en verankering daarvan in beleid, maatregelen en procedures.	
				2.13.5	Alle significante afwijkingen worden op zo'n wijze geanalyseerd dat de onderliggende oorzaak eenduidig wordt vastgesteld. Waar nodig vindt escalatie naar de klanten en derden plaats. Het management treft tijdig corrigerende maatregelen om afwijkingen als gevolg van de gevonden oorzaak in de toekomst te voorkomen.	
3.1	Netwerkbeveiliging	De dienstaanbieder moet de beveiliging van informatie in netwerken en de bescherming van de ondersteunende infrastructuur zodanig handhaven, dat de beschikbaarheid van de webapplicatie en de vertrouwelijkheid van het netwerkverkeer en de opgeslagen data worden gewaarborgd. Aangezien het netwerk een generiek 'onderstef' is voor alle mogelijke toepassingen, zijn veel maatregelen niet specifiek gericht op de beveiliging van webapplicaties, maar op de algemene beveiliging van de infrastructuur rondom de webapplicatie. De normen richten zich op het beveiligen van de informatiestromen op het transport- en netwerkniveau.	De maatregelen bieden een redelijke mate van zekerheid dat de beveiliging van informatie in netwerken en de bescherming van de ondersteunende infrastructuur zodanig is, dat de beschikbaarheid van de webapplicatie en de vertrouwelijkheid van het netwerkverkeer en de opgeslagen data worden gewaarborgd.	3.1.1	De organisatie heeft de actuele documentatie van het ICT-landschap vastgelegd, met daarin de bedrijfsprocessen, de technische componenten, hun onderlinge samenhang en de ICT-beveiligingsarchitectuur.	
				3.1.2	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.	
				3.1.3	De opzet van het netwerk garandeert dat alle gebruikers langs dezelfde netwerkpaden toegang krijgen tot webapplicaties, ongeacht hun fysieke locatie.	
				3.1.4	Het netwerk is gescheiden in logische en fysieke domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd is.	In de situatie dat een server en het bedrijfsnetwerk via dezelfde internetverbinding aan internet zijn verbonden is een DMZ een eis.
				3.1.5	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van protectie- en detectiemechanismen. Alle kwetsbaarheden zoals genoemd in de top 10 OWASP moeten minimaal zijn afgedekt.	Oude kwetsbaarheden die niet meer zijn opgenomen in OWASP 10 moeten ook blijvend bescherming krijgen.
				3.1.6	Het netwerk is gebaseerd op betrouwbare netwerkcomponenten, ondersteund door redundantie.	
				3.1.7	Bij toegang tot een site/pagina wordt verzekerd dat een gebruikt certificaat valide is en dus niet verlopen of ingetrokken.	
				3.1.8	Alle backend-verbindingen die publieke toegankelijk kunnen zijn, maken gebruik van een veilige verbinding en encryptie.	
				3.1.9	De webapplicatie communiceert alleen met onder- en achterliggende systemen op basis van statisch geconfigureerde (geparametriseerde) query's en commando's en uitsluitend ten behoeve van de noodzakelijke functionaliteit.	
3.2	Platformbeveiliging	De dienstaanbieder moet de beveiliging voor platformen/besturingssystemen zodanig ontwerpen, inrichten en handhaven, dat deze systemen beter bestand zijn tegen aanvallen van kwaadwillenden. De normen zien op maatregelen om platformbeveiliging voor webapplicaties in te richten. Deze maatregelen hebben allemaal als doel het besturingssysteem te 'hardenen'. 'Hardening' houdt in dat je het besturingssysteem zo inricht, dat het beter bestand is tegen aanvallen van kwaadwillenden. De technische stappen die nodig zijn om een besturingssysteem te hardenen verschillen per type besturingssysteem.	De maatregelen bieden een redelijke mate van zekerheid dat de beveiliging voor platformen/besturingssystemen zodanig zijn ontworpen, ingericht en worden gehandhaafd, dat deze systemen bestand zijn tegen aanvallen van kwaadwillenden.	3.2.1	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.	Ter voorkoming van het versturen van frauduleuze facturen moet gebruik worden gemaakt van de techniek DNSSEC naast het gebruik van SSL - certificaten of een gelijkwaardige beveiligingsmechanisme. "
				3.2.2	Door middel van hardening (op netwerk-, OS- en applicatieniveau) is de gebruikte techniek beveiligd tegen manipulatie en wordt voorkomen dat informatie over beveiligingsinstellingen onnodig wordt verschaft.	Hierbij moet gedacht voor het OS-, en applicatieniveau: patches, applicatie ondersteuning. Op netwerkniveau: periodieke vulnerabilitytest met gedocumenteerde actieopvolging .
				3.2.3	Kritieke delen van systemen (bijv. subprocessen, bestanden) worden beschermd door isolatie van overige delen.	
				3.2.4	Ieder platform filtert het netwerkverkeer met behulp van een lokale firewall, zodat het netwerkverkeer beperkt is tot de bekende, toegestane communicatiestromen.	
3.3	Applicatiebeveiliging	De dienstaanbieder moet waarborgen dat beveiliging wordt ingebouwd in webapplicaties. De aandacht richt zich op de kwetsbaarheden die in een webapplicatie aanwezig kunnen zijn. Het gaat hier om de wijze waarop deze kwetsbaarheden die in een webapplicatie aanwezig kunnen zijn. Het gaat hier om de wijze waarop deze kwetsbaarheden worden voorkomen en waarop de schade door misbruik van de kwetsbaarheden wordt beperkt.	De maatregelen bieden een redelijke mate van zekerheid dat de webapplicaties zijn beveiligd tegen kwetsbaarheden die in webapplicatie aanwezig kunnen zijn.	3.3.1	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.	
				3.3.2	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.	
				3.3.3	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.	
				3.3.4	Opbouwen van SQL statements gebeurt op een gestandaardiseerde manier waarbij SQL-injection wordt voorkomen.	
				3.3.5	De webapplicatie beperkt de informatie in de uitvoer tot de informatie die voor het functioneren van belang is.	Commentaarregels worden indien niet van toepassing meer uit de scripts (code) verwijderd.

# doelstelling	Onderwerp	Toelichting beheersdoelstelling	Beheersdoelstelling	# beheersmaatregel	Deze beheersmaatregelen zijn een baseline of eerste invulling.	Deze handreiking probeert de doelstellingen en maatregelen te verduidelijken nergens zijn opsommingen limitatief tenzij anders vermeld.
				3.3.6	Directory-listings zijn uitgeschakeld.	
				3.3.7	Op regelmatige basis wordt het niveau van informatiebeveiliging getest op veiligheidslekken en de resultaten hiervan worden gerapporteerd aan het management.	
				3.3.8	Afwijkingen en veiligheidslekken worden gesignaleerd en gerapporteerd aan het management.	
				3.3.9	De webserver is ingericht volgens een configuratie-baseline.	
				3.3.10	Er zijn maatregelen getroffen om te voorkomen dat cross-site scripting kan worden toegepast.	
				3.3.11	Er zijn maatregelen getroffen om te voorkomen dat er via aanpassing van de URL ongeautoriseerde toegang kan worden verkregen.	
3.4	Sessiebeheer	De dienst aanbieder moet waarborgen dat bij het beëindigen van de sessie de toegang tot de informatie wordt geblokkeerd, totdat de gebruiker opnieuw geïdentificeerd en geauthenticeerd is.	De maatregelen bieden een redelijke mate van zekerheid dat bij het beëindigen van de sessie de toegang tot de informatie wordt geblokkeerd, totdat de gebruiker opnieuw geïdentificeerd en geauthenticeerd is.	3.4.1	De (gebruikers) sessie die ontstaat na het succesvol aanmelden van een gebruiker, kent een beperkte levensduur en de gebruiker kan deze sessie zelf beëindigen.	
				3.4.2	Bij het beëindigen van de sessie wordt de toegang tot de informatie geblokkeerd.	
3.5	Vertrouwelijkheid en onweerlegbaarheid	De dienst aanbieder moet ervoor zorgen dat geen informatie wordt gelekt en dat onweerlegbaarheid wordt ondersteund. Gegevens worden op basis van gangbare encryptiemethoden versleuteld verzonden en opgeslagen.	De maatregelen bieden een redelijke mate van zekerheid dat geen informatie wordt gelekt en dat onweerlegbaarheid wordt ondersteund.	3.5.1	De dienst aanbieder treft maatregelen om te voorkomen dat sleutels niet veilig worden verzonden of onbeveiligd op de servers worden opgeslagen.	
				3.5.2	De dienst aanbieder gebruikt voor de versleuteling van de communicatie tussen browser en servers gangbare encryptietechnieken.	
				3.5.3	De dienst aanbieder zorgt voor een zodanige beveiliging, dat de data tegen mogelijke bedreigingen zijn beschermd.	
3.6	Monitoring, auditing en alerting	De dienst aanbieder moet ervoor zorgen, dat een omgeving ontstaat van nauw verwante (netwerk) componenten die moeiteloos met elkaar kunnen communiceren. Met de invoer van elke nieuwe beveiligingscomponent moet de vraag worden gesteld hoe deze component binnen de bestaande omgeving kan worden geïntegreerd. Belangrijk is vast te stellen welke services de omgeving van de component zal afnemen en op welke manier dat gebeurt (actief of passief, welke protocollen). De vereisten die uit deze overwegingen naar voren komen dienen vervolgens als input voor een productselectie. Door bij elke nieuwe of te vervangen beveiligingscomponent deze vereisten in ogenschouw te nemen, ontstaat een omgeving van nauw verwante componenten die moeiteloos met elkaar kunnen communiceren.	De maatregelen bieden een redelijke mate van zekerheid dat een omgeving ontstaat van nauw verwante (netwerk) componenten die moeiteloos met elkaar kunnen communiceren.	3.6.1	De dienst aanbieder heeft afdoende procedures en technieken geïmplementeerd om (slechts) geautoriseerde toegang mogelijk te maken en netwerken te identificeren.	
				3.6.2	Logging is zodanig geregeld dat deze slechts toegankelijk is voor de beheerder.	
				3.6.3	Waar nodig zijn correlaties aangebracht.	
				3.6.4	Systeemklokken worden gesynchroniseerd.	
				3.6.5	Bewaartermijnen voor logging zijn vastgesteld.	
				3.6.6	Logging is beveiligd tegen achteraf wijzigen.	
				3.6.7	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.	Hieronder wordt ook verstaan het aantoonbaar opvolging geven aan verbeteringen. Voor nadere detaillering geeft C.06 ICT-Beveiligingsrichtlijnen voor Webapplicaties van het NCS invulling.
				3.6.8	Maatregelen met betrekking tot informatiebeveiliging worden actief gemonitord op adequate werking en gelogd	
				3.6.8		
3.7	Logging	Logging dient er toe dat gebruikers weten wie wanneer welke transactie of mutatie heeft vastgelegd of gemuteerd om zekerheid te verkrijgen wie wanneer welke activiteit heeft gedaan om tot de gewenste verantwoording te komen.	De maatregelen bieden een redelijke mate van zekerheid dat de gebruiker van alle transacties die onderdeel zijn van een verantwoording, kan herleiden door wie en wanneer deze zijn uitgevoerd.	3.7.1	Bij de logging worden de identiteit van de gebruiker, de datum, het tijdstip en de gebruikte functionaliteit geregistreerd.	
				3.7.2	Transacties die automatisch zijn gegenereerd, kan de gebruiker herleiden naar herkomst en type.	
				3.7.3	Elke relevante wijziging van belangrijke vaste gegevens wordt gelogd.	

# doelstelling	Onderwerp	Doelstelling	Beheersdoelstelling	# beheersmaatregel	Deze beheersmaatregelen zijn een baseline of eerste invulling.	Deze handreiking probeert de doelstellingen en maatregelen te verduidelijken nergens zijn opsommingen limitatief tenzij anders vermeld.
4.1	Scheiding van klantomgevingen	Omdat er sprake is van een concentratie van veel verschillende administraties is het belangrijk dat de dienst aanbieder deze van elkaar scheidt. De gebruiker mag alleen toegang krijgen tot de administraties waarvan hij eigenaar is of waartoe hij door of namens de eigenaar is geautoriseerd.	De maatregelen bieden een redelijke mate van zekerheid dat een gebruiker alleen toegang krijgt tot de administraties waarvan hij eigenaar is of waartoe hij door of namens de eigenaar is geautoriseerd.	4.1.1 4.1.2 4.1.3 4.1.4 4.1.5	De verschillende administraties zijn voldoende logisch en/of fysiek van elkaar gescheiden. De dienst aanbieder monitort voortdurend of de scheiding tussen de administraties daadwerkelijk geborgd is. De gebruiker heeft alleen toegang tot zijn eigen administraties. Daartoe zijn passende technische beheersmaatregelen getroffen. De dienst aanbieder regelt dat bij signalering van een schending van de toegangsrechten passende maatregelen worden genomen. Als het mogelijk is dat meer gebruiksessies tegelijkertijd plaatsvinden, dan zijn er maatregelen getroffen om de integriteit van de gegevensverwerking, bijvoorbeeld als gevolg van het gelijktijdig aanpassen van dezelfde data, te waarborgen.	
4.2	Logische toegangsbeveiliging en autorisatiebeheer i) identificatie en authenticatie	Bij de toegang tot de administraties moeten identificatie en authenticatie op een adequate manier plaatsvinden. Ook moet de dienst aanbieder ervoor zorgen dat er in de applicatie toereikende functiescheidingen kunnen worden gerealiseerd. (i) Identificatie en authenticatie.	De maatregelen bieden een redelijke mate van zekerheid dat de identiteit en authenticiteit van de gebruiker bij inloggen wordt vastgesteld o.a. teneinde toereikende functiescheidingen te realiseren. (i) Identificatie en authenticatie.	4.2.1 4.2.2 4.2.3 4.2.4 4.2.5 4.2.6 4.2.7 4.2.8 4.2.9 4.2.10 4.2.11 4.2.12 4.2.13	Gebruiker-ID's zijn uniek. Default gebruiker-ID's voor de applicatie c.q. de dienst aanbieder zijn adequaat beveiligd. Wachtwoorden worden bij de invoer niet leesbaar op het scherm getoond. Wachtwoorden worden zodanig opgeslagen dat het originele wachtwoord niet kan worden achterhaald. Wachtwoorden zijn gebonden aan restricties, zoals minimale lengte en periodieke wijziging, die door de applicatie worden bewaakt. Een leeg wachtwoord is niet mogelijk. De gebruiker kan zijn eigen wachtwoord wijzigen en krijgt hiervan bevestiging op een vooraf ingesteld medium zoals een email en sms. Het wijzigen keuze voor het vooraf ingesteld medium wordt op het voorgaande medium bevestigd. Bij gebruik van andere authenticatiemethoden dan wachtwoorden moet ten minste een vergelijkbaar niveau van identificatie en authenticatie worden bereikt als bij het gebruik van wachtwoorden het geval is. Het aantal inlogpogingen is gelimiteerd. Bij het overschrijden van de limiet, wordt het gebruiker-ID geblokkeerd. Bij een succesvolle inlogpoging krijgt de gebruiker informatie over de datum en de tijd van de vorige aanmelding. Er vindt een registratie plaats van de laatste inlogdatum, zodat de applicatiebeheerder kan signaleren welke gebruiker-ID's geen gebruik van de applicatie maken en deze kan blokkeren. Als gebruik wordt gemaakt van externe login-faciliteiten dan komt de dienst aanbieder in het kader van zijn verantwoordelijkheid voor de authenticatie met de externe partner overeen wat de inlogvereisten zijn. Wachtwoorden worden alleen verstrekt via een beveiligd medium. Bij meerdere gebruikers dwingt de applicatie op een adequate wijze de controletechnische functiescheidingen van de gebruikersorganisatie af. Er zijn autorisatiemogelijkheden voor: - de applicatie als geheel; - specifieke modules of onderdelen; - specifieke functies; - specifieke gegevens en/of - het aanmaken, lezen, wijzigen en verwijderen van gegevens. Het is mogelijk de toegang tot de gehele applicatie af te schermen voor bepaalde gebruikers.	Als het ontvangstmiddel wijzigt dan moet hier melding van gemaakt worden op het oude ingestelde medium. Openbare e-mailadressen worden niet als veilig beschouwd. Nieuwe wachtwoorden mogen niet worden verstuurd via e-mail. Indien deze maatregel niet van toepassing is vanwege de reden dat er maar een gebruiker met mutatierechten toegang heeft tot de applicatie. Moet vastgesteld worden dat voor de gehele functionaliteit maar een gebruiker met mutatierechten toegang kan krijgen tot de applicatie. Uiteraard moet de authenticiteit worden vastgesteld van deze unieke gebruiker. Leesrechten voor een tweede gebruiker veronderstelt multilogin. Indien deze maatregel niet van toepassing is vanwege de reden dat er maar een gebruiker met mutatierechten toegang heeft tot de applicatie. Moet vastgesteld worden dat voor de gehele functionaliteit maar een gebruiker met mutatierechten
	Logische toegangsbeveiliging en autorisatiebeheer ii) Autorisatiebeheer	Bij de toegang tot de administraties moet de identiteit en authenticiteit ondubbelzinnig van de gebruiker worden vastgesteld o.a. teneinde toereikende functiescheidingen te realiseren. (ii) Autorisatiebeheer	De maatregelen bieden een redelijk in redelijke mate van zekerheid dat de identiteit en authenticiteit ondubbelzinnig van de gebruiker bij inloggen wordt vastgesteld o.a. teneinde toereikende functiescheidingen te realiseren. (ii) Autorisatiebeheer.			

# doelstelling	Onderwerp	Doelstelling	Beheersdoelstelling	# beheersmaatregel	Deze beheersmaatregelen zijn een baseline of eerste invulling.	Deze handreiking probeert de doelstellingen en maatregelen te verduidelijken nergens zijn opsommingen limitatief tenzij anders vermeld.
				4.2.14	Bij meerdere gebruikers is de gebruikersorganisatie in staat de toegekende autorisaties te beoordelen. De toegekende autorisaties kunnen naar verschillende gezichtspunten worden gerangschikt, zoals per gebruiker, gebruikersgroep of functie.	Indien deze maatregel niet van toepassing is vanwege de reden dat er maar een gebruiker met mutatierechten toegang heeft tot de applicatie. Moet vastgesteld worden dat voor de gehele functionaliteit maar een gebruiker toegang kan krijgen tot de applicatie. Uiteraard moet de authenticiteit worden vastgesteld van deze unieke gebruiker.
				4.2.15	Het invoeren, wijzigen en verwijderen van autorisatiegegevens heeft geen invloed op de beoogde operationele werkzaamheden.	
				4.2.16	Na verloop van tijd worden inactieve gebruikers automatisch uitgelogd.	
4.3	Kritieke functies	Voor de gebruikers van administraties is het van essentieel belang dat de kritieke functies voor hun eigen administratie goed geregeld zijn. Het moet mogelijk zijn om kritieke functies aan specifieke functionarissen toe te wijzen.	De maatregelen bieden een redelijke mate van zekerheid dat kritieke functies voor de gebruikersadministratie goed geregeld zijn doordat kritieke functies aan specifieke functionarissen zijn toe te wijzen.	4.3.1	Bij meerdere gebruikers is het mogelijk om de beheer functionaliteit toe te wijzen aan een specifiek gebruikersprofiel. In dat geval wordt gesproken van een superuser.	Indien deze maatregel niet van toepassing is vanwege de reden dat er maar een gebruiker met mutatierechten toegang heeft tot de applicatie. Moet vastgesteld worden dat voor de gehele functionaliteit maar een gebruiker toegang kan krijgen tot de applicatie. Uiteraard moet de authenticiteit worden vastgesteld van deze unieke gebruiker.
				4.3.2	De superuser kan, binnen de mogelijkheden van de afgenomen dienst, functionaliteiten activeren of deactiveren.	Indien deze maatregel niet van toepassing is vanwege de reden dat er maar een gebruiker met mutatierechten toegang heeft tot de applicatie. Moet vastgesteld worden dat voor de gehele functionaliteit maar een gebruiker toegang kan krijgen tot de applicatie. Uiteraard moet de authenticiteit worden vastgesteld van deze unieke gebruiker.
				4.3.3	De superuser kan gebruiker-ID's aanmaken, wijzigen en verwijderen. Het autorisatiebeheer van de desbetreffende administratie berust bij hem.	
				4.3.4	Het inregelen van de administratie is voorbehouden aan of gedelegeerd door de superuser.	
				4.3.5	De superuser kan een begrijpelijk rapport genereren dat inzicht geeft in de inrichting van de administratie en de tijlrijn van opeenvolgende wijzigingen.	
				4.3.6	Binnen de cloudoplossing wordt systematisch gecontroleerd of het verwijderen van data in strijd is met de wettelijke zevenjaars bewaartermijn en/of een soepele verwerking van de administratie belemmert. De gebruiker krijgt informatie over het mogelijke probleem en wordt expliciet om instemming en acceptatie van de gevolgen gevraagd.	
4.4	Gebruikersondersteuning	Het is voor gebruikers belangrijk dat zij bij het werken met de applicatie op een goede manier worden ondersteund.	De maatregelen bieden een redelijke mate van zekerheid dat gebruikers bij het werken met de applicatie op een goede manier worden ondersteund.	4.3.7	Een functionaliteit voor het opschonen van de logging is niet aanwezig.	
				4.4.1	De gebruikersondersteuning is inzichtelijk, up-to-date en eenvoudig toegankelijk.	
				4.4.2	Foutmeldingen omschrijven duidelijk de foutsituatie en bieden een mogelijke oplossing voor het probleem. Informatie over de technische werking van de applicatie blijft daarbij achterwege.	
4.5	Integriteit van de klantomgeving	Het verwerken van transacties kan alleen als er sprake is van een logisch en consistent geheel. Als dat niet het geval is en een transactie dus niet kan worden afgerond, dan blijkt dit uit de status van de transactie. De applicatie moet de gebruiker in staat stellen om de consistentie van zijn administratie zelfstandig vast te stellen.	De maatregelen bieden een redelijke mate van zekerheid dat de gebruiker de consistentie van zijn administratie zelfstandig kan vaststellen; transacties kunnen alleen verwerkt worden als sprake is van een logisch en consistent geheel.	4.5.1	Transacties en stamgegevens zijn uniek identificeerbaar.	
				4.5.2	De applicatie valideert de invoer van transacties door middel van logische invoercontroles.	
				4.5.3	Onafhankelijk van de wijze van invoer is op iedere verwerking van een transactie dezelfde set van controlemaatregelen van toepassing.	
				4.5.4	Transacties waarvan de invoer abrupt is onderbroken worden nadien hersteld of opnieuw ter verwerking aangeboden. Lukt dat niet, dan is voor de gebruiker duidelijk te zien dat de desbetreffende transactie niet is verwerkt.	
				4.5.5	De gebruiker kan per transactie, per dag of per boekjaar de integriteit van de administratie vaststellen. Afwijkingen zijn te herleiden naar individuele transacties.	
				4.5.6	Stamgegevens die zijn gebruikt in een transactie kunnen niet worden verwijderd. Ook kunnen geen elementen worden gewijzigd die invloed hebben op gedane transacties.	

# doelstelling	Onderwerp	Doelstelling	Beheersdoelstelling	# beheersmaatregel	Deze beheersmaatregelen zijn een baseline of eerste invulling.	Deze handreiking probeert de doelstellingen en maatregelen te verduidelijken nergens zijn opsommingen limitatief tenzij anders vermeld.
4.6	Koppeling en integratie met externe systemen	Het koppelen van of, anders gezegd, het aanbrengen van interfaces tussen de eigen applicatie en die van derden wordt steeds belangrijker. Het moet voor de gebruiker, op welke manier het koppelen ook plaatsvindt, te allen tijde duidelijk zijn dat de gegevensoverdracht juist en volledig gebeurt. Als fouten of verstoringen optreden, moet dat helder zijn en de integriteit van de administratie moet gewaarborgd blijven. Ook is het van belang dat ongeacht de wijze van invoer eenzelfde validatie van gegevens plaatsvindt.	De maatregelen bieden een redelijke mate van zekerheid dat te allen tijde voor de gebruiker duidelijk is of de gegevensoverdracht juist en volledig is gebeurt bij het koppelen van applicaties.	4.6.1	Voor ontwikkelaars van externe systemen die willen en mogen koppelen met de desbetreffende applicatie is zowel technische documentatie als gebruikersdocumentatie beschikbaar.	
				4.6.2	Bij het importeren van gegevens vindt een controle plaats op de vulling en de opmaak van verplichte invoervelden.	
				4.6.3	De gebruiker kan vaststellen dat de im- en export van gegevens juist, volledig en tijdig is gebeurd en of er correcties moeten worden aangebracht.	
				4.6.4	Bij de importfunctie worden dezelfde controles uitgevoerd als bij het invoeren via de gebruikersinterface.	
				4.6.5	Als de gegevensoverdracht door een storing wordt onderbroken, is de consistentie van de database gewaarborgd. De gebruiker krijgt een gespecificeerd overzicht van de eventuele fouten die door de storing zijn ontstaan.	
4.7	Logging en audit trail	Van alle transacties die onderdeel zijn van een verantwoording in een administratie moet de gebruiker kunnen herleiden door wie, wanneer, hoe en op basis waarvan ze zijn uitgevoerd. Adequate logging en audit trail, die de gebruiker kan raadplegen, zijn nodig. De dienstaanbieder is vrij in de keuze van de technische oplossing om aan deze voorwaarden tegemoet te komen.	De maatregelen bieden een redelijke mate van zekerheid dat de gebruiker, van alle transacties die onderdeel zijn van een verantwoording, kan herleiden door wie, wanneer, hoe en op basis waarvan deze zijn uitgevoerd.	4.6.6	De gebruiker kan exporteren naar gangbare formaten.	Het verwijderen van een loonrun behoort tot de relevante vaste gegevens.
				4.7.1	Elke wijziging van relevante vaste gegevens wordt gelogd.	
				4.7.2	Van transacties die onderdeel zijn van een verantwoording wordt vastgelegd door wie, wanneer, hoe en op basis waarvan deze is geregistreerd (audit trail). Wijzigingen die van invloed zijn op de verantwoording zijn traceerbaar. Indien een transactie invloed heeft op een verantwoording wordt de transactie definitief verondersteld.	
				4.7.3	Per administratie is inzicht in alle transacties, logging en audit trail.	
				4.7.4	Bij de logging worden de identiteit van de gebruiker, de datum, het tijdstip en de gebruikte functionaliteit geregistreerd.	
				4.7.5	Transacties die automatisch zijn gegenereerd, kan de gebruiker herleiden naar herkomst en type.	
				4.7.6	De gebruiker kan elke transactie eenvoudig en eenduidig herleiden naar het desbetreffende brondocument.	
				4.8.1	Het rapport vermeldt welke gegevens het bevat en waar die gegevens hun oorsprong vinden.	
				4.8.2	Het rapport is voorzien van: > titel of naam van het rapport > naam of nummer van de administratie > datum waarop het rapport is samengesteld > paginanummers (pagina x van y).	
				4.8.3	De velden in het rapport hebben duidelijke kopteksten.	
4.8.4	Als bij het samenstellen van het rapport dataselecties zijn gemaakt, moet het rapport de desbetreffende selectiecriteria vermelden.					
4.8.5	De gegevens in het rapport zijn volledig leesbaar. Er komen in het rapport bijvoorbeeld geen afgebroken gegevens of halve kolommen voor.					
4.8.6	De tellingen in het rapport zijn juist.					
4.8.7	Het is voor de gebruiker niet mogelijk om originele rapportstandaarden voor standaardrapportages aan te passen. Het aanpassen van overige rapporten is alleen toegestaan aan gebruikers die daarvoor geautoriseerd zijn.					
4.8.8	Als bij rapporten een drill-down mogelijk is, dan worden de onderliggende data juist en volledig weergegeven.					
4.8.9	De gebruiker kan de rapporten naar gangbare formaten exporteren.					

# doelstelling	Onderwerp	Doelstelling	Beheersdoelstelling	# beheersmaatregel	Deze beheersmaatregelen zijn een baseline of eerste invulling.	Deze handreiking probeert de doelstellingen en maatregelen te verduidelijken nergens zijn opsommingen limitatief tenzij anders vermeld.
5.1	Loonadministratie – basis	De applicatie moet de juistheid van de loonadministratie ondersteunen.	De maatregelen bieden een redelijke mate van zekerheid dat de applicatie de juistheid en volledigheid van de loonadministratie ondersteunt.	5.1.1	De applicatie bevat maatregelen die de interne consistentie tussen de loonaangifte, pensioenaangifte, loonjournaalposten, betaalbestanden en rapportages ondersteunt.	
5.2	Auditfile	Voor het verstrekken van gegevens door de ondernemer aan de Belastingdienst is de auditfile een belangrijk medium. De applicatie maakt een juiste en volledige overdracht van de financieel-gegevens via de auditfile mogelijk.	De maatregelen bieden een redelijke mate van zekerheid dat een juiste en volledige overdracht van de loonbelasting gegevens ten behoeve van de controle vanuit de Belastingdienst mogelijk maken.	5.2.1	De applicatie bevat maatregelen die de export van een auditfile, die door de Belastingdienst is geaccordeerd, ondersteunt.	
5.3	loon-aangifte	De applicatie moet een goede registratie van de Loonverplichtingen ondersteunen. Daartoe zijn naast een heldere en duidelijke structuur ook daarop afgestemde controlemechanismen noodzakelijk.	De maatregelen bieden een redelijke mate van zekerheid dat applicatie een goede registratie van de loon-verplichtingen aan de Belastingdienst ondersteunt via een heldere en duidelijke structuur met daarop afgestemde controlemechanismen.	5.3.1	De applicatie bevat maatregelen waarmee kan worden vastgesteld dat de loonaangifte technisch verwerkt kan worden door de Belastingdienst.	
				5.3.2	De dienst aanbieder heeft maatregelen om ervoor te zorgen dat de uitval die wordt gedetecteerd door de Belastingdienst en binnen zijn invloedssfeer is wordt gedetecteerd en aantoonbaar wordt terug gebracht.	Periodieke terugkoppeling vanuit OSWO / Belastingdienst van de veelgemaakte fouten. De bestanden worden aangeleverd met de volgende naamgeving "swo00000 - Reguliere terugkoppeling "nr. e vierwekenperiode / maand 2017" en "swo00000 - Extra terugkoppeling "maand 2017".
				5.3.3	De applicatie bevat maatregelen waarmee inzichtelijk is uit welke transacties de ingediende aangiften zijn samengesteld.	
				5.3.4	De applicatie is in staat te signaleren dat een correctieaangifte of heraanlevering noodzakelijk is.	De applicatie biedt inzicht in de transacties die (als)nog tot aangifte moeten leiden, zowel met betrekking tot de toekomst als voor de tijdvakken waarvoor reeds aangifte gedaan is.
5.4	Elektronisch bankieren	De applicatie biedt de mogelijkheid om een betaalbestand te exporteren/ automatische	De maatregelen bieden een redelijke mate van zekerheid dat een betaalbestand genereerd wordt waarmee geautomatiseerd betaald kan worden.	5.4.1	De applicatie bevat maatregelen waarmee de consistentie tussen de data (rekeningnummer, bedragen en tenaamstelling etc.) volgens de loonjournaalpost, loonaangifte en betaalbestand wordt bewerkstelligd.	Beveiliging van het genereerde bestand ligt bij de gebruikende entiteit.
5.5	Privacy	Binnen de applicatie is het niet mogelijk op privacy gevoelige data te versturen naar eindgebruikers	De maatregelen bieden een redelijke mate van zekerheid dat de privacy gevoelige data niet via onbeveiligde medium kan worden verstuurd.	5.5.1	De dienst aanbieder heeft maatregelen getroffen die zorgdragen dat wordt vastgesteld welke data privacy gevoelige zijn.	
				5.5.2	De dienst aanbieder heeft maatregelen die waarborgen dat er een risicoanalyse wordt gemaakt ten opzichte van het aanbieden van (nieuwe) functionaliteiten en het in overeenstemming zijn met de AVG.	
				5.5.3	De applicatie heeft maatregelen om ervoor te zorgen dat privacygevoelige data alleen via een veilige methode wordt verstuurd.	
5.6	Verwerken van wettelijke / fiscale wijzigingen		De maatregelen stellen in redelijke mate zeker dat de relevante fiscale wijzigingen tijdig, juist en volledig worden verwerkt.	5.6.1	De dienst aanbieder heeft maatregelen ingericht om ervoor te zorgen dat wijzigingen tijdig (voor de start van nieuwe fiscale verloningsjaar) worden doorgevoerd.	Tijdig is afhankelijk van de impact van de gebruiker. Algemene norm in ieder geval voor de verloning start van het nieuwe fiscale jaar dan moet voor de wijzigingen voor loonbelasting zijn doorgevoerd.
				5.6.2	De dienst aanbieder heeft maatregelen die ervoor zorgen dat de communicatie transparant is over de fiscale maatregelen die ondersteund worden door de applicatie.	
5.7	Pensioen		De maatregelen stellen in redelijke mate zeker dat de pensioenwijzigingen juist en volledig worden verwerkt.	5.7.1	De dienst aanbieder heeft maatregelen ingericht om ervoor te zorgen dat wijzigingen juist en volledig worden doorgevoerd.	
5.8	Cao		De maatregelen stellen in redelijke mate zeker dat er overeenstemming bestaat tussen de ondersteunde cao's volgens de applicatie en toegezegd in de communicatie van dienst aanbieder.	5.8.1	De dienst aanbieder heeft maatregelen en procedures om wijzigingen te identificeren, analyseren en effectueren in de applicatie.	Ter verduidelijking; indien een SWL aangeeft alle cao's ondersteund dan moet dit intern ondersteund worden door de SWL.
				5.8.2	De dienst aanbieder heeft maatregelen die ervoor zorgen dat transparant is welke cao's worden ondersteund en tot op welk niveau.	

# doelstelling	Onderwerp	Doelstelling	Beheersdoelstelling	# beheersmaatregel	Deze beheersmaatregelen zijn een baseline of eerste invulling.	Deze handreiking probeert de doelstellingen en maatregelen te verduidelijken nergens zijn opsommingen limitatief tenzij anders vermeld.
				5.8.3	De dienstaanbieder heeft maatregelen om fouten te constateren, op te volgen en indien noodzakelijk terug te koppelen naar de gebruiker.	

Wijzingen tussen versie 1.3 en 1.4

Toevoegen doelstelling 5.3 en maatregel 5.3.1.