Informatiebeveiligingsbeleid en eisen CIZ ICT-diensten

Europese aanbesteding 2016

Datum: 19/1/2016

Versie: 1.2

Inhoudsopgave

1 Doel van dit document

In dit document wordt een samenhangend beeld geschetst van de wijze waarop CIZ bij het uitvoeren van haar wettelijk taak zorg wil dragen voor de beveiliging van haar informatie in relatie tot de uit te besteden ICT diensten. Daarbij wordt naast de te hanteren kaders en algemene benadering ingezoomd op de verschillende onderwerpen waarbij de aanpak die CIZ voor staat meer inhoudelijk wordt omschreven.

De eisen zijn zo veel mogelijk op beleidsniveau geformuleerd (richting gevend) om de aanbieders de ruimte te bieden om naar eigen inzicht en expertise deze invulling te geven. Feitelijke eisen op operationeel niveau zijn niet opgenomen. Deze zullen later in de concretiseringsfase meegenomen worden.

2 Scope

Informatiebeveiligingsmaatregelen raken alle organisatie onderdelen, bedrijfsprocessen, systemen en informatiebronnen. De ICT dienstverlener zal niet alleen maatregelen moeten doorvoeren voor de door hem geleverde diensten maar ook zorgen dat de aansluiting op CIZ processen geborgd is, zoals de ITIL processen, bedrijfscontinuïteit en crisismanagement, enz.

3 Definitie van de informatiebeveiliging

Bij het uitvoeren van haar primaire taak verwerkt het CIZ veel bijzondere persoonsgegevens. Informatiebeveiliging neemt daarom bij het CIZ een belangrijke positie in, wat zich vertaald in een continu verbeterproces om continuïteit van de bedrijfsvoering en de beveiliging van privacy van onze cliënten te waarborgen.

Onder informatiebeveiliging verstaat CIZ het waarborgen van de

- Beschikbaarheid: betreft het waarborgen dat geautoriseerde gebruikers op de juiste momenten toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen).
- Integriteit: betreft het waarborgen van de juistheid, tijdigheid (actualiteit) en volledigheid van informatie en de verwerking ervan.
- Vertrouwelijkheid: betreft het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd.
- Controleerbaarheid: betreft de mogelijkheid om met voldoende zekerheid vast te kunnen stellen of wordt voldaan aan de eisen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid.

De ICT dienstverlener voor CIZ heeft in de uitvoering hiervan een significante rol en verantwoordelijkheid. Voor het inrichting van de beveiligingsorganisatie van CIZ wordt gebruik gemaakt van internationale standaarden en aangesloten op de geldende normenkaders vanuit de rijksoverheid.

4 Kaders

CIZ is een ZBO en valt onder het ministerie van VWS en maakt daarbij dus ook deel uit van de rijksoverheid. Naast algemene wetgeving heeft CIZ te voldoen aan kaders en richtlijnen die bij op deze plaats en rol binnen de overheid van toepassing zijn. Samen met haar eigen beleid resulteert dit in het volgende kaders:

<u>Wettelijk:</u>

- Wet Bescherming Persoonsgegevens (WBP)
  en haar aankomende opvolger, de Europese Algemene Verordening Gegevensbescherming
- Baseline informatiebeveiliging (BIR:2012)
- Archiefwet

<u>Regelgeving:</u>

- Norm ICT-beveiligingsassessments DigiD
- Richtsnoeren College Bescherming Persoonsgegevens (CBP)
- Privacy Impact assessment (PIA)

<u>Best practices:</u>

- OWASP top 10

Beleid:

- Informatiebeveiligingsbeleid CIZ 2016
- CIZ Beveiligingsovereenkomst ICT[1]

4.1 BIR

De voor de overheid verplichte standaarden ISO27001/ISO27002 zijn met aanvullingen opgenomen in de BIR. De BIR TNK is voor de Rijksoverheid verplicht. Afwijkingen zijn onder voorwaarden soms mogelijk.

De BIR is een gemeenschappelijke standaard die uitwisseling van departementaal vertrouwelijke informatie binnen de Rijksoverheid vergemakkelijkt door informatiebeveiligingsrisico's controleerbaar te beperken of op te heffen. Een gedeelte van de implementatie van de BIR normen zal door de ICT dienstverlener uitgevoerd worden. De BIR is geen doel op zich maar een norm binnen het Rijk om op uniforme wijze risico's tot acceptabele grootte terug te brengen voor als "Departementaal vertrouwelijke informatie" gerubriceerde informatie.

De ICT dienstverlener dient voor elk van de op zijn dienstverlening van toepassing zijnde normen en eisen de opzet, bestaan en werking te kunnen aantonen als CIZ of een externe auditor daar om vraagt.

CIZ is sinds 1-1-2015 een ZBO onder het ministerie van VWS en komt daarmee dichter tegen het Rijk aan te staan. In dat licht is het gevraagd dat bij het selecteren van informatiebeveiligingsoplossingen rekening wordt gehouden met (toekomstige) aansluitingsmogelijkheden van het Rijk.

5 IB Beleid

Het informatiebeveiligingsbeleid is vastgesteld in het document "Informatiebeveiligingsbeleid CIZ 2016 .pdf". Hieronder volgt een korte samenvatting.

Informatiebeveiliging volgt de eisen vanuit wet en regelgeving en de missie en visie van CIZ om haar taak zo efficiënt en effectief mogelijk uit te voeren. CIZ draagt vanuit haar rol een grote verantwoordelijkheid ten aanzien van het waarborgen van de vertrouwelijkheid van de medische gegevens van al onze cliënten. Door het integraal mee nemen van informatiebeveiliging in de eisen bij de ontwikkeling en implementatie van bedrijfsprocessen en ICT voorzieningen wordt de informatieveiligheid bij vernieuwingen geborgd. Daarnaast wordt voor de staande ICT omgeving en bedrijfsprocessen cyclisch risico analyses uitgevoerd, informatiebeveiligingsrisico's inzichtelijk gemaakt en proportionele mitigerende maatregelen getroffen.

De BIR is binnen de Rijksdienst voorgeschreven. Ook CIZ volgt dit beleid en legt hierover verantwoording af aan het ministerie van VWS. Periodieke interne en externe audits meten de compliance van CIZ aan de BIR.

De maatregelen in de BIR zijn passend voor departementaal vertrouwelijke informatie. Persoonsgegevens in de categorie 2 van de WBP vallen hier ook binnen. Voor bijzondere persoonsgegevens (WBP cat. 3), in het geval van CIZ zijn dat medische gegevens, zijn aanvullende maatregelen nodig.

6 Inrichting van de informatiebeveiliging

De vicevoorzitter van de raad van bestuur is eindverantwoordelijk voor de informatiebeveiliging. Het lijnmanagement is gedelegeerd verantwoordelijk voor de informatiebeveiliging in algemene zin en specifiek voor de BIR normen behorende bij haar verantwoordelijkheidsgebied. De CIO is door het bestuur gemandateerd voor alle besluiten op tactisch niveau. Samen met de CISO en internal auditor geeft hij sturing aan de informatiebeveiligingsprocessen en rapporteert minimaal een maal per kwartaal aan het bestuur in de Bestuursraad.

Vernieuwingen op bedrijfsvoering niveau worden besproken in het Advisory Board of Changes (ABC) en op ICT niveau in de Change Advisory Board (CAB). Voor beide processen is IB aangehaakt om zorg te dragen dat bij wijzigingen het huidige beveiligingsniveau minimaal gehandhaafd blijft.

[1] Beveiligingsovereenkomst ICT CIZ (220415 v 1.0).pdf

Rapportages van de normeigenaren(waaronder incidentrapportages) en uitkomsten van reguliere en ah hoc security audits zorgen voor inzicht in de actuele risico's, de effectiviteit van processen en maatregelen en uiteindelijk het actuele risico's profiel van CIZ voor de informatiebeveiliging.

7 CIZ IB strategie en eisen per thema

Bij de onderstaande thema's wordt meer per onderwerp ingezoomd op de informatiebeveiligingsaspecten, eisen en oplossingsrichtingen. Deze komen dus boven op de reeds gestelde kaders.

7.1 Classificatie van informatie

CIZ verwerkt naast de gebruikelijke bedrijfsvoering informatie (bestuurlijke, personele, financiële, etc. informatie) een grote hoeveelheid bijzondere persoonsgegevens. Het gaat hier om medische informatie afkomstig van cliënten zelf en informatie aangeleverd vanuit de medische disciplines. De omgang met dit type informatie vraagt extra aandacht om de privacy van onze cliënten te kunnen garanderen maar ook aan specifieke wettelijke normen te kunnen voldoen (w.o. de archiefwet).

7.2 Vertrouwelijkheid

CIZ gebruikt voor de indeling van de vertrouwelijkheid van haar informatie 3 categorieën, nl:

- Openbare informatie: dit is alle informatie die CIZ publiekelijk beschikbaar stelt via rapportages, eigen website e.d.
- Vertrouwelijke informatie: de BIR schrijft maatregelen voor die voldoende zijn voor de beveiliging van informatie tot en met Departementaal Vertrouwelijk. De reguliere CIZ bedrijfsvoering informatie valt hier onder en ook de WBP categorie 2 persoonsgegevens.
- Geheime informatie: de medische gegevens die CIZ verwerkt vallen onder de WBP categorie 3. Daarnaast heeft CIZ informatie die bij uitlekken ernstige schade kunnen veroorzakenzoals informatie over fraudeonderzoeken, inhoudelijke informatie over de (status van) de beveiliging van de ICT omgeving, enz. Deze informatie soorten vragen om een aanvullende maatregelen bovenop die van de BIR om de vertrouwelijkheid te waarborgen.

7.3 Beschikbaarheid, wettelijke termijnen en CIZ beleid

De wettelijke termijn waarbinnen CIZ op een zorgaanvraag een besluit moet afgeven is 6 weken. CIZ heeft echter zich zelf als doel gesteld om zo veel mogelijk de aanvragen binnen 2 weken af te handelen. Naast andere tijdgevoelige bedrijfsprocessen is ook de hoeveelheid aanvragen een beperkende factor als het gaat om acceptabele uitval van systemen.

CIZ wil voorkomen dat kwetsbare groep cliënten die ze bedient door gegevensverlies bij CIZ deze opnieuw moet aanleveren. Daarom is de volgende richtlijn voor gegevensverlies (RPO) gesteld:

	WLZ	Commu-ni-catie	Salaris-be-taling	Bedrijfs-voering	RPO (max)
Basisvoorzieningen	x	x	x	x	1 min.
Virtuele werkplek	x	x	x	x	1 min.
Mail	x	x		x	1 min.
Bedrijfsvoeringsapplicaties			x	x	1 min.
Portero (run)	x				1 min.
Portero (change)					1 min.
Sharepoint	x	x		x	1 min.
TOPdesk				x	1 min.
Bezwaar en beroep					1 min.
BI-omgeving / Onderzoek	x			x	1 min.

Voor de beschikbaarheid van het primaire proces en reguliere bedrijfsprocessen is de volgende richtlijn voor uitval (RTO) gesteld:

	WLZ	Commu-ni-catie	Salaris-be-taling	Bedrijfs-voering	RTO (max)
Basisvoorzieningen	x	x	x	x	4 uur
Virtuele werkplek	x	x	x	x	4 uur
Mail	x	x		x	1 uur
Bedrijfsvoeringsapplicaties			x	x	72 uur
Portero (run)	x				24 uur
Portero (change)					48 uur
Sharepoint	x	x		x	24 uur
TOPdesk				x	48 uur
Bezwaar en beroep					48 uur
BI-omgeving / Onderzoek	x			x	24 uur

Voorwaarde is dat voor spoedaanvragen (binnen 48 uur) er alternatieve bedrijfsscenario's (ABS) beschikbaar zijn.

Herstel van de gestructureerde en ongestructureerde data van het primaire proces (Portero systemen) moet mogelijk zijn voor een periode van 3 maanden waarbij de eerste week op dag niveau, dan een maand lang op week niveau, vervolgens een kwartaal lang op maand op niveau.

Voor de resterende data geldt hetzelfde schema, waarbij data minimaal 5 jaar hersteld kan worden, waarbij na het eerste jaar, halfjaarlijkse herstelpunten mogelijk zijn. Streven moet zijn om de RTO van ongestructureerde data zo kort mogelijk te houden (<24 uur).

Hersteleisen voor de BI systemen en informatie worden meegenomen in het ontwerp voor de betreffende omgeving.

In het geval van een crisis zijn er processen en voorzieningen beschikbaar om de impact op het primaire proces en de interne bedrijfsvoering van CIZ zo beperkt mogelijk te houden en de duur en effect van de uitval binnen de gestelde kaders te kunnen garanderen.

7.4 Servicemanagement en informatiebeveiliging

De kwaliteit van de servicemanagement processen is van invloed op de effectiviteit van de informatiebeveiligingsprocessen omdat die daar veelal van afhankelijk zijn (configuratiemanagement, changemanagement en incidentmanagement, enz). Een servicemanagementproces kan voor een deel bij CIZ zelf en een deel bij de ICT dienstenleverancier liggen en moet naadloos aansluiten voor een effectieve werking.

Een wijzigingsverzoek van CIZ moet door de ICT dienstenleverancier meer dan alleen technisch beoordeeld worden maar ook t.a.v. de beveiliging en mogelijk functionele consequenties (bijv. relaties tussen systemen).

Informatiebeveiligingsincidenten moeten door grote waakzaamheid, alerte signalering, inhoudelijke expertise, kennis van de CIZ werkprocessen en daarbij behorende systemen snel beoordeeld kunnen worden op impact en passend worden opgevolgd. Nieuw ontdekte kwetsbaarheden (hard- en software) moeten ook als een informatiebeveiligingsincident opgepakt worden. Registraties van (informatiebeveiligings)incidenten mogen nooit informatie met de classificatie geheime bevatten.

7.5 Identity Access Management (IAM)

CIZ wil haar organisatie en bedrijfsprocessen slim en efficiënt inrichten zodat de klant optimaal wordt bedient (snelheid, kwaliteit) maar wil ook nadrukkelijk de privacy van de klanten waarborgen. Beschikbaarheid en vertrouwelijkheid zijn twee kanten van dezelfde medaille. De gevolgen van het uitlekken van vertrouwelijke informatie worden door de striktere wetgeving steeds groter en vraagt daardoor om gerichte aandacht, zorg en controle om die te voorkomen.

7.5.1 Vertrouwelijkheid

Het informatiebeveiligingsbeleid van CIZ stelt daarom dat medewerkers in principe alleen toegang hebben tot die informatie die noodzakelijk is voor de uitvoering van haar functie of rol tenzij er zwaarwegende redenen zijn om hier van af te wijken. De toegang tot de CIZ werkomgeving, systemen en informatie moet fijnmazig gereguleerd kunnen worden. De authenticatie moet passen bij de wijze van toegang tot en de classificatie van de informatie. Gezien het feit dat het overgrote deel van de medewerkers toegang nodig heeft tot de primaire proces systemen wordt er om pragmatische redenen gesteld dat (in de toekomst) alle toegang tot de CIZ ICT omgeving 2 factor authenticatie vereist, bij voorkeur in combinatie met SSO.

7.5.2 Beschikbaarheid

De toegang tot de CIZ werkomgeving, systemen en informatie moet laagdrempelig en gebruikersvriendelijk zijn. Een tijd, plaats en apparaat of onafhankelijke standaard digitale werkomgeving die alleen bij het aanmelden om authenticatie vraagt, ook als er vanuit de CIZ werkomgeving systemen met authenticatie buiten het CIZ domein worden aangeroepen (ASP/SAAS). Management van de autorisaties is in principe centraal belegd, maar daar waar flexibiliteit noodzakelijk is voor de bedrijfsvoering kan het uitdelen van rechten in de organisatie belegd worden. Zo zouden managers zelf tijdelijke rechten kunnen toekennen voor de systemen waar zij eigenaar van zijn, in zoverre dit geen onacceptabele risico's met zich mee brengt.

Bij het selecteren van voorzieningen op het vlak IAM (en mogelijk hardware) dient rekening gehouden te worden met mogelijk toekomstig gebruik van de Rijkspas door CIZ als gebouwtoegangssysteem. Ook moet rekening gehouden worden met het gebruik van de pas als authenticatie middel voor toegang tot het CIZ netwerk, voor "follow me printing" en mogelijk beveiligde email en digitale handtekening.

7.6 Access devices, digitale werkomgeving en opslag van CIZ data

Door een gebruikersvriendelijke werkomgeving aan te bieden (door o.m. te letten op aspecten zoals die hierboven zijn genoemd) wordt de behoefte van medewerkers om eigen oplossingen te introduceren verkleind. Echter is consumerization, zoals BYOD, een voldongen feit en vraagt alertheid en flexibiliteit van ICT diensten leverancier. Vanuit informatiebeveiligingsoogpunt dienen de volgende principes gehanteerd te worden:

- CIZ heeft te allen tijde zicht op waar haar bedrijfsdata is opgeslagen (device, dienst, plaats).
- CIZ heeft controle over deze data (beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid).
- zero footprint voor de devices is het uitgangspunt (zoals in de BIR gesteld).
- de opslag voldoet aan de continuïteitseisen van CIZ en de archiefwet.
- centrale opslagsystemen mogen niet buiten de Europese Unie (EU) worden gesitueerd.
- CIZ informatie met de classificatie "geheim" mag nooit buiten de invloedsfeer van CIZ geraken (bijv. door in beslag name van gedeelde systemen van een andere klant).

7.7 Ontwikkeling en onderhoud/beheer informatiesystemen

Bij de ontwikkeling van informatiesystemen moeten samen met de functionele wensen ook de eisen t.a.v. de beveiliging en, indien van toepassing, fraude preventie worden meegenomen. CIZ heeft nog niet formeel de aanpak Grip op Secure Software Development (SSD) van het CIP maar staat positief tegenover en zien deze dan ook graag gebruikt worden bij haar ICT diensten leveranciers (in zoverre die van toepassing is).

Voor ontwikkelomgeving zijn andere benaderingen van de informatiebeveiliging mogelijk. Daarbij moet dan wel aan een aantal randvoorwaarden worden voldaan, zoals het volledig ontbreken van bedrijfsvoeringdata in het ontwikkeldomein, een volledig van de rest van de het ICT landschap geïsoleerd zone met strikte protocollen t.a.v. de export van code naar de test en productieomgevingen. Rechtstreekse toegang vanaf het CIZ LAN tot de ontwikkel omgeving is mogelijk mits er vooraf een risicoanalyse is uitgevoerd en er op basis daarvan schriftelijk goedkeuring is gegeven door de CIO van CIZ.

Externe toegang tot CIZ ICT systemen voor ontwikkel/beheer werkzaamheden dient op één uniforme wijze te zijn gefaciliteerd waarbij nooit sprake is van rechtstreekse toegang tot het CIZ netwerk maar bijvoorbeeld via een stepping stone constructie. Tooling voor beheerwerkzaamheden worden binnen het CIZ domein gehost.

Voor externe toegang tot de ontwikkel omgeving of ten behoeve van beheeractiviteiten is 2 factor authenticatie vereist.

7.8 Logging, rapportage, controle en audits en comply or explain

7.8.1 Logging

Relevante activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen moeten worden vastgelegd in audit-logbestanden ten behoeve van toekomstig onderzoek en toegangscontrole. De logging over informatiebeveilgingsgebeurtenissen moeten minimaal 5 jaar bewaard te worden. Met deze logging moet het, zonder al te grote inspanningen, mogelijk zijn om toegang tot en gebruik van de CIZ ICT omgeving door een gebruiker met tijd en plaats aanduidingen inzichtelijk te maken, zodanig dat deze als bewijsvoering kan dienen bij onderzoek naar mogelijk misbruik van ICT systemen en/of fraude.

7.8.2 Rapportages

CIZ wil proactief op de hoogte gehouden worden van de werking van de informatiebeveiligingsprocessen en het risico profiel van de CIZ ICT landschap door middel van periodieke en ad hoc rapportages (bij incidenten). De actuele beveiligingssituatie wordt laagdrempelig inzichtelijk gemaakt, bijvoorbeeld met een online dashboard.

7.8.3 Controle en audits

CIZ heeft te allen tijde het recht op inzage in de wijze waarop de ICT dienstenleverancier de informatiebeveiliging voor de CIZ ICT diensten heeft geborgd. De ICT dienstverlener verleent toegang en medewerking aan externe auditpartijen die in opdracht van CIZ audits uitvoeren op de naleving van wet en regelgeving in algemene zin en de uitvoering van de BIR maatregelen in het bijzonder. Jaarlijks wordt er minimaal één controle door CIZ en één audit/test door een externe partij uitgevoerd.

7.8.4 Comply or explain

De externe dienstverlener voldoet aan de voor de afgenomen ICT diensten relevante BIR normen, privacy wetgeving en kan de opzet, bestaan en werking van de maatregelen aantonen. Daar waar dit niet het geval is ligt er een door CIZ geaccepteerde explain verklaring [2] waarom aan een bepaalde norm uit de BIR niet wordt voldaan. Of er ligt een plan van aanpak om binnen een vastgesteld termijn aan de norm te gaan voldoen.

7.9 Informatie uitwisseling en veilige transport

CIZ krijgt via verschillende stromen vertrouwelijke informatie aangeleverd. CIZ stuurt zelf gegevens t.a.v. de indicatiebesluiten de zorg keten in. Daarnaast worden reguliere rapportages en ad hoc onderzoeksrapporten aan derde partijen aangeleverd. De kanalen waarover deze informatie verstuurt en ontvangen wordt dient passend bij de classificatie van die informatie beveiligd te zijn. Dit geldt voor o.a. de volgenden uitwisselingsvormen:

- Binnen krijgen van vertrouwelijke informatie via email ((toekomstige)cliënten en ketenpartners).
- Versturen van vertrouwelijke mail aan ketenpartners.
- Een "berichten box" waar geregistreerde ketenpartners informatie kunnen plaatsen en/of ophalen.
- Berichtenverkeer op basis van SOA aan vaste ketenpartners.
- Via de CIZ websites invoeren van tekst en uploaden van documenten.

7.10 Wet meldplicht datalekken

Per 1 januari 2016 is de Wet Meldplicht Datalekken van kracht. De wet verplicht de verantwoordelijke bij een datalek, waarbij er kans is op verlies of onrechtmatige verwerking van persoonsgegevens, melding te doen bij de toezichthouder, de Autoriteit Persoonsgegevens (AP) en de betrokkene. In het geval de ICT-dienstverlener een datalek en/of de gevolgen daarvan signaleert, dient deze direct het CIZ hiervan op de hoogte te stellen. Het CIZ is de verantwoordelijke en zal zorgdragen voor de opvolging. In geen geval is de ICT-dienstverlener gemachtigd zelf melding te maken bij de genoemde partijen anders dan het CIZ.

[2] BIR_explainprocedure_1.0_voor_ICCIO-1