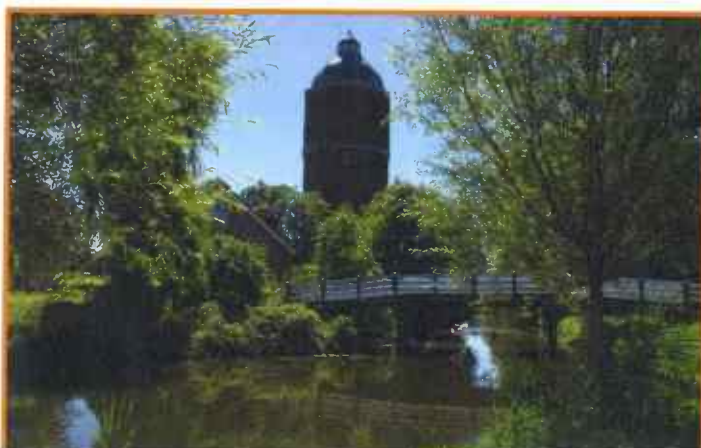




Informatieveiligheidsbeleid SED

Informatiebeveiliging op tactisch niveau 2020-2022

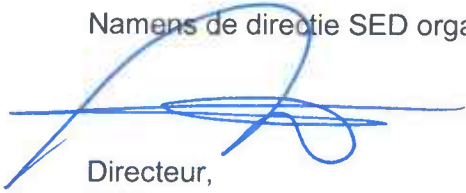


Versiebeheer

Versie	Datum	Door	Wijzigingen
0.1	September 2020	B.J. de Vries	Eerste opzet
0.2	September 2020	Margreet Smit Paul Gijben	Aanpassingen inhoudelijk
0.3	Oktober 2020	B.J. de Vries	Aanpassingen
0.9	Oktober 2020	Margreet Smit Paul Gijben	Opmerkingen en aanvullingen
1.0	November 2020	B.J. de Vries Paul Gijben	Definitief

Vastgesteld d.d. 2 december 2020

Namens de directie SED organisatie,



Directeur,
C.M. Minnaert

Inhoudsopgave

1.	Inleiding	4
5.	Beleid	6
5.1	Aansturing door de directie	6
6.	Organisatie van de informatiebeveiliging	6
6.1	Interne organisatie	6
6.2	Mobiele apparatuur en telewerken	7
7.	Veilig personeel	8
7.1	Voorafgaand aan het dienstverband	8
7.2	Tijdens het dienstverband	8
7.3	Beëindiging en wijziging van dienstverband	8
8.	Beheer van bedrijfsmiddelen	9
8.1	Verantwoordelijkheid voor bedrijfsmiddelen	9
8.2	Informatieclassificatie	9
8.3	Behandelen van media	9
9.	Toegangsbeveiliging	10
9.1	Bedrijfseisen voor toegangsbeveiliging	10
9.2	Beheer van toegangsrechten van gebruikers	10
9.3	Verantwoordelijkheden van gebruikers	10
9.4	Toegangsbeveiliging van systeem en toepassing	11
10.	Cryptografie	11
11.	Fysieke beveiliging en beveiliging van de omgeving	11
11.1	Beveiligde gebieden	11
11.2	Apparatuur	12
12.	Beveiliging bedrijfsvoering	12
12.1	Bedieningsprocedures en verantwoordelijkheden	12
12.2	Bescherming tegen malware	12
12.3	Back-up	12
12.4	Verslaglegging en monitoren	12
12.5	Beheersing van operationele software	13
12.6	Beheer van technische kwetsbaarheden	13
12.7	Overwegingen betreffende audits van informatiesystemen	13
13.	Communicatiebeveiliging	13
13.1	Beheer van netwerkbeveiliging	13
13.2	Informatietransport	13
14.	Acquisitie, ontwikkeling en onderhoud van informatiesystemen	14
14.1	Beveiligingseisen voor informatiesystemen	14
14.2	Beveiliging in ontwikkelings- en ondersteunende processen	14
14.3	Testgegevens	14
15.	Leveranciersrelaties	14
15.1	Informatiebeveiliging in leveranciersrelaties	14
15.2	Beheer van dienstverlening van leveranciers	15
16.	Beheer van informatiebeveiligingsincidenten	15
16.1	Beheer van informatiebeveiligingsincidenten en –verbeteringen	15
17.	Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	16
18.	Naleving	16
18.1	Naleving van wettelijke en contractuele eisen	16
18.2	Informatiebeveiligingsbeoordelingen	16
	Bijlage 1 Documenten behorende bij het InformatieBeveiligingsBeleid SED	17

1. Inleiding

Iedere medewerker van de SED werkt met informatie. Veel van deze informatie heeft een gevoelig karakter: gegevens van burgers vallen onder de privacy wetgeving, financiële gegevens van een gemeente zijn vaak nog niet openbaar, de voorbereiding van een vergunning kan reacties uitlokken etc. Daarom gaat de gehele SED organisatie zorgvuldig met de gegevens zelf en de procedures omtrent gegevens om en hanteert de SED een informatiebeveiligingsbeleid.

Het door de SED gehanteerde informatiebeveiligingsbeleid, ook wel informatieveiligheidsbeleid of IBBeleid genoemd, is beleid op tactisch niveau.

De kaders voor het IBBeleid op strategisch niveau worden aangegeven door de gGemeenten Stede Broec, Enkhuizen en Drechterland. De gemeenschappelijke uitvoeringsorganisatie SED realiseert het strategisch IBBeleid op tactisch en deels op operationeel niveau waarbij veel ICT gerelateerde zaken zijn uitbesteed aan een andere partij.

Bij de inrichting van de informatiebeveiliging van de SED worden de richtlijnen van de Vereniging Nederlandse Gemeenten (VNG) gevolgd welke zijn geformuleerd door de InformatieBeveiligingsDienst (IBD).

Een belangrijk deel van deze richtlijnen is vormgegeven als een norm: de Baseline Informatiebeveiliging Overheid (BIO), de opvolger van, onder andere, de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Voor de BIO gold 2019 als een overgangsjaar en zal 2020 het eerste jaar zijn waarin gemeenten en uitvoeringsorganisaties worden getoetst op de implementatie.

De juridische onderbouwing van de verplichting tot het beveiligen van informatie kan o.a. gevonden worden in de Algemene Verordening Persoonsgegevens (AVG).

In artikel 24 van de AVG wordt gesteld dat persoonsgegevens adequaat beschermd moeten worden:

Artikel 24 Verantwoordelijkheid van de verwerkingsverantwoordelijke

1. Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.
2. Wanneer zulks in verhouding staat tot de verwerkingsactiviteiten, omvatten de in lid 1 bedoelde maatregelen een passend gegevensbeschermingsbeleid dat door de verwerkingsverantwoordelijke wordt uitgevoerd.
3. Het aansluiten bij goedgekeurde gedragscodes als bedoeld in artikel 40 of goedgekeurde certificeringsmechanismen als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat de verplichtingen van de verwerkingsverantwoordelijke zijn nagekomen.

Met dit artikel is de verwerkingsverantwoordelijke tevens eindverantwoordelijke voor de informatiebeveiliging in al haar aspecten.

In art. 24 lid 3 wordt aangegeven dat aansluiting gezocht mag worden bij een goedgekeurde gedragscode. De BIO is de gedragscode, of norm, voor de gehele Nederlandse overheid.

Vanaf 2020 moeten overheden zich aantoonbaar aan deze norm houden.

Om dit aan te kunnen tonen moeten, o.a., beleidsdocumenten beschikbaar zijn, een Information Security Management System (ISMS) zijn ingericht waarin een PDCA cyclus (Plan-Do-Check-Act) gehanteerd wordt en een scala van praktische maatregelen genomen zijn om de informatiebeveiliging in de praktijk te brengen en de persoonsgegevens daadwerkelijk te beschermen waarbij risicobeheersing prioriteit heeft.

Vanwege de complexe situatie van de SED en de drie gemeenten wordt het IBBeleid zorgvuldig uitgewerkt.

In de beschrijving van de verschillende onderdelen van het beleid wordt de nummering van de hoofdstukken van de BIO aangehouden en begint het beleid met Hoofdstuk 5. Deze nummering wordt ook gehanteerd in normen voor informatiebeveiliging in andere branches en is afgeleid van de internationale norm voor informatiebeveiliging de ISO 27001/2.

Verschillende onderdelen van dit beleid geven aanleiding tot het opstellen van aparte documenten die dit beleid ondersteunen of mogelijk maken. Een lijst van deze documenten is te vinden in Bijlage 1.

5. Beleid

Het doel van het informatiebeveiligingsbeleid is het mogelijk maken van sturing door de directie SED op het gebied van de informatiebeveiliging. De directie is "in control" en legt vast in een beleid onder welke voorwaarden beslissingen in de informatiebeveiliging worden genomen.

5.1 Aansturing door de directie

De directie SED stuurt de uitvoering van het beleid rondom informatiebeveiliging rechtstreeks aan en ziet informatiebeveiliging als een van de belangrijkste aspecten in het omgaan met gegevens van burgers, medewerkers en bedrijven binnen de SED.

Hiertoe beschikt de directie SED over een actueel informatiebeveiligingsbeleid (IBBeleid SED, het voorliggende document) en een organisatie die het IBBeleid voorbereid, uitvoert, begeleidt, implementeert en controleert.

Het IBBeleid wordt tenminste iedere drie jaar geëvalueerd, indien noodzakelijk bijgesteld en vastgesteld. Omstandigheden kunnen het noodzakelijk maken dat de evaluatie, bijstelling en vaststelling eerder dan na drie jaar plaats vindt.

Het IBBeleid moet gezien worden als een raamwerk waarbij aan het voorliggende beleid uitwerkingen van aspecten van de informatiebeveiliging worden toegevoegd. Deze worden apart vastgesteld door de directie en bij de eerstvolgende evaluatie van het IBBeleid toegevoegd aan dit beleidsdocument.

6. Organisatie van de informatiebeveiliging

Informatiebeveiliging is iets dat de gehele organisatie aangaat. Het is niet zo dat de verantwoordelijkheid belegd wordt bij een enkele medewerker en dat het daarmee geregeld is. Iedere medewerker heeft een verantwoordelijkheid in de beveiliging van informatie en kan, en zal, daar op aangesproken worden.

Om de organisatie hierin goed te ondersteunen wordt een interne organisatie ingericht.

6.1 Interne organisatie

De directie SED rapporteert over de informatiebeveiliging aan het Dagelijks Bestuur van de SED. Rechtstreeks aan de directie van de SED rapportierend is:

Chief Information Security Officer (CISO)

De CISO is verantwoordelijk voor de implementatie van het IBBeleid in de SED organisatie en de samenwerking op dit gebied met de relaties van de SED. De CISO overlegt over IB aspecten met alle delen van de organisatie welke gegevens verwerken en/of hier een verantwoordelijkheid in hebben. Tevens is de CISO betrokken bij de overleggen met relaties voor wat betreft de IB. De precieze taken en verantwoordelijkheden zijn vastgelegd in het Functieprofiel CISO.

Aan de CISO rapporteren:

Information Security Officer (ISO)

De CISO geeft dagelijks leiding aan één of meerdere ISO's. Deze zijn verantwoordelijk voor de taken van het IBBeleid.

De precieze taken en verantwoordelijkheden zijn vastgelegd in het Functieprofiel ISO.

Privacy Officer (PO)

De CISO geeft dagelijks leiding aan één of meerdere PO's. Een PO verzorgt de dagelijkse werkzaamheden volgend uit de implementatie van de AVG, waaronder voorlichting en begeleiding van medewerkers, verwerkersovereenkomsten, controles en voorbereiding rapportages en mogelijk meldingen.

De precieze taken en verantwoordelijkheden zijn vastgelegd in het Functieprofiel PO.

Onafhankelijk:

Functionaris Gegevensbescherming (FG)

De FG neemt een onafhankelijke positie in in de organisatie. De FG ziet toe op de naleving van de AVG binnen de organisatie en adviseert de verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke voor de gegevens die de SED verwerkt is de directie SED. De verwerkingsverantwoordelijke voor de gegevens die de SED verwerkt namens de gemeenten is het college van de betreffende gemeente.

Doordat de FG toezicht houdt op de naleving van de AVG, houdt deze eveneens toezicht op de effectiviteit van het IBBeleid SED.

Relaties

De CISO houdt een overzicht bij met de relaties waarmee de SED informatie uitwisselt, met daarbij speciale aandacht voor gevoelige informatie. In dit overzicht wordt bijgehouden welke maatregelen er getroffen zijn om de informatie bij uitwisseling te blijven beschermen en hoe dat gecontroleerd wordt.

Een belangrijke relatie is die met het Shared Service Centrum DeSom (SSC DeSom) die het grootste deel van de geautomatiseerde verwerking van de gegevens, welke de SED beheert, verzorgt. De CISO SED onderhoudt een nauw contact met de CISO van SSC DeSom.

De CISO is verantwoordelijk voor de afstemming van de maatregelen betreffende de informatiebeveiliging en heeft dan ook een belangrijke bijdrage in de overeenkomsten die tussen de partijen gesloten worden.

De CISO zoekt waar mogelijk samenwerking en afstemming met CISO's in de regio en met landelijke organisaties zoals de IBD.

6.2 Mobiele apparatuur en telewerken

De medewerkers van de SED zijn niet altijd werkplek gebonden en in veel gevallen is het toegestaan om (een deel van) de werkzaamheden thuis uit te voeren. De vereisten omtrent de informatiebeveiliging zijn vastgelegd in het Thuiswerkprotocol.

Om dit mogelijk te maken stelt de SED mobiele apparatuur ter beschikking en staat, deels, het gebruik van eigen apparatuur toe.

Het beleid hierin, inclusief het IBBeleid voor mobiele apparatuur is vastgelegd in een document, BYOD en CYOD, dat mede door de CISO van de SED en SSC DeSom wordt onderhouden.

7. Veilig personeel

Het personeel van de SED werkt met gevoelige informatie. Deze informatie kan bestaan uit persoonsgegevens, waarop de AVG van toepassing is, en zelfs uit bijzondere persoonsgegevens. Daarnaast zijn er gegevens met een meer bedrijfsvertrouwelijk karakter, zoals financiële gegevens van de SED zelf, plannen en financiering van bedrijven, aanvragen van vergunningen etc. De SED gaat er vanuit dat iedere medewerker, en daarmee worden alle medewerkers bedoeld, niet alleen die in vaste dienst maar ook inhuurkrachten, stagiairs en vrijwilligers, zich van zijn of haar verantwoordelijkheid bewust is en zorgvuldig en veilig met de gegevens omgaat. In het personeelsbeleid worden enkele maatregelen genomen om dit te borgen¹.

7.1 Voorafgaand aan het dienstverband

Voorafgaand aan het dienstverband wordt van iedere medewerker een Verklaring Omtrent Gedrag (VOG) verlangd. Is deze niet beschikbaar dan kan de aanstelling heroverwogen worden of een herziene beslissing worden genomen.

Indien de medewerker te maken krijgt met een speciale klasse van vertrouwelijke gegevens kan besloten worden tot nader onderzoek, zoals een uitgebreide screening.

In de functieomschrijving, aanstellingsbrief of soortgelijk, is opgenomen welke verantwoordelijkheden de medewerker heeft ten aanzien van de omgang met informatie en de informatiebeveiliging. Tevens is er een meer algemeen gestelde brochure aangaande de informatiebeveiliging voor het personeel beschikbaar.

Het personeelsinformatiesysteem beschikt over een geautomatiseerde koppeling met de basale ICT infrastructuur. Hiermee wordt bereikt dat de toegang tot informatie geopend en gesloten wordt bij aanvang en beëindiging van de aanstelling. Dit systeem is gekoppeld met het geautomatiseerde rechtenbeheerssysteem zodat ook toegang tot applicaties en gegevensverzamelingen automatisch wordt aangepast bij wijziging van de aanstelling.

7.2 Tijdens het dienstverband

De medewerkers van de SED volgen verplicht een opleiding informatiebeveiliging die past bij de functie. Deze opleiding wordt regelmatig in vernieuwde vorm herhaald. De herhaling is van belang omdat het ICT-landschap voortdurend verandert en nieuwe vaardigheden en kennis worden vereist.

De continue opleiding² zorgt ervoor dat medewerkers attent blijven op mogelijke misstanden en bereid zijn deze te melden bij een centraal meldpunt dat beheerd wordt door de CISO. De medewerkers worden bij dit soort meldingen beschermd via de klokkenluidersregeling³.

7.3 Beëindiging en wijziging van dienstverband

Bij het beëindigen van het dienstverband worden automatisch alle rechten van de medewerker tot het gebruik van informatie ingetrokken. Mogelijk gebruikte apparatuur wordt ingeleverd.

¹ Veilige werkomgeving beleid incl privacy

² Zie ook Arbozorgbeleid 2020

³ Zie ook Handreiking ongewenste omgangsvormen SED organisatie en rol vertrouwenspersonen (intern), augustus 2020

Via de brochure informatiebeveiliging worden de medewerkers er nogmaals op attent gemaakt dat de geheimhoudingsplicht, die deel uitmaakt van de aanstelling, geldig blijft na het beëindigen van het dienstverband.

8. Beheer van bedrijfsmiddelen

Om te kunnen werken beschikken de medewerkers van de SED over de juiste middelen: gegevens, programmatuur en apparatuur om gegevens mee te verwerken, faciliteiten op de werkplek, communicatiemiddelen etc.

De algemene regel is dat informatie welke door de SED wordt beheerd alleen via door de SED beschikbaar gestelde bedrijfsmiddelen wordt verwerkt. Alleen met extra maatregelen kan hiervan worden afgeweken, zoals, onder andere, vastgelegd in het Thuiswerkprotocol en het Beleid BYOD en CYOD.

8.1 Verantwoordelijkheid voor bedrijfsmiddelen

De SED houdt alle medewerkers aan een gedragscode voor wat betreft het omgaan met informatie in het algemeen en met vertrouwelijke informatie in het bijzonder.

De leidinggevende zal medewerkers regelmatig op deze gedragscode wijzen en in voorkomende gevallen de kennis ervan toetsen, bijvoorbeeld tijdens een functioneringsgesprek.

8.2 Informatieclassificatie

Alle informatie die door de SED verwerkt wordt is ingedeeld in klassen naar aanleiding van een risico afweging. Het basisniveau van alle informatie is "vertrouwelijk" (BBN 2). De meeste informatie bevat immers persoonsgegevens of is bedrijfsvertrouwelijk. Indien informatie openbaar is dan is dit expliciet aangegeven. Een hoger niveau (BBN 3, Staatsgeheimen) komt binnen de SED niet voor. Een nuancering van het basisniveau kan toegepast worden indien daar behoefte aan is.

8.3 Behandelen van media

Gegevens kunnen op verschillende media staan. Naast de servers in de beveiligde computerruimten zijn er in gebruik:

- USB-sticks
- Papier
- Verwijderbare harddisks of SSD's
- Laptops
- Tablets en mobiele telefoons
- CD's en DVD's

De regel is dat vertrouwelijke informatie niet op verwijderbare media mag worden opgeslagen. Voor laptops, tablets en mobiele telefoons geldt dit ook, met daarbij de uitzondering dat deze wel programmatuur voor de toegang tot vertrouwelijke informatie (b.v. mail, OneDrive) aan boord mogen hebben als de apparatuur onder beheer van de SED staat.

Indien media niet meer gebruikt worden, dan worden deze ingeleverd op een centraal punt waarna het wissen en vernietigen via een goedgekeurde procedure volgt. Het bedrijf dat de media vernietigt verstrekt een certificaat van vernietiging. Van de procedure wordt een registratie bijgehouden.

9. Toegangsbeveiliging

Hoewel de meeste medewerkers van de SED voor hun werk toegang tot ICT faciliteiten en de beheerde informatie nodig hebben ligt het niet voor de hand dat alle medewerkers bij alle informatie kunnen. Alleen toegang tot informatie welke noodzakelijk is om het werk te doen (need-to-know) en waar de medewerker impliciet of expliciet toestemming voor heeft is toegelaten (AVG). Dit vereist regulering van de toegang tot faciliteiten en informatie, ook wel bekend onder de term autorisatiebeheer.

9.1 Bedrijfseisen voor toegangsbeveiliging

De gegevens welke door de SED beheerd worden, alsmede de aan de gegevens gekoppelde processen, worden uitsluitend verwerkt op ICT faciliteiten welke onder beheer staan van de SED, of beheerd worden door de organisatie waaraan de SED dit beheer heeft uitbesteed.

Mobiele apparatuur kan alleen gebruikt worden indien deze door de SED ten behoeve van de werkzaamheden verstrekt wordt (CYOD).

Eigen, of ongeautoriseerde, apparatuur (BYOD) krijgen geen toegang tot de gegevens welke door de SED beheerd worden, tenzij ze voldoen aan de maatregelen welke zijn genoemd in het vigerende CYOD/BYOD beleid en reglement.

9.2 Beheer van toegangsrechten van gebruikers

Voor het aanmelden en afsluiten van gebruikers van de ICT faciliteiten en andere geautomatiseerde processen is een procedure in gebruik welke wordt beheerst door de afdeling Personeelszaken en de SED Servicedesk. Deze afdelingen registreren iedere medewerker, al dan niet in loondienst, en kent een elektronische identiteit toe.

De elektronische identiteit, gebruikersnaam, is individueel. Groepsnamen of namen die alleen een functie beschrijven worden niet toegepast omdat deze anonimiteit in het omgaan met gegevens bevorderen.

De medewerker krijgt alleen toegang tot die gegevens en applicaties welke noodzakelijk zijn voor de uitoefening van de werkzaamheden. Deze toegangsrechten worden bijgehouden in een autorisatiematrix die jaarlijks wordt geëvalueerd en bijgewerkt. Dit jaarlijkse proces vindt plaats onder de verantwoordelijkheid van de CISO die hierover rapporteert aan de directie SED.

Het vaststellen welke rechten bij welke functie van toepassing zijn vindt eveneens plaats onder de verantwoordelijkheid van de CISO in samenwerking met Personeelszaken, applicatiebeheerders en verantwoordelijke leidinggevenden.

9.3 Verantwoordelijkheden van gebruikers

Gebruikers van de faciliteiten beschikken over een manier om zich te authenticeren bij de systemen waarmee zij werken. Zij gebruiken hiervoor, onder andere, een wachtwoord dat zij geheimhouden.

Om het gemakkelijk te maken complexe wachtwoorden beschikbaar te hebben wordt aan de gebruikers een wachtwoordenkluis ter beschikking gesteld.

Gestreefd wordt naar zo min mogelijk keren inloggen (Single Sign On, SSO) om het aantal gebruikte wachtwoorden en het intikken daarvan te beperken.

Naast wachtwoorden zijn andere vormen van authenticatie in gebruik waarbij biometrische eigenschappen en two-factor principes toegepast worden. Het streven is naar een wachtwoordloze en toch veilige omgeving te groeien.

9.4 Toegangsbeveiliging van systeem en toepassing

Aan welke eisen wachtwoorden moeten voldoen is vastgelegd in het wachtwoordenbeleid.

Dit beleid is afgestemd op de technische mogelijkheden die de dienstverlener kan bieden.

Daarnaast is het wachtwoordenbeleid erop gericht, zonder iets aan beveiliging in te leveren, zo gemakkelijk mogelijk hanteerbaar te zijn voor gebruikers en beheerders, conform de eisen die in de BIO zijn geformuleerd.

Voor medewerkers met een taak in het beheer van gegevens of faciliteiten kunnen strengere regels geformuleerd worden.

10. Cryptografie

Ten behoeve van de pseudonimisering van persoonsgegevens, het beveiligen van de verbinding met websites en voor het versleutelen van het transport van vertrouwelijke gegevens wordt gebruik gemaakt van cryptografische technieken. In de praktijk komt het er op neer dat de SED gebruik maakt van diverse certificaten met daarin de cryptografische sleutels.

Binnen de SED, en in samenwerking met ketenpartners, wordt een beleid (cryptografiebeleid) vastgesteld waarin is aangegeven:

- Wanneer cryptografie wordt ingezet
- Wie verantwoordelijk is voor het beheer van de certificaten en wie verantwoordelijk is voor de toepassing
- Welke vorm van cryptografie wordt ingezet.

11. Fysieke beveiliging en beveiliging van de omgeving

Om te voorkomen dat onbevoegden toegang krijgen tot informatie is het noodzakelijk de fysieke toegang tot plaatsen waar informatie wordt verwerkt te beveiligen. Immers, toegang tot een computer binnen een gebouw leidt gemakkelijker tot informatie dan vanaf een computer buiten het gebouw. Daarnaast kunnen kwaadwillenden schade aanrichten aan de infrastructuur of infrastructuur gebruiken voor criminele activiteiten.

11.1 Beveiligde gebieden

Voor alle gebouwen van de gemeenten en de SED geldt een toegangssysteem via pasjes. Alleen medewerkers met de juiste bevoegdheden hebben toegang tot gebouwen en ruimten.

Voorzieningen van de ICT infrastructuur zijn opgesteld in ruimten die alleen toegankelijk zijn met speciale bevoegdheden.

De bevoegdheden op de pasjes zijn gekoppeld met het Personeelsinformatiesysteem op dezelfde manier als de bevoegdheden voor toegang tot informatie en worden in een gekoppeld systeem beheerd.

Faciliteiten die kritiek zijn voor de informatieverwerking zijn opgesteld in ruimten voorzien van de juiste beveiliging voor wat betreft toegang en preventie van brand, wateroverlast etc. Indien mogelijk zijn de faciliteiten opgesteld bij een partner die hierin is gespecialiseerd, zoals thans bij SSC DeSom.

11.2 Apparatuur

Apparatuur op de vaste werkplekken van de SED en de gemeenten wordt beheerd door een partner. Voor deze apparatuur is een beleid betreffende de elektronische werkplek opgesteld.

12. Beveiliging bedrijfsvoering

De SED heeft de informatie verwerkende faciliteiten uitbesteed aan een andere partij. Het grootste deel is onder gebracht bij SSC DeSom.

Met alle partijen is een dienstenovereenkomst en een Service Level Agreement afgesloten en deze zijn aangevuld met een Verwerkingsovereenkomst conform de AVG.

12.1 Bedieningsprocedures en verantwoordelijkheden

In de SLA wordt, voor wat betreft de informatiebeveiliging, vastgelegd:

- afspraken en rapportage over de infrastructuur welke door de partner wordt beheerd. Dit is er op gericht dat de SED van mogelijke risico's op de hoogte is en deze kan betrekken in besluitvorming;
- afspraken en rapportage over wijzigingen in de informatie verwerkende faciliteiten;
- de afspraken inzake het testen en accepteren van de infrastructuur, applicaties en andere informatie verwerkende faciliteiten. Dit wordt gezien als een gezamenlijke verantwoordelijkheid.

12.2 Bescherming tegen malware

In de SLA is vastgelegd dat de partner maatregelen neemt om de faciliteiten, die de SED gebruikt, te beschermen tegen malware.

Het personeel van de SED en de Gemeenten wordt opgeleid om malware te herkennen, vermijden, melden en, indien mogelijk, te bestrijden. Gevonden malware dient altijd gemeld te worden aan de CISO.

12.3 Back-up

In samenwerking met de partner wordt voor iedere gegevensverzameling een backup beleid vastgesteld. Hierin is opgenomen de regeling hoe het backup beleid op reguliere basis getest wordt.

12.4 Verslaglegging en monitoren

Voor het vastleggen van gebeurtenissen in de informatie verwerkende faciliteiten worden logs bijgehouden conform de Handreiking Aanwijzing Logging, v. 2.0, maart 2019, IBD.

De monitoring is ingericht middels een SIEM en/of SOC. De SED ontvangt verslagen van de monitoring, zoals vastgelegd in de SLA.

12.5 Beheersing van operationele software

Voor de beheersing van operationele software zijn functioneel applicatiebeheerders aangesteld binnen de SED. De beheersing van de infrastructuur en daarbij behorende Operating Systemen en Middleware applicaties wordt geregeld door andere partijen.

12.6 Beheer van technische kwetsbaarheden

Met de partners is een beleid ten behoeve van het beheer van technische kwetsbaarheden van de informatiesystemen vastgelegd in de SLA. Hierin wordt ingegaan op het patchbeheer, de communicatie met beheerders en gebruikers en op welke manier mitigerende maatregelen worden vastgesteld.

Het is aan gebruikers verboden zelf software in de informatie verwerkende infrastructuur te installeren.

Wat hierin is toegestaan op mobiele apparatuur is vastgelegd in het BYOD/CYOD Beleid.

12.7 Overwegingen betreffende audits van informatiesystemen

De toetsing van de beveiliging van informatiesystemen en -infrastructuur aan de hand van de BIO is vanaf 2020 onderdeel van de reguliere ENSIA audit.

13. Communicatiebeveiliging

Informatie wordt voortdurend getransporteerd over verschillende soorten netwerken en via andere media. De SED borgt de veiligheid van deze informatie bij binnenkomst, tijdens transport en bij versturen volgens de geldende normen. Hiertoe zijn in de Dienstenovereenkomsten en de SLA's met SSC DeSom en andere partijen beheers-afspraken vastgelegd.

13.1 Beheer van netwerkbeveiliging

De netwerkbeveiliging is belegd bij een andere partij, thans SSC DeSom. SSC DeSom beheert alle netwerkverbindingen van de SED en de Gemeenten, zoals vastgelegd in de Dienstenovereenkomst en de SLA.

SSC DeSom rapporteert hierover aan de SED en stelt verbeteringen voor.

13.2 Informatietransport

Voor de communicatie binnen de SED en de Gemeenten wordt gebruik gemaakt van de beveiligde verbindingen die de SSC DeSom beheert. Deze voldoen aan de juiste veiligheidsnormen.

Voor communicatie met andere overheidsorganisaties wordt gebruik gemaakt van beveiligde verbindingen waarvoor aparte afspraken worden gemaakt met de communicatiepartners. Hierbij worden de aanwijzingen van de IBD gevolgd.

Voor veilige communicatie met burgers en anderen wordt gebruik gemaakt van een veilige website en een veilige email emailfaciliteit. Het gebruik van berichtendiensten is alleen toegestaan in uitzonderlijke gevallen en indien de veiligheid van de berichtendienst is aangetoond.

14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen

De informatie infrastructuur welke de SED gebruikt is ontworpen volgens de principes van “privacy-by-design” en “information-security-by-design”.

Om dit inzichtelijk te maken houdt de SED een (eenvoudig) informatie architectuur schema bij zodat nieuwe informatieprocessen en -faciliteiten een duidelijke plaats kunnen krijgen en ontwikkelingen getoetst kunnen worden.

14.1 Beveiligingseisen voor informatiesystemen

Bij nieuw aan te schaffen informatiesystemen of bij wijzigingen in bestaande wordt altijd een risico analyse uitgevoerd door de projectleider. Indien persoonsgegevens verwerkt worden kan dit in de vorm van een DPIA.

14.2 Beveiliging in ontwikkelings- en ondersteunende processen

Bij de ontwikkeling van de informatie architectuur wordt aangesloten bij bestaande principes en normen en worden de principes van “security-by-design” toegepast. Ontwikkelingen vinden altijd plaats in samenwerking met de leverancier.

Voordat nieuwe, gewijzigde of nieuw ontwikkelde systemen of processen in gebruik worden genomen worden deze uitvoerig getest volgens een vastgestelde methodiek.

14.3 Testgegevens

Voor het testen van informatiesystemen worden sets met testgegevens onderhouden. Deze sets bestaan, indien mogelijk, niet uit gegevens die uit de werkelijkheid afkomstig zijn maar zijn speciaal voor de testdoeleinden samengesteld.

De testgegevens worden, om de continuïteit van de kwaliteit van de gegevensverwerking aan te kunnen tonen, telkens hergebruikt en, indien nodig, aangevuld.

Gestreefd wordt naar het zo veel mogelijk automatiseren van de testprocessen.

15. Leveranciersrelaties

De faciliteiten voor de informatievoorziening heeft de SED in handen gegeven van leveranciers, waarvan SSC DeSom de belangrijkste is. De SED streeft er naar een professionele relatie met alle leveranciers te onderhouden en eisen aan en overleg over informatiebeveiliging is daar onderdeel van.

15.1 Informatiebeveiliging in leveranciersrelaties

Ten behoeve van de inkoop van informatievoorziening gerelateerde zaken is een pakket van eisen opgesteld. DPIA en risicoanalyse maakt daar onderdeel van uit zodat de SED de privacybescherming en informatiebeveiliging mee kan nemen in besluitvorming over aanschaf, ontwikkeling en wijziging.

Met leveranciers worden overeenkomsten afgesloten waar de informatiebeveiliging een duidelijke plaats in heeft, conform de GIBIT standaard. Het niet nakomen van eisen aan de informatiebeveiliging is grond voor het ontbinden van de overeenkomst.

Iedere overeenkomst bevat een exit-strategie welke de continuïteit van de informatievoorziening garandeert. Deze exit-strategie wordt tijdens de looptijd van de overeenkomst tenminste één maal geëvalueerd en, indien mogelijk, geoefend.

15.2 Beheer van dienstverlening van leveranciers

Er wordt een register van overeenkomsten betreffende de informatievoorzieningen bijgehouden waarin de aspecten van de privacy bescherming en informatiebeveiliging worden genoteerd in de vorm van prestatie-indicatoren.

16. Beheer van informatiebeveiligingsincidenten

De SED zal altijd te maken hebben met incidenten in de informatievoorziening. Deze kunnen betrekking hebben op de vertrouwelijkheid van gegevens, op de privacy van personen, de continuïteit van de informatievoorziening en op de integriteit van gegevens. De SED wil leren van deze incidenten. Deze geven wellicht aanleiding tot aanpassingen of maatregelen die incidenten in de toekomst helpen voorkomen.

16.1 Beheer van informatiebeveiligingsincidenten en –verbeteringen

Er is een meldpunt ingericht, en bekend gemaakt, waar medewerkers van de SED en van de Gemeenten (vermoedde) incidenten met de privacybescherming en informatiebescherming kunnen melden.

Medewerkers kunnen deze incidenten melden zonder dat zij daar op aangesproken worden, in tegendeel, zij worden aangesproken op het niet melden van incidenten.

De incidenten worden bijgehouden in een incidentenregister.

Alle incidenten worden met de grootst mogelijke prioriteit onderzocht en beoordeeld. In voorkomende gevallen worden incidenten gemeld aan partners waarna gezamenlijke acties worden afgesproken.

In gevallen waarop dit van toepassing, zoals incidenten met een regionaal of landelijk karakter of incidenten waarvoor gespecialiseerde kennis nodig is, is zal het CERT van de IBD (Computer Emergency Response Team van de Informatie BeveiligingsDienst van de VNG) betrokken worden.

Alle incidenten worden beoordeeld door de CISO die beslist over verder te nemen acties, veelal in samenspraak met de CISO van de beherende partij.

De CISO rapporteert ieder kwartaal over de incidenten aan de directie SED.

17. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

De continuïteit van de informatievoorziening is onderdeel van de informatiebeveiliging. Het niet beschikbaar zijn van informatie wordt gezien als informatiebeveiligingsincident en is, als het om persoonsgegevens gaat, een datalek in de zin van de AVG.

De SED en de Gemeenten hebben de faciliteiten voor de informatievoorziening uitbesteed aan een partner. In de dienstenovereenkomst en de SLA zijn afspraken over de continuïteit van de informatievoorziening opgenomen. De afspraken met alle partners, waaronder de leverancier van de stroomvoorziening, zijn gebundeld in het Informatie-continuïteitsplan dat ieder jaar aan de hand van inzichten en incidenten wordt geëvalueerd en mogelijk bijgesteld.

18. Naleving

Als overheidsinstelling houdt de SED zich aan de wet en kan dat ook aantonen.

Dit uit zich in, onder andere, het aantoonbaar naleven van contractuele eisen, respecteren van intellectuele eigendomsrechten (licenties), het bijhouden en beschermen van registraties en het aanstellen van de juiste functionarissen.

18.1 Naleving van wettelijke en contractuele eisen

Alle informatieprocessen in de SED en de Gemeenten vallen onder een van de domeinmanagers die zich daarmee “proces eigenaar” kan noemen. De proces eigenaar bepaalt hoe er met de gegevens in het proces wordt omgegaan en stelt een bewaartermijn vast.

Voor het toezicht op de juiste verwerking van persoonsgegevens is een Functionaris Gegevensbescherming aangesteld (FG). Deze rapporteert rechtstreeks aan de verwerkingsverantwoordelijke: Voor de Gemeenten het College van B en W, voor de SED de directie SED. De FG heeft het mandaat zijn functie uit te oefenen volgens de wettelijke richtlijnen.

18.2 Informatiebeveiligingsbeoordelingen

Voor de beoordeling van en het overzicht op de informatiebeveiliging is een Information Security Management System (ISMS) geïmplementeerd, waarvoor de CISO verantwoordelijk is. De CISO zorgt voor de reguliere rapportage uit het ISMS aan de directie SED.

Jaarlijks wordt door de directie SED een auditplan opgesteld. Hierin worden extern geïnitieerde audits (zoals de DigiD en SUWInet audits) meegenomen en wordt de ENSIA systematiek gevolgd. Informatiebeveiliging is een vast onderdeel van het auditplan.

Ter ondersteuning van de beoordeling van de audits voert de SED regelmatig controles uit op de informatiebeveiliging. Werkplekinspecties, penetratietests en kwetsbaarheden analyses maken hier onderdeel van uit.

Bijlage 1 Documenten behorende bij het Informatie-BeveiligingsBeleid SED

6 Organiseren van informatiebeveiliging

1. Functieprofiel CISO
2. Functieprofiel ISO
3. Functieprofiel PO
4. Functieprofiel FG
5. Overzicht relaties SED waarmee gegevens worden uitgewisseld en IB maatregelen
6. Regeling mobile devices

7 Veilig personeel

7. Algemene brochure informatiebeveiliging voor personeel SED
8. Project geautomatiseerde koppeling Personeelsinformatiesysteem – ICT infrastructuur
9. Opleidingsplan ICT-vaardigheden en informatiebeveiliging voor het personeel van de SED
10. Klokkenluidersregeling

8 Beheer van bedrijfsmiddelen

11. Gedragscode omgaan met informatie
12. Classificatie van gegevens binnen de SED, inclusief risico afwegingen
13. Registratie van vernietiging van media

9 Toegangsbeveiliging

14. Thuiswerkprotocol
15. CYOD/BYOD beleid en reglement
16. Autorisatiematrix
17. Wachtwoordenbeleid

10 Cryptografie

18. Beleid cryptografie

11 Fysieke beveiliging en beveiliging van de omgeving

19. Voor de fysieke beveiliging wordt aansluiting gevonden in de vigerende beveiligingsplannen voor de gemeenten en de SED. Dit wordt nader ingevuld.
20. Beleid elektronische werkplek. (clear screen etc.)

12 Beveiliging bedrijfsvoering

21. Dienstenovereenkomsten, SLA's en Verwerkingsovereenkomsten partners
22. Testbeleid
23. Backupbeleid

13 Communicatiebeveiliging

24. Overzicht beveiligde communicatiekanalen

14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen

25. Architectuur overzicht informatieverwerking SED
26. Testgegevens

15 Leveranciersrelaties

- 27. Eisen bij inkoop
- 28. Register overeenkomsten informatievoorziening

16 Beheer van informatiebeveiligingsincidenten

- 29. Register incidenten informatiebeveiliging en privacybescherming

17 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

- 30. Informatie-continuïteitsplan

18 Naleving

- 31. Register bewaartermijnen gegevensverzamelingen
- 32. ISMS
- 33. Jaarlijks auditplan