CVDR

Officiële uitgave van Hoeksche Waard.

Nr. CVDR622817_1

29 maart 2019

Besluit van het college van burgemeester en wethouders van de gemeente Hoeksche Waard houdende regels omtrent Tactische richtlijnen Informatiebeveiliging Hoeksche Waard 2019-2020

1 Samenvatting

1.1 Inleiding

Het document "Strategisch Informatiebeveiligingsbeleid Hoeksche Waard 2019-2020" en het document "Tactische richtlijnen Informatiebeveiliging Hoeksche Waard 2019-2020 ", vormen gezamenlijk het nieuwe gemeentelijk framework voor informatiebeveiliging. Het is gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), conform de VNG resolutie (nov 2013) “Informatiebeveiliging, randvoorwaarde voor de professionele gemeente.”

1.2 Werking

- In een separaat document "Strategisch Informatiebeveiligingsbeleid Hoeksche Waard 2019-2020" worden de strategische uitgangspunten en verantwoordelijkheden ten aanzien van de gemeente op het gebied van informatiebeveiliging en gegevensbescherming benoemd, welke als basis dienen voor Tactische richtlijnen.
- Het Strategisch informatiebeveiligingsbeleid treedt in werking na vaststelling door het College van B&W, en is geldig tot eind 2020.

Figuur 1. Relatie Strategisch Informatiebeveiligingsbeleid en Tactische Richtlijnen

- In dit document "Tactische Richtlijnen Informatiebeveiliging Hoeksche Waard", wordt volgens internationale standaarden (NEN/ISO 27002:2005/7 en BIG) het inhoudelijke normenkader beschreven. Hierin staan de normen en maatregelen ten behoeve van risicomanagement en controle die op basis van “pas-toe-leg-uit” gelden voor alle organisatieonderdelen van de gemeente Hoeksche Waard.
- Hiermee kunnen de afzonderlijke organisatieonderdelen Informatiebeveiliging inrichten en aantoonbaar verantwoorden.
- De "Tactische richtlijnen Informatieveilighed Hoeksche Waard" treedt in werking na vaststelling door de Directie.

2 Informatiebeveiligingsbeleid

2.1 Samenvatting Strategisch Informatiebeveiligingsbeleid

Informatie is één van de belangrijkste bedrijfsmiddelen van de gemeente Hoeksche Waard voor het realiseren van de bedrijfsdoelstellingen. Hoe we willen en moeten omgaan met informatie, staat onder invloed van interne ambities (o.a. zaakgericht werken, digitale publieksdienstverlening) en externe ontwikkelingen (o.a. participatiesamenleving, cybercriminaliteit). De **betrouwbaarheid** (beschikbaarheid, integriteit) van informatiesystemen en vertrouwen in informatie (privacy, controleerbaarheid) zijn dan ook van groot belang. Ook burgers, bedrijven en ketenpartners verwachten betrouwbare informatie.

2.1.1Risico’s

We lopen grote bedrijfsrisico's bij verlies van gegevens, uitval van ICT, of het kennisnemen of manipuleren van bepaalde informatie door onbevoegden. Door schaalvergroting en (externe) ketensamenwerking neemt de kans op zulke incidenten toe en de impact ervan is groot. Het kan ernstige (politieke) gevolgen hebben voor burgers, bedrijven, partners en de eigen organisatie. Informatiebeveiliging is daarom van essentieel belang. Daarom is de aanpak van informatiebeveiliging in Hoeksche Waard ‘risk based’.

2.1.2Belang van informatiebeveiliging

Het proces van Informatiebeveiliging zorgt voor de bescherming van de privacy en van vitale maatschappelijke functies waarbij informatie cruciaal is: zoals verkeer, vervoer, openbare orde en beveiliging. Het gaat om informatie in alle verschijningsvormen: elektronisch, op papier en mondeling uitgewisseld. Goede informatiebeveiliging maakt verantwoorde elektronische dienstverlening mogelijk, evenals nieuwe, innovatieve manieren van werken. Het is daarbij een randvoorwaarde dat medewerkers verantwoord en bewust omgaan met bedrijfsinformatie. Het Strategisch Informatiebeveiligingsbeleid is hiertoe het kader.

2.1.3Inhoud Strategisch Informatiebeveiligingsbeleid

Het Strategisch Informatiebeveiligingsbeleid beschrijft verder

- Doel en doelgroepen
- Scope
- Visie op interne en externe ontwikkelingen
- PDCA Proces van informatiebeveiliging
- Organisatie van de informatiebeveiliging
- Verantwoordelijkheden
- Taken en rollen
- Rapportage over Informatiebeveiliging
- ICT crisisbeheersing en samenwerking
- Externe partijen

3 Tactische Richtlijnen

Deze Tactische Richtlijnen helpen de organisatieonderdelen Informatiebeveiliging in te richten en aantoonbaar te verantwoorden, zoals verwoord in het trategisch Informatiebeveiligingsbeleid.

- Het lijnmanagement van organisatieonderdelen is en blijft verantwoordelijk voor informatiebeveiliging.
- Elke lijnmanager beoordeelt via een risicoanalyse welke mensen en middelen nodig zijn om haar werkprocessen en eigendommen aantoonbaar te kunnen beveiligen volgens het Strategische beleid met behulp van deze Tactische Richtlijnen Informatiebeveiliging.

3.1 Pas toe of leg uit

Het "Pas toe of leg uit" beginsel betekent dat organisatieonderdelen alleen mogen afwijken van deze richtlijnen ingeval van redenen van bijzonder gewicht, rekening houdend met de wet.

- Organisaties leggen afwijkingen gemotiveerd vast in de administratie om zich te allen tijde over de mate van naleving aantoonbaar te verantwoorden in het jaarverslag.
- Voorgenomen uitzonderingen op deze Tactische Richtlijnen worden ter beoordeling voorgelegd aan de adviseur Informatiebeveiliging (CISO).
- Geaccepteerde uitzonderingen zijn toegelaten tot de eerst volgende herziening van het Informatiebeveiligingsbeleid en worden op dat moment opnieuw beoordeeld.
- Minimaal elke 4 jaar zullen de doelstellingen in beleid en richtlijnen worden geëvalueerd en indien er wijzigingen nodig blijken wordt een nieuwe versie gepubliceerd.

4 Risicobenadering

Een integrale risicobenadering maakt besturing van informatiebeveiliging vanuit de bedrijfslaag mogelijk richting processen, applicatielaag en technische laag. De bedrijfsdoelstellingen benadrukken **betrouwbaarheid** en **vertrouwen** in de samenwerking met mensen om een optimale participatie en bedrijfsefficiency te behalen.

- De proceseigenaar identificeert de kwetsbaarheid van zijn werkproces en de dreigingen die kunnen leiden tot een beveiligingsincident, rekening houdend met de beschermingseisen van de informatie.
- Het kwaliteitsniveau van **betrouwbaarheid** (beschikbaarheid, integriteit) en **vertrouwen** (vertrouwelijkheid, controleerbaarheid, onweerlegbaarheid) voor proces en informatiesystemen wordt op de bedrijfslaag vastgesteld met een bedrijfsimpactanalyse (BIA).
- De uitkomst van deze risicoanalyses bepaalt welke normen en maatregelen moeten worden toepast om relevante dreigingen te beheersen op het gebied van mensen, apparatuur, programmatuur, gegevens, omgeving, organisatie en diensten (MAPGOOD).
- Indien een proces of informatiesysteem gevoelige gegevens bevat (persoonlijk, medisch, financieel), wordt een Privacy Impact Analyse (PIA) uitgevoerd en de doelbinding van de gegevensverzameling vastgelegd.

Voor een nadere uitwerking zie hoofdstuk Gebruik van middelen, onderwerp classificaties.

5 Gebruik van middelen en informatie

Bereiken en handhaven van een passende bescherming van middelen en gemeentelijke informatie.

5.1 Risico's

- Bedrijfsmiddelen en informatie zijn blootgesteld aan risico's zoals diefstal, beschadiging of onoordeelkundig gebruik, waarbij niet voor alle ICT-configuratie items is vastgelegd wie de eigenaar/hoofdgebruiker is.
- Onduidelijkheid wie verantwoordelijk is voor gegevensbestanden, waardoor ook niemand verantwoordelijk is voor de beveiliging en kan optreden bij incidenten.

5.2 Het gebruik van (privé)middelen en gemeentelijke informatie

- Medewerkers dienen bij het gebruik van ICT-middelen, social media en gemeentelijke informatie de nodige zorgvuldigheid te betrachten en de integriteit en goede naam van de gemeente te waarborgen.
- Medewerkers gebruiken gemeentelijke informatie primair voor het uitvoeren van de aan hen opgedragen taken en het doel waarvoor de informatie is verstrekt.
- Privégebruik van gemeentelijke informatie en bestanden is niet toegestaan.
- Werken op afstand en het gebruik van privé middelen is toegestaan mits medewerkers zich houden aan de bepalingen van de Reglement gebruik e-mail, internet en social media en overige ICT-middelen.
- De medewerker is gehouden aan de regels, zoals:
  - Illegale software mag niet worden gebruikt voor de uitvoering van het werk.

- Er bestaat geen plicht de eigen computer te beveiligen, maar de gemeentelijke informatie daarop wel.
- Het verbod op ongewenst gebruik in de (fysieke) kantooromgeving geldt ook als dat via de eigen computer plaatsvindt.

- De medewerker neemt passende technische en organisatorische maatregelen om gemeentelijke informatie te beveiligen tegen verlies of tegen enige vorm van onrechtmatig gebruik. De medewerker houdt hierbij in ieder geval rekening met:
  - de beveiligingsclassificatie van de informatie (zie hieronder);
  - de door de gemeente gestelde beveiligingsvoorschriften (o.a. dit beleid);
  - aan de werkplek verbonden risico's (o.a. meekijken, afluisteren);
  - het risico door het benaderen van gemeentelijke informatie met andere dan door de gemeente verstrekte of goedgekeurde ICT-apparatuur.

5.3 Classificatie

5.3.1Risico's

- Geen inzicht in welke informatie en informatiesystemen het belangrijkst zijn voor de primaire processen.
- Onjuiste classificatie draagt bij aan het onjuist beschermen van informatie en bedrijfsmiddelen met als risico, dat deze verloren kunnen gaan of openbaar worden gemaakt terwijl dat niet de bedoeling is.

5.3.2Beheersmaatregelen

Classificatie maakt het vereiste beschermingsniveau zichtbaar en maakt direct duidelijk welke maatregelen nodig zijn. Er wordt geclassificeerd op drie betrouwbaarheidsaspecten van informatie: Beschikbaarheid, Integriteit (juistheid, volledigheid) en Vertrouwelijkheid (BIV). De principes Controleerbaarheid en Onweerlegbaarheid worden separaat getoetst indoen nodig.

Er zijn vier beschermingsniveaus van laag naar hoog, zoals in onderstaande tabel weergegeven.

Niveau	Beschikbaarheid	Integriteit	Vertrouwelijkheid
Geen	**Nietnodig** gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn	**Nietzeker** informatie mag worden veranderd *(schrijfrechten)*	**Publiek of Openbaar**informatie mag door iedereen worden ingezien (leesrechten) *(bv: www.gemeentehw.nl)*
Laag	**Noodzakelijk of 1 week** informatie mag incidenteel niet beschikbaar zijn	**Beschermd** het bedrijfsproces staat enkele (integriteits-)fouten toe	**Intern of Bedrijfsvertrouwelijk**informatie is toegankelijk voor alle medewerkers van de organisatie voor uitvoeren bedrijfsprocessen
Midden	**Belangrijk of 1 dag**informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk *(bv: primaireprocesinformatie)*	**Hoog** het bedrijfsproces staat zeer weinig fouten toe *(bv: [illegible])*	**Vertrouwelijk** informatie is alleen toegankelijk voor een specifieke en beperkte groep gebruikers en/of periode *(bv: financiële (persoons)gegevens)*
Hoog	**Essentieel of 4 uur**informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten *(bv: basisregistraties)*	**Absoluut** het bedrijfsproces staat geen fouten toe	**Geheim** informatie is alleen toegankelijk voor beperkte groep direct geadresseerde(n) *(bv: zorggegevens en strafrechtelijke informatie)*

Tabel 2: Classificatieniveaus

- De eigenaar van de gegevens (veelal ook de proceseigenaar) bepaalt het vereiste beschermingsniveau (classificatie). Indien sprake is van wettelijke eisen wordt dit expliciet aangegeven. De eigenaar van de gegevens bepaalt wie toegang krijgt tot welke gegevens.

- De bronhouder van basisregistraties heeft een doorslaggevende stem als het gaat om toegang tot informatie uit de basisregistraties. De bronhouder moet bij classificaties in projecten en processen zoals “Open, tenzij”, “Open Data” en “Big Data” betrokken worden.
- De CISO classificeert op het niveau van processen, informatie en informatiesystemen. Classificaties van alle bedrijfskritische systemen zijn centraal vastgelegd door de CISO en worden jaarlijks gecontroleerd door alle Organisatieonderdelen.
- Classificatie beoogt een balans tussen risico’s en kosten voor tegenmaatregelen. Indien naar verhouding met geringe extra kosten meer beveiliging kan worden bewerkstelligd, bv door standaardisatie, geldt dit als “best passend”.

6 Personeel

Reducerenvanhetrisicovandiefstal,fraudeofmisbruikvanfaciliteitenenbewerkstelligendat medewerkers hun verantwoordelijkheden begrijpen.

6.1 Risico’s

- Het aannemen of inhuren van nieuw personeel en het laten verrichten van werkzaamheden door externe medewerkers verdient extra aandacht, omdat menselijk falen en bedreigingen van menselijke aard significante invloed kunnen hebben op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie.
- Het laat of niet melden van uitdienst treden, functiewijziging, of innemen van bedrijfsmiddelen kan leiden tot ongeautoriseerde toegang tot informatie en onnodige kosten van ongebruikte licenties, beheer en middelen

6.2 Organisatorische aspecten

- Het lijnmanagement is verantwoordelijk voor het juist afhandelen van de beveiligingsaspecten van het aangaan, wijzigen en beëindigen van een dienstverband of een overeenkomst met externen. HRM is kadersteller en houdt toezicht op dit proces.
- Bij beëindiging van het dienstverband of functie (bij interne overplaatsing) en beëindiging van inhuur worden alle bedrijfsmiddelen van de organisatie geretourneerd. Autorisaties worden in opdracht van het lijnmanagement onmiddellijk geblokkeerd.
- Medewerkers die werken met vertrouwelijke of geheime informatie overleggen voor indiensttreding een Verklaring Omtrent het Gedrag (VOG). De VOG wordt indien nodig herhaald tijdens het dienstverband.
- Het lijnmanagement bepaalt welke rol(len) de medewerker moet vervullen en welke autorisaties voor het raadplegen, opvoeren, muteren en afvoeren van gegevens moeten worden verstrekt.
- Alle medewerkers (en voor zover van toepassing externe gebruikers van onze systemen) dienen training te krijgen in procedures en/of voorlichting over procedures die binnen hun Organisatieonderdeel gelden voor informatiebeveiliging. Deze training en/of voorlichting dient regelmatig te worden herhaald om het beveiligingsbewustzijn op peil te houden.
- Bij inbreuk op de beveiliging gelden voor medewerkers de gebruikelijke disciplinaire maatregelen, zoals onder meer genoemd in het Ambtenarenreglement en de Regeling ICT en Informatiegebruik.
- Regels die volgen uit dit beleid gelden ook voor externen die in opdracht van de gemeente Hoeksche Waard werkzaamheden uitvoeren.

6.3 Bewustwording

- Het concern bevordert algehele communicatie en bewustwording informatiebeveiliging.
- Het lijnmanagement bevordert alle dat medewerkers zich houden aan beveiligingsrichtlijnen. Afspraken hierover worden vastgelegd in het management contract.
- In werkoverleggen wordt periodiek aandacht geschonken aan informatiebeveiliging. Voor zover relevant worden hierover afspraken vastgelegd in planningsgesprekken.

7 Fysieke beveiliging

Hetvoorkomenvanonbevoegdefysieketoegangtot,schadeaanofverstoringvanhetterreinen de informatie van de organisatie.

7.1 Risico's

- Onbevoegde toegang tot kritieke systemen of waardevolle informatie. Bij het ontbreken van registratie zijn incidenten bovendien niet herleidbaar tot individuen.
- Door bijvoorbeeld de inzet van externen, de toeloop van leveranciers en andere niet- medewerkers of het feit dat de medewerkers op meerdere locaties op geruime afstand van elkaar gevestigd zijn, is het betrekkelijk eenvoudig voor niet-medewerkers om toegang tot de panden te krijgen door tegelijk met een geautoriseerde medewerker naar binnen te gaan.
- Als informatie zichtbaar op bureaus ligt, is er een risico m.b.t. de vertrouwelijkheid.
- Geen procedures voor het veilig verwijderen of hergebruiken van ICT-apparatuur.
- Bescherming van apparatuur, waaronder apparatuur die buiten de locatie wordt gebruikt en het verwijderen van bedrijfseigendommen, is noodzakelijk om het risico van toegang door onbevoegden tot informatie te verminderen en om de apparatuur en informatie te beschermen tegen verlies of schade.

7.2 Beheersmaatregelen

- De beheersmaatregelen zijn in overeenstemming met het "Strategisch informatiebeveiligingsbeleid Hoeksche Waard 2019-2020"
- De schade aan informatiesystemen door bedreigingen van buitenaf (zoals brand, overstroming, explosies, oproer, stroomonderbreking) wordt beperkt door passende preventieve maatregelen.
- In diverse panden van de gemeente wordt gebruik gemaakt van cameratoezicht. Het maken en gebruiken van beeldmateriaal is beperkt door de AVG en nadere regels.
- De fysieke toegang tot ruimten waar zich informatie en ICT-voorzieningen bevinden is voorbehouden aan bevoegd personeel. Registratie van de verleende toegang ondersteunt de uitvoering van de toegangsregeling.
- Serverruimtes, datacenters en daar aan gekoppelde bekabelingsystemen zijn ingericht in lijn met geldende 'best practices'.
- (Data) verbindingen worden beschermd tegen interceptie of beschadiging.
- Reserve apparatuur en back-ups zijn gescheiden in twee datacenters, om de gevolgen van een calamiteit te minimaliseren.
- Gegevens en programmatuur worden van apparatuur verwijderd of veilig overschreven voordat de apparatuur wordt afgevoerd. Informatie wordt bewaard en vernietigd conform de Archiefwet 1995 en de daaruit voortvloeiende Archiefbesluiten.

8 Beveiliging van apparatuur en informatie

Waarborgenvaneencorrectenveiliggebruikvan ICTvoorzieningen

8.1 Risico's

- Het ontbreken van documentatie kan leiden tot fouten, niet-uniforme wijze van gegevensinvoer, of in geval de beheerder/bediener uitvalt, tot problemen rondom de continuïteit.
- Onjuiste autorisaties kunnen leiden tot foutieve handelingen, fraude en verduistering.
- Het niet uitvoeren en vastleggen van technische en functionele applicatietesten en/of de resultaten hiervan, kan in bepaalde omstandigheden (tijdsdruk, vakantieperiodes, etc.) leiden tot een verhoogd risico van uitval of gegevens verlies.
- De gemeente gaat steeds meer samenwerken (en informatie uitwisselen) in ketens en besteedt meer taken uit. Bij beheer van systemen en gegevens door een derde partij, kan ook informatie van de gemeente op straat komen te liggen. De gemeente blijft verantwoordelijk voor de informatiebeveiliging van haar gegevens in dat deel van de keten, waarbij het beheer bij een andere partij ligt.
- Programmatuur en ICT-voorzieningen zijn kwetsbaar voor virussen.
- Het ontbreken van een regeling voor antivirus bescherming bij medewerkers thuis leidt tot hogere beveiligingsrisico's.

8.2 Beheersmaatregelen

8.2.1 Organisatorische aspecten

- In beginsel mag niemand autorisaties hebben om een gehele cyclus van handelingen in een informatiesysteem te beheersen, zodanig dat beschikbaarheid, integriteit of vertrouwelijkheid

kan worden gecompromitteerd. Indien dit toch noodzakelijk is dient een audit trail te worden vastgelegd van alle handelingen en tijdstippen in het proces, dusdanig dat transactie kan worden herleid. De audit trail is niet toegankelijk voor degene wiens handelingen worden vastgelegd.
- Er is een aantoonbare scheiding tussen beheertaken en overige gebruikstaken. Beheerwerkzaamheden worden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker.
- Bij externe hosting van data en/of services (uitbesteding, cloud computing) blijft de gemeente Hoeksche Waard eindverantwoordelijk voor de betrouwbaarheid van uitbestede diensten. Dit is gebonden aan regels en vereist goede (contractuele) afspraken en controle hierop (zie Strategisch Informatiebeveiligingsbeleid hoofdstuk 5, 'externe partijen').
- Externe hosting van data en/of services dienen als project te worden behandeld:
  - Aanmelding bij het governance proces
  - Goedgekeurd door het lijnmanagement
  - In overeenstemming met Wet- en regelgeving, Informatiebeveiligingsbeleid en algemeen gemeentelijk beleid;
  - Voldoen aan de eisen voor externe hosting: bv risicoanalyse, dataclassificatie zijn verplicht
  - Vooraf gemeld bij ICT t.b.v. toetsing op beheeraspecten

8.2.2Systeemplanning en –acceptatie
- Nieuwe systemen, upgrades en nieuwe versies worden getest op impact en gevolgen en pas geïmplementeerd na formele acceptatie en goedkeuring door de opdrachtgever (veelal de proceseigenaar). De test en de testresultaten worden in de regel gedocumenteerd.
- Systemen voor ontwikkeling, test en acceptatie (OTA) zijn logisch gescheiden van Productie (P) om onbevoegde toegang tot of wijzigingen in productiesystemen te voorkomen.
- In de OTA worden test accounts gebruikt. Er wordt in beginsel niet getest met productie accounts, tenzij voor de test absoluut noodzakelijk en dan met instemming van de proceseigenaar.
- Vertrouwelijke of geheime data uit de productieomgeving mag in principe niet worden gebruikt in de ontwikkel-, test-, opleidings-, en acceptatieomgeving tenzij de gegevens zijn geanonimiseerd of gepseudonimiseerd. Indien het toch noodzakelijk is om data uit productie te gebruiken is uitdrukkelijke toestemming van de eigenaar van de gegevens vereist.
- Het gebruik van ICT middelen wordt gemonitord ten behoeve van een tijdige aanpassing van de beschikbare capaciteit aan de vraag.

8.2.3Technische aspecten
- Alle gegevens anders dan classificatie 'geen' worden versleuteld conform beveiligingseisen in de Informatiebeveiliging architectuur.
  - Classificatieniveau 'laag': transportbeveiliging buiten het Hoeksche Waardse netwerk
  - Classificatieniveau 'midden': transport en berichtbeveiliging
  - Classificatieniveau 'hoog': transport, berichtbeveiliging en versleuteling bij opslag

- Versleuteling vindt plaats conform best practices (de stand der techniek), waarbij geldt: de vereiste encryptie is sterker naarmate gegevens gevoeliger zijn.
- Gegevens op papier worden beschermd door een deugdelijke opslag en regeling voor de toegang tot archiefruimten.
- Bij het openen of wegschrijven van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. Ook inkomende en uitgaande e-mails worden hierop gecontroleerd. De update voor de detectiedefinities vindt in beginsel dagelijks plaats.
- Op verschillende niveaus binnen de ICT-infrastructuur (netwerkcomponenten, servers, pc's) wordt antivirus software van verschillende leveranciers toegepast.
- Alle apparatuur die is verbonden met het netwerk van de gemeente Hoeksche Waard moet worden geïdentificeerd.
- 'Mobile code' wordt uitgevoerd in een logisch geïsoleerde omgeving om de kans op aantasting van de integriteit van het systeem te verkleinen. De mobile code wordt altijd uitgevoerd met minimale rechten zodat de integriteit van het host systeem niet aangetast wordt.
- Documenten, opslagmedia, in- en uitvoergegevens en systeemdocumentatie worden beschermd tegen onbevoegde openbaarmaking, wijziging, verwijdering en vernietiging.
- Het (ongecontroleerd) kopiëren van 'geheime' gegevens is niet toegestaan, behalve voor back-up door bevoegd systeembeheer.

- Alle informatie die wordt geplaatst op websites van de gemeente wordt beschermd tegen onbevoegde wijziging. Op algemeen toegankelijke websites wordt alleen openbare informatie gepubliceerd.

- Groepen informatiediensten, gebruikers en informatiesystemen worden op het netwerk gescheiden zodat de kans op onbevoegde toegang tot gegevens verder wordt verkleind.
- Afhankelijk van de risico's die verbonden zijn aan on line transacties worden maatregelen getroffen om onvolledige overdracht, onjuiste routing, onbevoegde wijziging, openbaarmaking, duplicatie of weergave te voorkomen.
- Het netwerk wordt gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de betrouwbaarheid van het netwerk niet onder het afgesproken minimum niveau (service levels) komt.

8.2.4Mobiele (privé)apparatuur en thuiswerkplek

- Beveiligingsmaatregelen hebben betrekking op zowel door de gemeente verstrekte middelen als privé apparatuur (BYOD: 'bring your own device'). Op privé apparatuur waarmee verbinding wordt gemaakt met het Hoeksche Waardse netwerk is de gemeente bevoegd om beveiligingsinstellingen af te dwingen. Het betreft installatie van een beveiligde container (zero footprint) of VDI software. In andere gevallen betreft het onder meer: controle op wachtwoord, encryptie, aanwezigheid van malware, etc. Het gebruik van privé apparatuur waarop beveiligingsinstellingen zijn verwijderd ('jailbreak', 'rooted device') is niet toegestaan.
- Op verzoek van de gemeente dienen medewerkers de installatie van software om bovenstaande beleidsregel te handhaven toe te staan (denk bijvoorbeeld aan 'mobile device management software'). De beveiligingsinstellingen, zoals bedoeld in bovenstaande regel, zijn uitsluitend bedoeld ter bescherming van gemeentelijke informatie en integriteit van het gemeentelijke netwerk.
- In geval van dringende redenen kunnen noodmaatregelen worden getroffen, zoals wissen van apparatuur op afstand. Deze noodmaatregelen kunnen, voor zover dit noodzakelijk is, betrekking hebben op privé-middelen en privé-bestanden.

8.2.5Back up en recovery

- In opdracht van de gegevenseigenaar, maakt de Organisatie eservekopieën van alle essentiële bedrijfsgegevens en programmatuur zodat de continuïteit van de gegevensverwerking kan worden gegarandeerd.
- De omvang en frequentie van de back-ups is in overeenstemming met het belang van de data voor de continuïteit van de dienstverlening en de interne bedrijfsvoering, zoals gedefinieerd door de eigenaar van de gegevens (de classificatietabel is leidraad).
- Bij ketensystemen dient het back-up mechanisme de data-integriteit van de informatieketen te waarborgen.
- De back-up en herstelprocedures worden regelmatig (tenminste 1 x per jaar) getest om de betrouwbaarheid ervan vast te stellen.

8.2.6Informatie-uitwisseling

- Digitale documenten van de gemeente waar burgers en bedrijven rechten aan kunnen ontlenen maken gebruik van PKI Overheid certificaten voor tekenen en/of encryptie.
- Er is een (spam) filter geactiveerd voor inkomende e-mail berichten.

8.2.7Logging en Controle

- Het gebruik van informatiesystemen, alsmede uitzonderingen en informatiebeveiligings- incidenten worden vastgelegd in logbestanden, op een manier die in overeenstemming is met het risico en zodanig dat tenminste wordt voldaan aan alle relevante wettelijke eisen. Relevante zaken om te loggen zijn:
  - type gebeurtenis (zoals back up/restore, reset wachtwoord, betreden ruimte, toegang tot (geclassificeerde) informatie, wijzigen van informatie en verwijderen van informatie);
  - handelingen met speciale bevoegdheden;
  - (pogingen tot) ongeautoriseerde toegang;
  - systeemwaarschuwingen;
  - (poging tot) wijziging van de beveiligingsinstellingen.

- Een logregel bevat minimaal:
  - een tot een natuurlijk persoon herleidbare gebruikersnaam of ID;
  - de gebeurtenis;
  - waar mogelijk de identiteit van het werkstation of de locatie;
  - het object waarop de handeling werd uitgevoerd;
  - het resultaat van de handeling;
  - de datum en het tijdstip van de gebeurtenis.

- In een logregel worden alleen de voor de rapportage noodzakelijke gegevens opgeslagen.

- Er worden maatregelen getroffen om te verzekeren dat gegevens over logging beschikbaar blijven en niet gewijzigd kunnen worden door een gebruiker of systeembeheerder. De wettelijke bewaartermijn is 6 maanden.
- Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers. Hierbij is de toegang beperkt tot leesrechten.
- Logbestanden worden regulier beoordeeld en over afwijkingen wordt in de lijn gerapporteerd.

8.3 Beheer van dienstverlening door een derde partij

Een passend niveau van informatiebeveiliging implementeren en bijhouden en dit vastleggen in een (verwerkers)overeenkomst, contracten en/ofconvenanten.

De organisatie controleert de implementatie van de maatregelen, die zijn vastgelegd in overeenkomsten, bewaakt de naleving van de overeenkomsten en beheert wijzigingen om te waarborgen dat de beveiliging aan alle eisen voldoet, die met de derde partij zijn overeengekomen.

8.3.1Risico's

- De gemeente gaat steeds meer samenwerken en informatie uitwisselen in ketens en besteedt meer taken uit. Bij beheer van systemen en gegevens door een derde partij kan ook informatie van de gemeente op straat komen te liggen. De gemeente blijft verantwoordelijk voor de informatiebeveiliging van haar gegevens in dat deel van de keten, waarbij het beheer bij een andere partij ligt.

8.3.2Beheersmaatregelen

- De beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de (verwerkers)overeenkomst voor dienstverlening door een derde partij worden geïmplementeerd en uitgevoerd.
- De diensten, rapporten en registraties, die door de derde partij worden geleverd, worden gecontroleerd en beoordeeld en er worden periodiek audits uitgevoerd.
- Wijzigingen in de dienstverlening door derden, in bijvoorbeeld bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging, worden beheerd.

8.3.3Uitgangspunten

- In de DVO voor dienstverlening is aandacht besteed aan informatiebeveiliging.
- Er is een basiscontract voor de toegang tot de ICT-voorzieningen en/of de informatievoorziening (bestanden, gegevens) door derden waarin kaders staan voor de toegang tot ICT-voorzieningen door derden. In contractbeheer, applicatiebeheer en functioneel beheer is naleving van de gemaakte afspraken opgenomen.
- Programmatuur en ICT-voorzieningen zijn kwetsbaar voor virussen.
- Het ontbreken van een regeling voor antivirus bescherming bij medewerkers thuis leidt tot hogere beveiligingsrisico's.

8.4 Behandeling van media

Voorkomen van onbevoegde openbaarmaking, modificatie, verwijdering of vernietigingvan informatie en bedrijfsmiddelen.

Media worden beheerst en fysiek beschermd.

Vastgestelde procedures om documenten, opslagmedia (bijvoorbeeld USB-sticks, back-up tapes, schijven),in-en uitvoergegevensensysteemdocumentatietebeschermentegenonbevoegde openbaarmaking, wijziging, verwijdering en vernietiging.

8.4.1Risico's

- Verwijderbare media kan informatie bevatten, die in onbevoegde handen kan vallen bij onjuist gebruik, verlies of diefstal.

8.4.2Beheersmaatregelen

- Er dienen procedures te worden vastgesteld voor het beheer van verwijderbare media.
- Er dienen procedures te worden vastgesteld voor het op een veilige manier verwijderen van media als ze niet langer nodig zijn.
- Systeemdocumentatie dient te worden beschermd tegen onbevoegde toegang.

8.4.3Uitgangspunten

- Er zijn procedures voor het beheer van verwijderbare media en voor het veilig verwijderen of hergebruiken van ICT-apparatuur.
- Harde schijven en andere media worden adequaat gewist of vernietigd bij afstoting of hergebruik. In ieder geval indien er vertrouwelijke informatie is opgeslagen en/of licentie plichtige programmatuur op is geïnstalleerd.
- Er zijn richtlijnen voor het opbergen van papieren en computermedia. In ieder geval voor gevoelige of kritieke bedrijfsinformatie.
- Innamebeleid voor mobiele apparatuur , zoals laptops, pda's, iPads, voor wanneer deze niet meer worden gebruikt.
- Encryptie op informatie met het classificatielabel vertrouwelijk en zeer geheim.

8.5 Uitwisseling van informatie

Handhaven van beveiliging van informatie en programmatuur, die wordt uitgewisseld binneneen organisatie en met enige externe entiteit.

Een formeel uitwisselingsbeleid m.b.t. de uitwisseling van informatie en programmatuur tussen organisaties, dat in lijn is met de uitwisselingsovereenkomsten en relevantewetgeving.

Vastgesteldeproceduresennormenterbeschermingvaninformatieenfysiekemedia,die informatie bevatten die wordt getransporteerd.

8.5.1Risico's

- Verlies of diefstal van laptops, USB-sticks, iPads e.d., waarbij bovendien informatie in verkeerde handen komt.

8.5.2Beheersmaatregelen

- Vaststellen formeel beleid, formele procedures en formele beheersmaatregelen om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen.
- Vaststellen overeenkomsten voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.
- Beschermingsmaatregelen voor media die informatie bevatten tegen onbevoegde toegang, misbruik of het corrumperen tijdens transport buiten de fysieke begrenzing van de organisatie.
- Bescherming van informatie, die een rol speelt bij elektronische berichtuitwisseling.

8.5.3Uitgangspunten

- Gevoelige informatie (classificatie vertrouwelijk en zeer geheim) wordt nooit bekend gemaakt via telefoon of fax, in verband met bijvoorbeeld afluisteren.
- Geformaliseerde situatie rondom het transport van de back-ups en de mogelijkheden van leveranciers om toegang tot het netwerk te verkrijgen.
- Een basisraamwerk met randvoorwaarden voor gegevensuitwisseling met ketenpartners.
- Bewustzijn en sociale controle om het risico op het lekken van informatie via telefoon e.d. te laten afnemen.

9 Logische toegangsbeveiliging

Beheersen van de toegang tot informatie, ICT-voorzieningen en bedrijfsprocessen op grondvan bedrijfsbehoeften en beveiligingseisen.

9.1 Risico's

- Wanneer toegangsbeheersing niet expliciet gebaseerd is op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en/of een aanvullende risicoanalyse, is niet duidelijk of het juiste niveau van beveiliging wordt gehanteerd.
- Verstoringen door onjuist gebruik van ICT-ruimtes of ICT-componenten (m.n. waar ook niet ICT-teams toegang hebben).

Logische toegang is primair gerelateerd aan de classificatie van de informatie. De identiteit van een gebruiker die toegang krijgt tot gemeentelijke informatie dient eerst te worden vastgesteld.

9.2 Uitgangspunten

- De eigenaar van de data is bevoegd toegang te verlenen
- Voor applicaties waarin vertrouwelijke informatie wordt verwerkt, bepaalt de eigenaar van de voorzieningen een autorisatiematrix voor gebruikers, rekening houdend met persoonlijke identificatie, rollen en functiescheiding.
- Accounts zijn persoonsgebonden. Er worden in de regel geen “algemene” identiteiten gebruikt. Voor herleidbaarheid en transparantie is het namelijk nodig om te weten wie een bepaalde actie heeft uitgevoerd. Indien dit geen (wettelijke) eis is kan worden gewerkt met functionele accounts. Daarvoor zijn richtlijnen opgesteld.
- De Gemeente Hoeksche Waard maakt (waar mogelijk) gebruik van bestaande (landelijke) voorzieningen voor authenticatie, autorisatie en informatiebeveiliging (zoals: DigiD en eHerkenning). Intern is de Personeels Informatie en Management Systeem (PIMS) de bron voor identiteiten.

9.3 Authenticatie en autorisatie

- Wachtwoorden worden voor een beperkte periode toegekend (maximaal 6 maanden). Wachtwoorden dienen aan eisen van complexiteit te voldoen, deze worden afgedwongen door het systeem. Voor medewerkers met speciale bevoegdheden (systeem en functioneel beheerders) gelden strengere eisen.
- De gebruiker is verantwoordelijk voor het geheim blijven van zijn wachtwoord.
- Authenticatiemiddelen zoals wachtwoorden worden beschermd tegen inzage en wijziging door onbevoegden tijdens transport en opslag (encryptie).
- Autorisatie is zoveel mogelijk rol gebaseerd. Autorisaties worden toegekend via functie(s) en organisatie onderdelen.
- Toegang tot informatie met classificaties ‘midden’ of ‘hoog’ vereist ‘multifactor’ authenticatie (bijv. naam/wachtwoord + token).
- Voor toegang tot een virtuele werkplek (VDI) of externe toegang is ‘multifactor’ authenticatie (bijv. naam/wachtwoord + token) vereist.

9.4 Externe toegang

- Een Organisatieonderdeel kan een externe partij toegang verlenen tot het gemeentelijke netwerk. Hiervoor geldt de procedure aanvragen externe toegang. Externe partijen kunnen niet op eigen initiatief verbinding maken met het besloten netwerk van de gemeente, tenzij uitdrukkelijk overeengekomen.
- De externe partij is verantwoordelijk voor authenticatie en autorisatie van haar eigen medewerkers. De gemeente Hoeksche Waard heeft het recht hierop te controleren.

9.5 Mobiel en thuiswerken

- Voor werken op afstand is een virtuele thuiswerkomgeving beschikbaar. Toegang tot vertrouwelijke informatie wordt verleend op basis van multifactor authenticatie.
- Onbeheerde apparatuur (privé apparaten of de ‘open laptop’) kan gebruik maken van beveiligde draadloze toegangspunten (WIFI). Deze zijn logisch gescheiden van het Hoeksche Waardse bedrijfsnetwerk.
- Mobiele bedrijfsapplicaties worden bij voorkeur zo aangeboden dat er geen gemeentelijke informatie wordt opgeslagen op het mobiele apparaat (“zero footprint”). Gemeentelijke informatie dient te worden versleuteld bij transport en opslag conform classificatie eisen.
- Voorzieningen als externe e-mail, webmail, sociale netwerken en clouddiensten (dropbox, gmail, etc.) zijn door het lage beschermingsniveau (veelal alleen naam en wachtwoord, of het ontbreken van versleuteling of externe opslag) niet geschikt voor het delen van vertrouwelijke en geheime informatie.

9.6 Overige maatregelen

- Het fysieke (bekabelde) netwerk is niet toegankelijk voor onbeheerde apparatuur.
- Het netwerk van de gemeente Hoeksche Waard is gesegmenteerd (werkplekken voor gebruikers en serversystemen zijn logisch gescheiden)
- Tussen segmenten met verschillende beschermingsniveaus worden filters (bv Firewalls, Access Control Lists –ACLs of IPS) geïmplementeerd.

10 Beveiliging van informatiesystemen (software)

Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.

10.1 Risico's

- Fouten, verlies, onbevoegde modificatie of misbruik van informatie in toepassingen.
- Onvoldoende bescherming van de vertrouwelijkheid, authenticiteit of integriteit van informatie.

10.2 Organisatorische aspecten

- Toetsing op Informatiebeveiligingsbeleid is onderdeel van de architectuurtoets voor projecten met een ICT component en onderdeel van de project start en eind architectuur (Architectuurparagraaf, PSA en PEA).
- Projectmandaten worden voorzien van een advies op informatiebeveiliging.
- In het programma van eisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen worden ook relevante beveiligingeisen opgenomen.

10.3 Softwareontwikkeling en onderhoud

- Applicaties worden ontwikkeld en getest o.b.v. landelijke richtlijnen voor beveiliging, Secure Software Development (SSD) en zoals richtlijnen voor beveiliging van webapplicaties. Er wordt bij implementatie, veranderingen en minimaal jaarlijks tenminste getest op bekende kwetsbaarheden zoals vastgelegd in de OWASP top 10.
- Webapplicaties van derden waarop content van gemeente Hoeksche Waard wordt getoond moeten eveneens voldoen aan richtlijnen voor beveiliging van webapplicaties (NCSC). Tevens gelden de richtlijnen voor externe toepassingen.
- Webapplicaties worden voor in productie name onder meer getest op invoer van gegevens (grenswaarden, format, inconsistentie, SQL injectie, etc.).
- De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen (bijv. door checksums).
- Alleen gegevens die noodzakelijk zijn voor de gebruiker worden in de applicatie gepresenteerd ('uitgevoerd'), rekening houdend met beveiligingseisen (classificatie).
- Toegang tot broncode is beperkt medewerkers die deze code onderhouden of installeren.
- Technische kwetsbaarheden worden regulier met een minimum van 2 keer per jaar gerepareerd door 'patchen' van software, of ad hoc bij acute dreiging. Welke software wordt geupdate wordt mede bepaald door de risico's.

10.4 Encryptie (versleuteling)

- De gemeente Hoeksche Waard gebruikt encryptie conform PKIoverheid standaard.
- Beveiligingscertificaten worden centraal beheerd door de Organisatie.

11 Beveiligingsincidenten

Bewerkstelligen dat (informatiebeveiliging) incidenten zodanig kenbaar worden gemaakt dat tijdig maatregelen kunnen worden genomen.

11.1 Risico's

- Als incidenten niet geregistreerd worden, is niet duidelijk waar en wanneer er zich incidenten voor doen of voor hebben gedaan. Op deze wijze kan er geen lering worden getrokken uit deze incidenten om deze in de toekomst te voorkomen of om preventief betere maatregelen te implementeren.

11.2 Melding en registratie

- De medewerker dient geconstateerde of vermoede beveiligingslekken en beveiligingsincidenten direct te melden bij de adviseur Informatiebeveiliging (CISO).

- Beveiligingsincidenten worden gemeld bij de ICT service desk en als zodanig geregistreerd en voorgelegd aan de decentrale beveiligingsfunctionaris. Voor afhandeling geldt de reguliere rapportage en escalatielijn (zie organisatie van Informatiebeveiliging).
- Beveiligingsincidenten met vertrouwelijk informatie worden centraal geregistreerd en overeenkomstig beveiligd en behandeld. Afhankelijk van de ernst van een incident is er een meldplicht bij de Authoriteit Persoonsgegevens.

12 Bedrijfscontinuïteit

Tegengaan van onderbreking van bedrijfsactiviteiten en bescherming van kritische informatiesystemen tegendegevolgenvanomvangrijkestoringenoframpenenomtijdig herstel te bewerkstelligen.

12.1 Risico's

- Wanneer er niet of nauwelijks invulling gegeven wordt aan de continuïteitsplanning is er naast een vals gevoel van beveiliging, ook grote kans op ad hoc maatregelen als een calamiteit zich voordoet.
- Het uitvallen van medewerkers (ziekte, sterven, ontslag) kan een reële bedreiging zijn.

12.2 Organisatorische aspecten

- De gemeente Hoeksche Waard voert een business impact analyse uit aan de hand van de 'zelftoets voor bedrijfscontinuïteitsmanagement (BCM)'. Afhankelijk van de bevindingen worden per Organisatieonderdeel vervolgacties gepland.
- De gemeente Hoeksche Waard heeft een BCM plan. In de continuïteitsplannen wordt minimaal aandacht besteed aan:
    - Identificatie van essentiële procedures voor bedrijfscontinuïteit.
    - Verantwoordelijkheden en taken: wie het plan mag activeren en wanneer, maar ook wanneer er weer gecontroleerd wordt teruggegaan.
    - Veilig te stellen informatie (aanvaardbaarheid van verlies van informatie).
    - Prioriteiten en volgorde van herstel en reconstructie.
    - Documentatie van systemen en processen.
    - Kennis en kundigheid van personeel om de processen weer op te starten.
- Er worden minimaal jaarlijks oefeningen, testen of audits gehouden om de BCM plannen te toetsen (opzet, bestaan en werking). Aan de hand van de resultaten worden de plannen bijgesteld en wordt de organisatie bijgeschoold.

13 Naleving

Voorkomen van schending van enige wetgeving, wettelijke en regelgevende ofcontractuele verplichtingen, en van beveiligingseisen.

13.1 Risico's

- Niet aantoonbaar kunnen voldoen aan wet en regelgeving;
- Aansprakelijkheid voor schade bij datalekken (EU Algemene verordening gegevensbescherming);
- Ontbreken van stuurinformatie en rapportage voor het proces van Informatiebeveiliging.

13.2 Organisatorische aspecten

- Het verbeteren van de kwaliteit van informatiebeveiliging is een continu proces en onderdeel van alle gemeentelijke processen waarin wordt gewerkt met gevoelige informatie. Informatiebeveiliging is een kwaliteitskenmerk van het primaire proces, waarop het management van elk Organisatieonderdeel stuurt. De kwaliteit wordt gemeten aan:
    - de mate waarin een volledige set aan maatregelen is geïmplementeerd, gebaseerd op vastgesteld beleid;

- effectiviteit van de geïmplementeerde maatregelen;
- de mate waarin de informatiebeveiliging het bereiken van de strategische doelstellingen ondersteunt.

- De CISO zorgt namens de gemeentesecretaris voor het toezicht op de uitvoering van het Informatiebeveiligingsbeleid.
- Externe (hosting) providers en leveranciers leggen verantwoording af aan hun opdrachtgevers over de naleving van het Informatiebeveiligingsbeleid. Bij uitbestede (beheer)processen kan een verklaring bij leveranciers worden opgevraagd (TPM of ISAE3402-verklaring).
- Naleving van regels vergt in toenemende mate ook externe verantwoording, bijvoorbeeld voor het gebruik van DigiD, Suwi en GBA. Aanvullend op het Informatiebeveiligingsbeleid kunnen daarom specifieke normen gelden voor Organisatieonderdelen.
- Periodiek wordt de kwaliteit van informatiebeveiliging in opdracht van de CISO onderzocht door het team Control en door onafhankelijke externen (bijvoorbeeld door middel van 'penetratietesten'). Minimaal jaarlijks worden audits/onderzoeken gepland. De bevindingen worden gebruikt voor de verdere verbetering van de informatiebeveiliging.
- In de P&C cyclus wordt gerapporteerd over informatiebeveiliging aan de hand van het 'in control' statement.
- Door periodieke controle volgens het ENSIA Framework, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie.

13.3 (Wettelijke) kaders

- Een overzicht van relevante wet- en regelgeving is opgenomen als bijlage in het Strategisch Informatiebeveiligingsbeleid.
- Het gebruik van persoonsgegevens geregeld in de Algemene Verordening Gegevensbescherming (AVG).
- Voor elk type registratie wordt de bewaartermijn, het opslagmedium en eventuele vernietiging bepaald in overeenstemming met wet, regelgeving, contractuele verplichtingen en bedrijfsmatige regelgeving. Bij de keuze van het opslagmedium wordt rekening gehouden met de bewaartermijn, de achteruitgang van de kwaliteit van het medium in de loop van de tijd en de voortdurende beschikbaarheid van hulpmiddelen (zoals hard- en software) om de gegevens te raadplegen en te bewerken.
- Bij het (laten) vervaardigen en installeren van programmatuur wordt er voor gezorgd dat de intellectuele eigendomsrechten die daar op rusten niet worden geschonden.

Bijlage 1: Relevante documenten en bronnen

- NEN/ISO 27001 en 27002 (Code voor Informatiebeveiliging), 2005/7
- Baseline Informatiebeveiliging Gemeenten (BIG), KING, 2013
- Wetgeving, wetten.overheid.nl
- NCSC: http://www.ncsc.nl
- IBD: http://www.ibdgemeenten.nl
- GEMMA Procesarchitectuur 2.0, 2011; www.kinggemeenten.nl/media/348541/procesarchitectuur%202.0.pdf
- NORA: http://www.noraonline.nl/wiki/NORA_online

Bijlage 2: Relevante begrippen

Audit: Vastlegging van de complete keten van opeenvolgende wijzigingen op een object in een bepaalde periode.
Basis beveiligingsniveau: Het geheel van maatregelen van beveiliging dat wordt bereikt door het implementeren en toepassen van de normen zoals geformuleerd in de Code voor Informatiebeveiliging, Business Continuïty Management en artikel 16 van de WBP en waaraan de NORA een nadere uitwerking geeft, onder meer door normen voor ICT-voorzieningen.
Bedrijfsmiddel: Elk middel waarin of waarmee bedrijfsgegevens kunnen worden opgeslagen en/of verwerkt en waarmee toegang tot gebouwen, ruimten en ICT-voorzieningen kan worden verkregen: een bedrijfsproces, een gedefinieerde groep activiteiten, een gebouw, een apparaat, een ICT-voorziening of een gedefinieerde groep gegevens.
Beschikbaarheid: De waarborg dat vanuit hun functie geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen
Beveiliging: Het brede begrip van informatiebeveiliging, d.w.z. inclusief fysieke beveiliging, Business Continuïty Management (BCM), ofwel beschikbaarheid van bedrijfsprocessen en persoonlijke beveiliging en integriteit.
Beveiligingsincident: Het manifest worden van een beveiligingsrisico (dreiging, oorzaak) als gevolg van een overtreding van beveiligingsregel, bijv. onbevoegde toegang tot ICTvoorzieningen.
Clear Desk: Anders dan Clean Desk, waarbij het bureau helemaal leeg is, betekent Clear Desk dat er geen vertrouwelijke informatie op het bureau ligt.
Controleerbaarheid: De mate waarin de werkelijkheid of representaties daarvan toetsbaar zijn, dat wil zeggen te vergelijken met andere 'werkelijkheden of representaties daarvan' zodat objectieve oordeelsvorming mogelijk wordt
Filtering: Het gecontroleerd doorlaten van gegevens op het grensvlak tussen zones in een netwerk.
Firewall: Het geheel van software- en eventueel ook hardwarevoorzieningen dat voorkomt dat ongewenst verkeer van de ene netwerkzone terecht komt in de andere, teneinde de beveiliging in de laatstgenoemde te verhogen.
Hardening: Overbodige functies in besturingssystemen uitschakelen en/of van het systeem verwijderen en zodanige waarden toekennen aan beveiligingsinstellingen dat een maximale beveiliging ontstaat.
ICT-voorzieningen: Applicaties en technische infrastructuur, of wel het geheel van ICT- voorzieningen.
In control statement: Binnen de gebruikelijke Planning en Control cyclus moet door B&W een in control statement worden afgegeven over het BIG. De in control verklaring moet inzicht geven aan welke BIG normen wordt voldaan en voor welke BIG normen een explain is gedefinieerd.
Informatiebeveiliging: Het process van vaststellen van de vereiste betrouwbaarheid van informatieverwerking in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.
Informatiesysteem: Een samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.
Integrale beveiliging is de beveiliging van vastgestelde te beschermen belangen (TBB) door op basis van risicomanagement en een kosten/batenanalyse een samenhangend stelsel van beveiligingsmaatregelen te selecteren en te implementeren. Het besturingsmodel voor integrale beveiliging sluit aan bij de besturingsuitgangspunten binnen de gemeenten: het lijnmanagement is integraal verantwoordelijk en dus ook voor de beveiliging van de TBB.
Integriteit: Het waarborgen van de juistheid en volledigheid en tijdigheid van informatie en de verwerking ervan. Als de tijdigheid van gegevens bepaald wordt door omstandigheden buiten het systeem, kan deze vanzelfsprekend niet als integriteitseis voor het systeem gesteld worden.
Logging: Vastlegging van systeemhandelingen.
Malware: Software met ongewenste functies, zoals virussen en trojans.
Mobile code: Code afkomstig van een ander systeem die lokaal uitgevoerd wordt, bijv. Javascript, Flash of Silverlight.
Onvertrouwd: Geen zekerheid over het beveiligingsniveau of zekerheid over het lager dan vereiste beveiligingsniveau.
Onweerlegbaarheid: Het niet kunnen ontkennen iets te hebben gedaan (bijvoorbeeld een bericht te hebben ontvangen dan wel te hebben verstuurd).
Patch: Klein onderdeel van software dat de leverancier van software uitgeeft om fouten in door hem vervaardigde software te repareren.
Query: Bevraging in een vraagtaal, die op basis van gebruikersvriendelijke en krachtige commando's selecties en berekeningen op bestanden kan uitvoeren, in eerste instantie
alleen voor raadpleegdoeleinden.
SiSa: Single information, single audit betekent eenmalige informatieverstrekking, eenmalige accountantscontrole. SiSa is de manier waarop medeoverheden (provincies, gemeenten en gemeenschappelijke regelingen) aan het Rijk ieder jaar verantwoorden of en hoe ze de specifieke uitkeringen hebben besteed.

Technische infrastructuur:Het geheel van ICT-voorzieningen voor generiek gebruik, zoals servers, firewalls, netwerkapparatuur, besturingssystemen voor netwerken en servers, database management systemen en beheer- en beveiligingstools, inclusief bijbehorende systeembestanden.
Two-factor authenticatie: Two-factor authenticatie vereist het gebruik van twee van de drie volgende authenticatiemethoden: 1) iets dat de gebruiker weet (b.v. password, PIN);
2) iets dat de gebruiker heeft (b.v. toegangspas, sleutel); en 3) iets dat de gebruiker is (b.v. biometrische eigenschap zoals een vingerafdruk).
Vertrouwd: In overeenstemming met een door een bevoegde autoriteit vastgesteld beveiligingsniveau. Bijvoorbeeld vertrouwde zones of vertrouwde netwerken.
Vertrouwelijkheid: Het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd.
Vertrouwelijke informatie: Informatie die niet algemeen bekend mag worden (bron: van Dale). In het kader van de BIG worden maatregelen beschreven die voldoen voor de behandeling van gerubriceerde informatie tot en met vertrouwelijke en persoonsvertrouwelijke informatie, zoals bedoeld in Artikel 9 van de AVG
Verwijderbare media: Opslagmiddelen die los van apparatuur kunnen worden verwijderd en meegenomen. Zoals CD-ROM, USB stick, verwijderbare schijven, tapes of gedrukte media.
Zone: De logische verzameling van ICT-voorzieningen met hetzelfde beveiligingsniveau, die via beveiligde koppelvlakken gegevens kunnen uitwisselen.