gemeente lingewaard

GEMEENTEBLAD

Officiële uitgave van de gemeente Lingewaard

Nr. 304868

9 september 2021

Informatiebeveiligingsbeleid gemeente Lingewaard

Inleiding
Dit document geeft algemene beleidsuitgangspunten over informatiebeveiliging. Deze uitgangspunten hebben een sterk normerend karakter en geven keuzes weer. Dit document is het optimum beleid gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO).
In dit document is een aanzienlijk aantal beleidsuitgangspunten nader uitgewerkt en zijn beveiligingseisen en -maatregelen opgenomen, die organisatie breed voor alle processen en systemen gelden.
Onderdeel van dit document is een beheerstructuur voor informatiebeveiliging, waarmee verantwoordelijkheden voor informatiebeveiliging worden belegd en informatiebeveiliging wordt ingebed in de reguliere planning- en control cyclus binnen de (kwaliteits¬handhaving van de) bedrijfsvoering.

De toegepaste hoofdstukken uit de Strategische variant van de Baseline Informatiebeveiliging voor Gemeenten zijn:
- 5 Beveiligingsbeleid;
- 6 Organisatie van informatiebeveiliging;
- 7 Beheer van bedrijfsmiddelen;
- 8 Beveiliging van personeel;
- 9 Fysieke beveiliging en beveiliging van de omgeving;
- 10 Beheer van communicatie- en bedieningsprocessen;
- 11 Toegangsbeveiliging;
- 12 Verwerving, ontwikkeling en onderhoud van informatiesystemen;
- 13 Beheer van informatiebeveiligingsincidenten;
- 14 Bedrijfscontinuïteitsbeheer;
- 15 Naleving.

Informatiebeveiliging
Informatiebeveiliging is de verzamelnaam voor de processen, die ingericht worden om de betrouwbaarheid van processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen al dan niet opzettelijk onheil. Het begrip ‘informatiebeveiliging’ heeft betrekking op:

- *beschikbaarheid / continuïteit*: het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- *exclusiviteit / vertrouwelijkheid*: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn;
- *integriteit / betrouwbaarheid*: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

Waarom informatiebeveiliging?
Informatie is één van de belangrijkste bedrijfsmiddelen van de gemeente. Toegankelijke en betrouwbare overheidsinformatie is essentieel voor de gemeente, die zich verantwoordelijk gedraagt, aanspreekbaar en servicegericht is, die transparant en proactief verantwoording aflegt aan burgers en raadsleden en die met minimale middelen maximale resultaten behaalt. De bescherming van waardevolle informatie is datgene waar het uiteindelijk om gaat. Hoe waardevoller de informatie is, hoe meer maatregelen er getroffen moeten worden.

Reikwijdte en afbakening informatiebeveiliging
Informatiebeveiliging is meer dan ICT, computers en automatisering. Het gaat om alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, DVD, USB, SD kaart, beeldscherm et cetera) en alle informatie verwerkende systemen (applicaties, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen), maar vooral ook mensen en processen. Studies laten zien dat de meeste incidenten niet voortkomen uit gebrekkige techniek, maar vooral door menselijk handelen en een tekort schietende organisatie. Voorbeelden van informatiebeveiligingsmaatregelen zijn: clean desk policy implementeren of hoe om te gaan met mobiele devices en aanwijzingen voor telewerken.

Informatiebeveiligingsbeleid van de gemeente Lingewaard
Het bestuur en management spelen een cruciale rol bij het uitvoeren van dit informatiebeveiligingsbeleid. Zo maakt het management een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente hebben, de risico’s die de gemeente hiermee loopt en welke van deze risico’s onacceptabel hoog zijn. Op basis hiervan zet het management dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitbrengen en handhaven van een informatiebeveiligingsbeleid van en voor de hele de gemeente. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid en de relevante landelijke en Europese wet- en regelgeving.
De gemeente is zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van het beleid. Hierbij geldt:

- Er is wetgeving waar altijd aan voldaan moet worden, zoals (niet uitputtend) bijvoorbeeld BRP, SUWI, BSN, BAG en PUN, maar ook de archiefwet.
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Nederlandse Overheid (BIO).
- De gemeente stelt dit normenkader vast, waarbij er ruimte is voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.

De volgende uitgangspunten zijn ontleend aan de Code voor Informatiebeveiliging (NEN/ISO 27002:2007) en de BIO:

1. Informatie en informatiesystemen zijn van kritiek en vitaal belang voor de gemeente. De verantwoordelijkheid voor informatiebeveiliging ligt bij het (lijn)management, met het **College van B&W als eindverantwoordelijke**. De verantwoordelijkheden voor de bescherming van gegevens en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd.
2. Door **periodieke controle, organisatie brede planning én coördinatie** wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
3. Informatiebeveiliging is een **continu verbeterproces**. 'Plan, do, check en act' vormen samen het **management systeem** van informatiebeveiliging.
4. De organisatiebrede **informatiebeveiligingsfunctionaris**/Chief Information Security Officer (= CISO) - binnen de gemeente Lingewaard aangeduid als de CISO - ondersteunt vanuit een **onafhankelijke positie** de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover.
   Daarnaast kennen we deelfuncties in de informatiebeveiliging zoals
   Voor Suwinet: security officer Suwinet
   Voor de BRP: de security officer BRP
   Voor de reisdocumenten: de beveiligingsfunctionaris Reisdocumenten en Rijbewijzen
   Voor de rijbewijzen: beveiligingsfunctionaris Reisdocumenten en Rijbewijzen
5. De gemeente stelt de benodigde **mensen en middelen beschikbaar** om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid.
6. **Regels en verantwoordelijkheden** voor het beveiligingsbeleid dienen te worden vastgelegd en **vastgesteld**. Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
7. Iedere medewerker, zowel vast als tijdelijk, intern of extern is **verplicht waar nodig gegevens en informatiesystemen te beschermen** tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

Dit Informatiebeveiligingsbeleid treedt in werking na vaststelling door College van B&W. Hiermee komt het oude Informatiebeveiligingsbeleid van de gemeente Lingewaard te vervallen.

1 Uitgangspunten informatiebeveiliging

1.1 Het belang van informatie(veiligheid)

Informatie is één van de voornaamste bedrijfsmiddelen van Lingewaard. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de bedrijfsvoering maar ook leiden tot imagoschade. Ernstige incidenten hebben mogelijk negatieve gevolgen voor burgers, bedrijven, partners en de eigen organisatie met waarschijnlijk ook politieke consequenties. Informatieveiligheid is daarom van groot belang. Informatiebeveiliging is het proces dat dit belang dient.

Visie

De komende jaren zet de gemeente Lingewaard in op het verhogen van informatieveiligheid en verdere professionalisering van de informatiebeveiligingsfunctie in de organisatie. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van burgers en bedrijven. [1] Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

Het proces van informatiebeveiliging is primair gericht op bescherming van informatie, maar is tegelijkertijd een 'enabler'; het maakt bijvoorbeeld elektronische dienstverlening op verantwoorde wijze mogelijk, evenals nieuwe, innovatieve manieren van werken. De focus is informatie uitwisselen in alle verschijningsvormen, zoals elektronisch, op papier en mondeling. Het gaat niet alleen over bescherming van privacy, maar ook over bescherming van vitale maatschappelijke functies die worden ondersteund met informatie (verkeer, vervoer, openbare orde en veiligheid, etc.). Het gaat ook niet alleen over ICT: verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid. [2]

1.2 Doelstelling

Dit informatiebeveiligingsbeleid is het kader voor passende technische en organisatorische maatregelen om informatie te beschermen en te waarborgen, waarmee de gemeente voldoet aan relevante wet en regelgeving. De gemeente Lingewaard streeft er naar om "in control" te zijn en daarover op professionele wijze jaarlijks verantwoording af te leggen via een Verklaring Van Toepasselijkheid. In control betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn en dat er een SMART-planning is van de maatregelen die nog niet genomen zijn en als laatste dat dit geheel verankerd is in de PDCA-cyclus.

1.3 Uitgangspunten

- Het informatiebeveiligingsbeleid van de gemeente Lingewaard is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving. [3]
- Het beleid is gebaseerd op de Code voor Informatiebeveiliging (NEN/ISO 27002) en de BIO.
- Het Informatiebeveiligingsbeleid wordt vastgesteld door het College van B&W van de gemeente Lingewaard. Het College van B&W herijkt periodiek het Informatiebeveiligingsbeleid.
- Het College van B&W van de gemeente Lingewaard is volgens de Algemene Verordening Gegevensverwerking (AVG) de verantwoordelijke voor de verwerking van persoonsgegevens en dus ook voor een veilig en rechtmatig gebruik van Suwinet. Security officer Suwinet ziet hier op toe.

1.4 Risicobenadering

- De aanpak van informatiebeveiliging (Informatiebeveiligingsbeleid) in Lingewaard is 'risk based'. Dat wil zeggen: beveiligingsmaatregelen worden getroffen op basis van een toets tegen de baseline. Indien een systeem meer maatregelen nodig heeft, wordt een risicoanalyse uitgevoerd. Daartoe inventariseert de proceseigenaar de kwetsbaarheid van zijn werkproces en de dreigingen die kunnen leiden tot een beveiligingsincident, rekening houdend met de beveiligingseisen van de informatie. Het risico is de kans op beveiligingsincidenten en de impact daarvan op het werkproces en wordt bepaald door de proceseigenaar: **risico = kans x impact.**

1.5 Doelgroepen

Het Informatiebeveiligingsbeleid is bedoeld voor alle in- en externe medewerkers van de gemeente:

Doelgroep	Relevantie voor Informatiebeveiligingsbeleid
College van B&W	Integrale verantwoordelijkheid
Directie	Kaderstelling en implementatie
Alle leidinggevenden	Sturing op informatieveiligheid en controle op naleving
Alle medewerkers	Gedrag en naleving
Proces en gegevenseigenaren	Classificatie: bepalen van beschermingseisen van informatie

1) *Met betrouwbare informatievoorziening wordt bedoeld dat de volgende zaken geregeld zijn: beschikbaarheid (continuïteit van de bedrijfsvoering), integriteit (juistheid, volledigheid) en vertrouwelijkheid (geautoriseerd gebruik) van gegevens en informatie.*

2) *Medewerker = (1) ambtenaar in de zin van het Ambtenarenreglement of (2) degene die op arbeidsovereenkomst of anderszins betaalde of niet-betaalde werkzaamheden voor een organisatieverricht.*

3) *Daarbij geldt het 'comply or explain' principe (pas toe of leg uit)*

Het directieteam	Planvorming binnen de informatiebeveiligingskaders
de CISO	Algemene en dagelijkse coördinatie van de informatiebeveiliging, adviseren over de implementatie van het informatiebeveiligingsbeleid
Personeelszaken	Arbeidsvoorwaardelijke zaken
Facilitaire zaken	Fysieke toegangsbeveiliging
het team Informatievoorziening	Technische beveiliging
Auditors	Onafhankelijke toetsing van het beleid
Leveranciers en ketenpartners	Compliance aan het beleid

1.6 Scope

De scope van dit beleid omvat alle processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente en externe partijen (bijv. politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.
Dit informatiebeveiligingsbeleid is een algemene basis. Dit normenkader geldt dus expliciet ook voor de bedrijfsprocessen waarin de audtis en/of zelfevaluaties DigiD assessment, BAG inspectie, Suwinet, BRP, reisdocument en rijbewijzen zich op richten.

1.7 Informatiebeveiligingsbeleid en architectuur

Informatiebeveiliging is onderdeel van de informatiearchitectuur en zal worden uitgewerkt als onderdeel van die architectuur. Deze architectuur beschrijft onder meer principes, richtlijnen en maatregelen o.b.v. verschillende beschermingsniveaus (classificatie).[4]

1.8 Wat is ENSIA?

ENSIA staat voor Eenduidige Normatiek Single Information Audit en betekent eenmalige informatieverstrekking en eenmalige IT-audit.
Het project ENSIA heeft tot doel het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid gebaseerd op de Baseline Informatiebeveiliging Nederlandse Overheid.
ENSIA helpt gemeenten in één keer slim verantwoording af te leggen over informatieveiligheid gebaseerd op de BIO (Baseline Informatiebeveiliging Nederlandse Overheid). De verantwoordingssystematiek over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Werk en Inkomen (SUWInet) is samengevoegd en gestroomlijnd.
Uitgangspunt is het horizontale verantwoordingsproces aan de gemeenteraad. Dit vormt de basis voor het verticale verantwoordingsproces aan de nationale partijen die een rol hebben in het toezicht op informatieveiligheid.

1.9 Waarom ENSIA?

Tijdens de Buitengewone Algemene Ledenvergadering van de VNG van november 2013 is de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' aangenomen. Met het aannemen van de resolutie erkennen alle gemeenten het belang van informatieveiligheid en de BIO als het gemeentelijk basisnormenkader voor informatieveiligheid. In de resolutie hebben gemeenten afgesproken hun eigen toezichthouder, de gemeenteraad, in het jaarverslag te informeren over informatieveiligheid. Ook roepen de gemeenten in de resolutie op om de verantwoordingslasten over informatieveiligheid te verminderen. Dit vormde de aanleiding voor de start van het project ENSIA.

2 Organisatie van de informatiebeveiliging

2.1 Risico's

Volgens de baseline zijn de te beperken risico's in dit domein:

- Het niet expliciet beleggen van verantwoordelijkheden en bijbehorende activiteiten, procedures en instrumenten, verhindert het daadwerkelijk en structureel uitvoeren en borgen van de beheersmaatregelen.

2.2 Doelstellingen

Conform de baseline stellen we als organisatie onszelf de volgende doelstellingen in dit domein:

4) *De processen van informatiebeveiliging worden onderdeel van de volgende GEMMA versie om daarmee de basis voor informatieveiligheid te verankeren als integraal onderdeel van de bedrijfsvoering.*

- Beheren van de informatiebeveiliging binnen de organisatie.
- Er is een beheerkader vastgesteld om de implementatie van informatiebeveiliging in de organisatie te initiëren en te beheersen.
- Goedkeuring door het College van B&W en Het directieteam van het informatiebeveiligingsbeleid, de toewijzing van de rollen en de coördinatie en beoordeling van de implementatie van het beleid binnen de organisatie.

2.3 Beheersmaatregelen

De baseline maakt onderscheid in de volgende beheersmaatregelen voor dit domein:

Beheersmaatregelen voor de interne ambtelijke organisatie

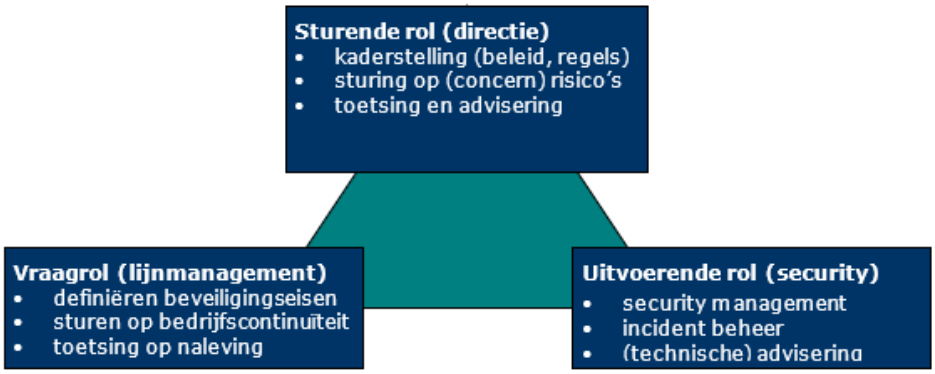
- Het College van B&W van de gemeente Lingewaard is integraal verantwoordelijk voor de beveiliging (in de beslissende rol) van informatie binnen de werkprocessen van de gemeente..
  Het College van B&W stelt kaders voor informatiebeveiliging op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders;
- De directie (in de sturende rol) is verantwoordelijk voor kaderstelling en sturing.
  De directie: [5]
  - stuurt op concern risico's;
  - controleert de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen;
  - controleert of deze maatregelen voldoende bescherming bieden en;
  - evalueert periodiek beleidskaders en stelt deze waar nodig bij.

- De leidinggevenden van de verschillende onderdelen van de organisatieonderdelen zijn in de vragende rol verantwoordelijk voor de integrale beveiliging van hun organisatie onderdeel. [6]
  De leidinggevenden:
  - stellen op basis van een expliciete risicoafweging betrouwbaarheidseisen voor zijn informatiesystemen vast (classificatie);
  - zijn verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
  - sturen op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn);
  - rapporteren over compliance aan wet- en regelgeving en algemeen beleid van de gemeente in de managementrapportages.
  - Het directieteam moet het bewustzijn van de medewerkers op het gebied van informatiebeveiliging stimuleren. Dit vindt plaats door informatieveiligheid via een i-bewustzijnscampagne actief uit te dragen in de organisatie.

- Facilitaire zaken is in de uitvoerende rol verantwoordelijk voor de uitvoering van de beveiligingsmaatregelen.
- De manager IV is verantwoordelijk voor:
  - o beveiliging van de informatievoorziening en implementatie van beveiligingsmaatregelen, die voortvloeien uit betrouwbaarheidseisen (classificaties);
  - o is verantwoordelijk voor alle beheeraspecten van informatiebeveiliging, zoals ICT security management, incident en problem management, facilitaire en personele zaken;
  - o verzorgt logging, monitoring en rapportage; levert klanten (technisch) beveiligingsadvies.

5) *Met betrekking tot de i-functie geeft de CISO op dagelijkse basis namens de directie invulling aan de sturende rol door besluitvorming in de directie voor te bereiden en toe te zien op de uitvoering ervan.*

6) *Zie ook: strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten*



Figuur 1: relaties

Beheersmaatregelen m.b.t. de taken en rollen

- Het College van B&W stelt formeel het Informatiebeveiligingsbeleid vast. De uitvoering van het beleid moet gecontroleerd worden, zowel het College van B&W als Gemeenteraad (controle functie) kunnen hiervoor opdracht geven om dit te (laten) controleren. De directie adviseert het College van B&W formeel over vast te stellen beleid.
- De CISO (Chief Information Security Officer), geeft namens de directie op dagelijkse basis invulling aan de sturende rol door besluitvorming in de directie voor te bereiden en toe te zien op de uitvoering ervan.
- De taken m.b.t. informatiebeveiliging die hieruit voortvloeien zijn belegd bij de 'Chief Information Security Officer' (de CISO). De CISO bevordert en adviseert gevraagd en ongevraagd over IB en rapporteert eens per jaar concernbreed aan de directie over de stand van zaken. De coördinatie van informatiebeveiliging is belegd bij een strategische adviesfunctie binnen alle organisatie onderdelen. Uitvoerende taken zijn zoveel mogelijk belegd bij (decentrale) security functionarissen zoals security officer Suwinet, de security officer BRP, de beveiligingsfunctionaris Reisdocumenten en Rijbewijzen en beveiligingsfunctionaris Reisdocumenten en Rijbewijzen. Deze security functionarissen rapporteren aan de CISO. Over het functioneren van informatiebeveiliging wordt minimaal jaarlijks gerapporteerd conform de PDCA cyclus.
- Facilitaire zaken en het team Informatievoorziening heeft een security functionaris aangesteld voor dagelijks beheer van technische IB-aspecten. De security functionaris rapporteert aan de CISO. Informatiebeveiliging is onderdeel van de PDCA rapportagecyclus.

Wie	Plan: Kaderstelling	Do: Uitvoering	Check: Controle	Act: Verbetering
Sturen: Directie dagelijkse uitvoering: CIO/de CISO, decentrale security functionarissen	Ontwikkelen van kaders (beleid en architectuur); reglementen; meerjarenplanning.	Inbedding landelijke en EU-richtlijnen, advisering, handreikingen, crisisbeheersing en incident respons.	Controle, audit, pentesten.	Bijsturen: opdrachtverstrekking voor verbeteracties. Rapportage aan directie/ College van B&W
Vragen: Alle organisatie onderdelen	Formuleren van beveiligingseisen (classificatie) en opstellen clusterbeleid en beveiligingsplannen.	Stimuleren van beveiligingsbewustzijn bij medewerkers, risico- en bedrijfscontinuïteit-management.	Interne controle (IC), sturen op naleving van regels door medewerkers (gedrag), compliancy.	Verbeteren bedrijfscontinuïteit. Rapportage aan CIO/de CISO.
Uitvoeren : De manager IV en Facilitaire zaken	Beleidsvoorbereiding, technische onderzoeken (marktverkenningen).	Leveren van diensten (ICT), incidentbeheer, logging, monitoring en ICT advies.	Vulnerability scanning, evaluatie en rapportage.	Uitvoeren verbeteracties. Advies aan de CIO/de CISO over aanpassingen aan de informatievoorziening.

Beheersmaatregelen m.b.t. het instellen van de projectgroep Informatiebeveiliging

De CISO stelt een organisatie voor van security gerelateerde functionarissen en organiseert ten minste eenmaal per kwartaal een (security) overleg met dit gremium. De CISO is voorzitter en verder bestaat

de projectgroep Informatiebeveiliging in ieder geval uit relevante ICT en personele en fysieke beveiliging experts, en indien nodig zijn inkoop, control en het team Communicatie vertegenwoordigd. Tevens kunnen de diverse decentrale securityfunctionarissen zoals security officer Suwinet, de security officer BRP en de beveiligingsfunctionaris Reisdocumenten en Rijbewijzen worden gevraagd om deel te nemen. Daarnaast worden de Privacy officer en de FG (functionaris gegevensbescherming) uitgenodigd voor het overleg.

Het overleg heeft binnen de gemeente een adviesfunctie richting de CIO[7] of gelijkwaardig of rechtstreeks aan Het directieteam en richt zich met name op beleid en adviseert over tactisch/strategische informatiebeveiliging kwesties.
Het onderwerp Informatiebeveiliging dient verder een vast onderdeel te zijn op de agenda van Het directieteam zodat er sturing kan plaatsvinden op de uitgevoerde activiteiten.

Beheersmaatregelen m.b.t. externe partijen

- Informatiebeveiligingsbeleid, landelijke normen en wet en regelgeving gelden ook voor externe partijen (leveranciers, ketenpartners) waarmee de gemeente samenwerkt (en informatie mee uitwisselt).[8] Ook voor externe partijen geldt hierbij het "pas toe of leg uit" beginsel.
- Bij contractuele overeenkomsten gelden in beginsel altijd de eigen Inkoop Voorwaarden van de gemeente Lingewaard (de GIBIT voorwaarden zijn vastgesteld voor de gemeente Lingewaard), waarin onder meer geheimhouding, privacybescherming en aansprakelijkheid zijn geregeld. Afwijkingen dienen te worden getoetst aan Informatiebeveiligingsbeleid zoals vastgesteld door de organisatie. Vereiste beveiligingsmaatregelen worden aanvullend vastgelegd in contracten en/of bewerkersovereenkomsten. Daarin is onder meer geborgd dat beveiligingsincidenten onmiddellijk worden gerapporteerd en dat de gemeente het recht heeft afspraken te (laten) controleren via een auditor "right to audit".
- Voor het tot stand brengen van datakoppelingen met externe partijen, gelden naast dit generiek informatiebeveiligingsbeleid specifieke procedures. Het doel van deze procedures is risicobeheersing. Voor externe hosting van data en/of services gelden naast dit generieke informatiebeveiligingsbeleid de richtlijnen voor cloud computing. Voor de externe hosting geldt de Open Security Architecture (OSA) en/of de Cloud Security Alliance Controls Matrix (CM) van de Cloud Security Alliance (CSA).
- De gemeente is gehouden aan:
  - regels omtrent grensoverschrijdend dataverkeer;
  - toezicht op naleving van regels door externe partijen;
  - hoogste beveiligingseisen voor bijzondere categorieën gegevens; [9]
  - melding bij de Autoriteit Persoonsgegevens bij uitbesteding van het bewerken van persoonsgegevens en toestemming van de Autoriteit Persoonsgegevens bij doorgifte van persoonsgegevens naar landen buiten de EU.

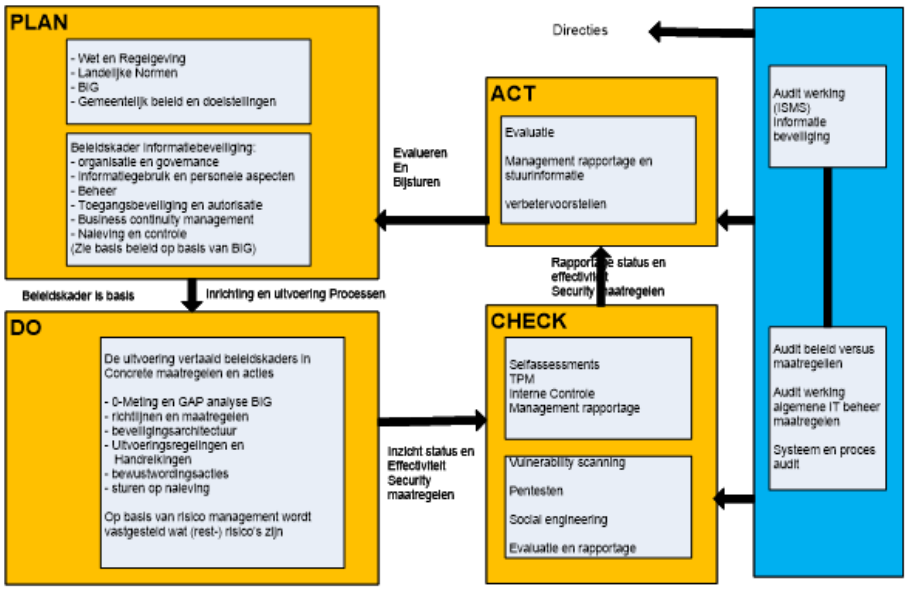
Beheersmaatregelen m.b.t. ICT crisisbeheersing en landelijke samenwerking

- Voor interne crisisbeheersing is er een crisisteam geïnstalleerd, in ieder geval bestaande uit de burgemeester, en de directie. De werkwijze dient te zijn vastgelegd.
- De gemeente Lingewaard participeert in allerlei landelijke platforms en onderhoudt o.a. contacten met de Informatie Beveiliging Dienst (= IBD) van KING.

Beheersmaatregelen m.b.t. de PDCA cyclus

- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het management systeem van informatiebeveiliging.[10] Deze kwaliteitscyclus is in onderstaande figuur weergegeven.

7) *CIO of "gelijkwaardig" kan bijvoorbeeld hoofd ICT, Ondersteuning, Facilitair Bedrijf zijn.*
8) *Beleidsregels voor externe partijen zijn beschreven in de Baseline Informatiebeveiliging Nederlandse Gemeenten.*
9) *Ras of etnische afkomst, politieke opvattingen, religie of overtuiging, het lidmaatschap van een vakvereniging, genetische gegevens of gegevens over gezondheid of seksueel gedrag of strafrechtelijke veroordelingen*
10)*ISO 27001*



Figuur 2: Information Security Management System

- Plan: De cyclus start met Informatiebeveiligingsbeleid, gebaseerd op wet- en regelgeving, landelijke normen zoals de BIO en 'best practices', uitgewerkt in regels voor onder meer informatiegebruik, bedrijfscontinuïteit en naleving. Planning geschiedt op jaarlijkse basis en wordt indien nodig tussentijds bijgesteld. De planning op hoofdlijnen is onderdeel van het jaarplan en uitgewerkt in het informatiebeveiligingsplan (Informatiebeveiligingsbeleid) van de gemeente dat periodiek wordt bijgesteld door de projectgroep Informatiebeveiliging. Afdelingsspecifieke activiteiten kunnen eventueel worden gepland in het afdelingsplan in de lijn.
- Do: Het beleidskader is de basis voor risicomanagement, uitvoering van (technische) maatregelen en bevordering van het beveiligingsbewustzijn. Uitvoering geschiedt op dagelijkse basis en maakt integraal onderdeel uit van het werkproces.
- Check: Control is onderdeel van het werkproces met als doel: waarborgen van de kwaliteit van informatie en ICT, en compliance aan wet- en regelgeving.

  Externe controle: betreft controle buiten het primaire proces door een auditor.[11] Dit heeft het karakter van een steekproef. Jaarlijks worden diverse onderzoeken uitgevoerd, waarbij de CISO in principe opdrachtgever is. Bevindingen worden gerapporteerd aan Het directieteam.
- Act: De cyclus is rond met de uitvoering van verbeteracties o.b.v. check en externe controle. De cyclus is een continu proces; de bevindingen van controles zijn weer input voor de jaarplanning en beveiligingsplannen. De bevindingen worden in beginsel gerapporteerd aan Het directieteam. Voor ingrijpende verbeteracties wordt een gevraagde beslissing voorgelegd.

Beheersmaatregelen m.b.t. Suwinet

- De taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, de inrichting, het beheer en de beveiliging van Suwinet gegevens, applicaties, processen en infrastructuur zijn beschreven en duidelijk en zijn gescheiden belegd. Operationeel beheer, functioneer beheer, technisch beheer, aansturing ICT-leveranciers, autorisatiebeheer zijn belegd.
- Informatie Voorziening is eigenaar van Suwinet.
- Security officer Suwinet beheert en beheerst de beveiligingsprocedures en -maatregelen in het kader van Suwinet zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd.
- Security officer Suwinet bevordert en adviseert over de beveiliging van Suwinet en verzorgt rapportages over de status en controleert dat de beveiliging van de Suwinet maatregelen wordt nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet.
- Security officer Suwinet rapporteert rechtstreeks aan het hoogste management.

11)*Van onder meer de IT auditor, de accountant (jaarrekening), rijksoverheid (voor bijv. basisregistraties) en interne auditors.*

- Het beveiligingsbeleid/plan moet aantoonbaar centraal beschikbaar zijn voor alle gebruikers. Bijvoorbeeld beschikbaar op intranet of op de afdelings-/organisatieschijf. Het uitdragen van het beleid/plan moet niet alleen onder de direct bij de beveiliging betrokken medewerkers plaatsvinden, maar bij alle mensen in de organisatie die Suwinet gebruiken.
- Een adequaat ingerichte organisatie is een belangrijke voorwaarde voor het realiseren van een voldoende beveiligingsniveau voor Suwinet. Het gaat dan met name over functiescheiding. Zo zullen in principe de functies gebruik van Suwinet, beheer van autorisaties Suwinet, controle op het gebruik van Suwinet en beslissen over wie welke functies krijgt in Suwinet gescheiden moeten zijn. Door middel van functiescheiding worden risico's beperkt. Wanneer functiescheiding niet of onvoldoende is geïmplementeerd verhoogt dit de kans op oneigenlijk gebruik en/of misbruik zonder dat dit wordt ontdekt.
- De diverse functies noodzakelijk voor Suwinet moeten schriftelijk zijn vastgelegd, of er een heldere overweging ten grondslag ligt aan de toedeling van taken en of er functiescheiding is toegepast. Het is daarbij van belang dat er een splitsing is tussen beschikkende, controlerende en uitvoerende taken. Er wordt met name gekeken naar vier gescheiden functies. Beoordeeld wordt of minimaal de volgende functies bij verschillende personen zijn belegd:
  - uitvoering van taken (het gebruik van Suwinet zoals door de klantmanager);
  - beheer van autorisaties (toegang verlenen tot Suwinet, de applicatiebeheerder van Suwinet);
  - kwaliteitszorg en borging van rechtmatig gebruik (controle op gebruik van Suwinet, bijvoorbeeld de security officer Suwinet);
  - management (beslissen over bevoegdheden van functiegroepen en/of individuele medewerkers, uitdragen belang goed gebruik, bijsturen na oneigenlijk gebruik, optreden na misbruik Suwinet) .

3 Beheer van bedrijfsmiddelen

3.1 Risico's m.b.t. de verantwoordelijkheid voor de bedrijfsmiddelen

Volgens de baseline zijn de te beperken risico's in dit domein:

- 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 over de vraag wie verantwoordelijk is voor gegevensbestanden, waardoor feitelijk niemand verantwoordelijk is voor de beveiliging en niemand echt zal optreden bij incidenten.

3.2 Doelstellingen m.b.t. de verantwoordelijkheid voor de bedrijfsmiddelen

Conform de baseline stellen we als organisatie onszelf de volgende doelstellingen in dit domein:

- Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie.
- Voor alle bedrijfsmiddelen is de eigenaar vastgelegd alsook de verantwoordelijke voor het handhaven van de beheersmaatregelen.

3.3 Beheersmaatregelen m.b.t. de verantwoordelijkheid voor de bedrijfsmiddelen

De baseline maakt onderscheid in de volgende beheersmaatregelen voor dit domein:

- Alle bedrijfsmiddelen moeten geïdentificeerd zijn en er moet een inventaris van worden bijgehouden.
- Alle informatie en bedrijfsmiddelen, die verband houden met ICT-voorzieningen, aan een 'eigenaar' toewijzen.
- Regels vaststellen, documenteren en implementeren voor het aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen.
- Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen.
- De verantwoordelijkheid voor specifieke beheersmaatregelen mag door de eigenaar worden gedelegeerd, maar de eigenaar blijft verantwoordelijk voor een goede bescherming van de bedrijfsmiddelen.
- Medewerkers dienen bij het gebruik van ICT-middelen, social media en informatie de nodige zorgvuldigheid te betrachten en de integriteit en goede naam van de gemeente te waarborgen.
- Medewerkers gebruiken informatie primair voor het uitvoeren van de aan hen opgedragen taken en het doel waarvoor de informatie is verstrekt.
- Privégebruik van informatie en bestanden is niet toegestaan. Voor het werken op afstand en het gebruik van privémiddelen worden nadere regels opgesteld.

- De medewerker zelf neemt passende technische en organisatorische maatregelen om 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 informatiebeveiligingsbeleid);
  - aan de werkplek verbonden risico's;
  - het risico door het benaderen van informatie met andere dan door de gemeente verstrekte of goedgekeurde ICT-apparatuur.

3.4 Classificatie van informatie

Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen t.a.v. processen en informatiesystemen worden beveiligingsclassificaties gebruikt. [12] 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 tijdigheid) en vertrouwelijkheid (= BIV).

Er zijn drie beschermingsniveaus van laag naar hoog. Daarnaast is er nog een niveau 'geen'. Dit niveau geeft aan dat er geen beschermingseisen worden gesteld, bijvoorbeeld omdat informatie openbaar is. De niveaus zijn in onderstaande tabel weergegeven. Tussen haakjes staan voorbeelden. Deze niveaus zijn bedacht om het proces van classificeren te vereenvoudigen.

3.5 Risico's m.b.t. de classificatie van informatie

Volgens de baseline zijn de te beperken risico's in dit domein:

- Geen inzicht in welke componenten het belangrijkst zijn voor de primaire processen.
- Geen of een 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.

3.6 Doelstellingen m.b.t. de classificatie van informatie

Conform de baseline stellen we als organisatie onszelf de volgende doelstellingen in dit domein:

- Informatie heeft een geschikt niveau van bescherming.
- Classificatie van informatie om bij verwerking de noodzaak en bescherming te kunnen aangeven.
- Adequate niveaus van bescherming van informatie zijn gedefinieerd en de noodzaak voor aparte verwerkingsmaatregelen is gecommuniceerd.

3.7 Beheersmaatregelen m.b.t. de classificatie van informatie

De baseline maakt onderscheid in de volgende specifieke beheersmaatregelen voor dit domein:

- De eigenaar van de gegevens is de proceseigenaar, dat wil zeggen de lijnmanager die de integrale verantwoordelijkheid heeft over het bedrijfsproces. De classificatietabel heeft betrekking op alle in beheer zijnde gegevensverzamelingen, gegevensdragers, informatiesystemen, servers en netwerkcomponenten.
- Het object van classificatie is informatie. We classificeren op het niveau van informatiesystemen (of informatieservices). Alle classificaties van alle bedrijfskritische systemen zijn centraal vastgelegd door de CISO en dienen jaarlijks gecontroleerd te worden door de eigenaren van gegevens.
- Informatie kan meer of minder gevoelig of kritisch zijn. Voor bepaalde informatie kan een extra niveau van bescherming of een speciale verwerking nodig zijn.
- De eigenaar van de gegevens 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 en met welke rechten.
- Er wordt gestreefd naar een zo 'laag' mogelijk classificatieniveau; te hoge classificatie leidt tot onnodige kosten. Bovendien dient informatie in beginsel voor zoveel mogelijk mensen beschikbaar te zijn (transparante overheid).
- Er wordt gestreefd naar een balans tussen het te lopen risico en de kosten van tegenmaatregelen
- Een technische oplossing verdient altijd de voorkeur boven gedragsverandering of een administratieve procedure.
- Informatie classificeren met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie.

12 Dit is in detail beschreven in de component architectuur Informatiebeveiliging 2014, CIO, 2014.

- Opstellen en uitdragen classificatiebeleid binnen de gemeente.
- Er dienen geschikte samenhangende procedures te worden ontwikkeld en geïmplementeerd voor de classificering en verwerking van informatie overeenkomstig het classificatiesysteem dat formeel is vastgesteld.

Niveau	Vertrouwelijkheid	Integriteit	Beschikbaarheid
Geen	**Openbaar** informatie mag door iedereen worden ingezien *(bv: algemene informatie op de externe website van de gemeente*	**Niet zeker** informatie mag worden veranderd *(bv: templates en sjablonen)*	**Niet nodig** gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn *(bv: ondersteunende tools als routeplanner)*
Laag	**Bedrijfsvertrouwelijk** informatie is toegankelijk voor alle medewerkers van de organisatie *(bv: informatie op het intranet)*	**Beschermd** het bedrijfsproces staat enkele (integriteits-) fouten toe *(bv: rapportages)*	**Belangrijk** informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk *(bv: primaire proces informatie)*
Midden	**Vertrouwelijk** informatie is alleen toegankelijk voor een beperkte groep gebruikers *(bv: persoonsgegevens, financiële gegevens*	**Hoog** het bedrijfsproces staat zeer weinig fouten toe *(bv: bedrijfsvoeringinformatie en primaire procesinformatie zoals vergunningen)*	**Noodzakelijk** informatie mag incidenteel niet beschikbaar zijn *bv: administratieve gegevens)*
Hoog	**Geheim** informatie is alleen toegankelijk voor direct geadresseerde(n) *(bv: zorggegevens en strafrechtelijke informatie)*	**Absoluut** het bedrijfsproces staat geen fouten toe *(bv: informatie op de website)*	**Essentieel** informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten *(bv: basisregistraties)*

3.8 Toelichting

De te nemen maatregelen moeten worden afgestemd op de risico's, waarbij rekening dient te worden gehouden met technische mogelijkheden en de kosten van maatregelen. Dit is vaak situatie-afhankelijk. Naarmate de gegevens een gevoeliger karakter hebben, of gezien de context waarin ze gebruikt worden een groter risico inhouden, dienen zwaardere eisen aan de beveiliging van die gegevens te worden gesteld. In het algemeen kan worden gesteld, dat indien met naar verhouding geringe extra kosten meer beveiliging kan worden bewerkstelligd, dit als 'passend' kan worden beschouwd. Extra beveiliging is echter niet meer passend, indien de kosten voor het beperken van de risico's disproportioneel hoog zijn. [13] Kort gezegd: risico's en tegenmaatregelen dienen in balans te zijn.

4 Beveiliging van personeel

4.1 Risico's

Volgens de baseline zijn de te beperken risico's in dit domein:

- 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.

4.2 Doelstellingen

Conform de baseline stellen we als organisatie onszelf de volgende doelstellingen in dit domein:

- Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen.
- De verantwoordelijkheden ten aanzien van beveiliging zijn vóór het dienstverband vastgelegd in passende functiebeschrijvingen en in de arbeidsvoorwaarden.
- Alle kandidaten voor een aanstelling, ingehuurd personeel en externe gebruikers worden gescreend, in het bijzonder ingeval van vertrouwensfuncties.

13 Dit is uitebreid beschreven in: 'Beveiliging van persoonsgegevens', AUTORITEIT PERSOONSGEGEVENS richtsnoeren, 2013.

- Werknemers, ingehuurd personeel en externe gebruikers, die ICT-voorzieningen gebruiken tekenen een overeenkomst over hun beveiligingsrollen en –verantwoordelijkheden.

4.3 Beheersmaatregelen

De baseline maakt onderscheid in de volgende beheersmaatregelen voor dit domein:

Beheersmaatregelen m.b.t. het personeelsbeleid

- Het management is integraal verantwoordelijk voor het juist afhandelen van de beveiligingsaspecten van het aangaan, wijzigen en beëindigen van een dienstverband of een overeenkomst met externen. De HR-afdeling houdt toezicht op dit proces.
- Bij beëindiging van het dienstverband en inhuur worden alle bedrijfsmiddelen van de organisatie geretourneerd. Autorisaties worden in opdracht van de proceseigenaar van het desbetreffende bedrijfsproces ingetrokken.
- Medewerkers die zullen gaan werken met vertrouwelijke of geheime informatie zullen voor indiensttreding een Verklaring Omtrent het Gedrag (= VOG) overleggen. De VOG wordt herhaald tijdens het dienstverband.
- De eigenaar van het bedrijfsproces 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 de geldende procedures voor informatiebeveiliging. Deze training 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 regelingen.
- Regels die volgen uit dit beleid en andere regelingen gelden ook voor externen, die in opdracht van de gemeente werkzaamheden uitvoeren.

Beheersmaatregelen m.b.t. bewustwording

- Het management bevordert algehele communicatie en bewustwording rondom informatieveiligheid en laat voorbeeldgedrag zien.
- Het directieteam bevordert dat medewerkers (en externe gebruikers van de systemen) zich houden aan beveiligingsrichtlijnen. Afspraken hierover worden vastgelegd.
- In werkoverleggen wordt door de leidinggevende periodiek aandacht geschonken aan informatieveiligheid. Voor zover relevant worden hierover afspraken vastgelegd in planningsgesprekken.

5 Fysieke beveiliging en beveiliging van de omgeving

5.1 Risico's

Volgens de baseline zijn de te beperken risico's in dit domein:

- 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 verhoogd 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.

5.2 Doelstellingen

Conform de baseline stellen we als organisatie onszelf de volgende doelstellingen in dit domein:

- Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie, bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten.
- ICT-voorzieningen, die kritieke of gevoelige bedrijfsactiviteiten ondersteunen, behoren fysiek te worden ondergebracht in beveiligde ruimten, beschermd door afgegrensde beveiligde gebieden, in een gecontroleerde omgeving, beveiligd met geschikte beveiligingsbarrières en toegangsbeveiliging. Ze behoren fysiek te worden beschermd tegen toegang door onbevoegden, schade en storingen.

- Het voorkomen van verlies, schade of diefstal van apparatuur en bescherming tegen fysieke bedreigingen en gevaren van buitenaf.

5.3 Beheersmaatregelen

De baseline maakt onderscheid in de volgende beheersmaatregelen voor dit domein:

- Alle objecten (gebouwen) van de gemeente krijgen op basis van generieke profielen een risicoprofiel toegewezen. Dit is het generieke risicoprofiel dat het beste aansluit bij het object.
- De schade door bedreigingen van buitenaf (zoals brand, overstroming, explosies, oproer, stroomonderbreking) wordt beperkt door passende preventieve maatregelen.
- Toegang tot niet-openbare gedeelten van gebouwen of beveiligingszones is alleen mogelijk na autorisatie daartoe.
- De uitgifte van toegangsmiddelen wordt geregistreerd.
- In gebouwen met beveiligde zones houdt beveiligingspersoneel toezicht op de toegang. Hiervan wordt een registratie bijgehouden.
- De kwaliteit van toegangsmiddelen (deuren, sleutels, sloten, toegangspassen) is afgestemd op de zonering (en het risicoprofiel).
- In diverse panden van de gemeente wordt gebruik gemaakt van cameratoezicht. Het gebruik van beeldmateriaal is beperkt door de Algemene Verordening Gegevensverwerking (AVG) en nadere regels (zoals bijvoorbeeld de WOR).
- 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 daaraan 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 locaties of 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.

6 Beheer van communicatie en bedieningsprocessen

6.1 Risico's

Volgens de baseline zijn de te beperken risico's in dit domein:

- 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.

6.2 Doelstellingen

Conform de baseline stellen we als organisatie onszelf de volgende doelstellingen in dit domein:

- Waarborgen van een correcte en veilige bediening van ICT-voorzieningen.
- Vastgestelde verantwoordelijkheden en procedures voor beheer en bediening van alle ICT-voorzieningen. Dit omvat tevens de ontwikkeling van geschikte bedieningsinstructies.
- Toepassing, waar nodig, van functiescheiding om het risico van nalatigheid of opzettelijk misbruik te verminderen.

6.3 Beheersmaatregelen

De baseline maakt onderscheid in de volgende beheersmaatregelen voor dit domein:

<u>Organisatorische beheersmaatregelen</u>

- 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 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 eindverantwoordelijk voor de betrouwbaarheid van de uitbestede diensten. Dit is gebonden aan regels en vereist goede (contractuele) afspraken en controle hierop.
- Externe hosting van data en/of services wordt:
  - goed gekeurd door de verantwoordelijk lijnmanager;
  - geregeld in overeenstemming met het informatiebeveiligingsbeleid;
  - vooraf gemeld bij het team Informatievoorziening t.b.v. toetsing op beheeraspecten.

Beheersmaatregelen m.b.t. de systeemplanning 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 gedocumenteerd.
- Systemen voor Test en/of Acceptatie zijn logisch gescheiden van Productie (P).
- Faciliteiten voor testen, acceptatie en productie zijn gescheiden om onbevoegde toegang tot of wijziging in het productiesysteem te voorkomen.
- In de test en acceptatie omgeving worden testaccounts gebruikt. Er wordt in beginsel niet getest met productie accounts, mits voor de test absoluut noodzakelijk.
- Vertrouwelijke of geheime data uit de productieomgeving mag niet worden gebruikt in de test-, opleidings-, en acceptatieomgeving tenzij de gegevens zijn geanonimiseerd. Indien het toch noodzakelijk is om data uit productie te gebruiken, is uitdrukkelijke toestemming van de eigenaar van de gegevens vereist en dienen er procedures te worden gevolgd om data op dezelfde wijze te beschermen als productie data.
- Het gebruik van ICT-middelen wordt gemonitord ten behoeve van een tijdige aanpassing van de beschikbare capaciteit aan de vraag.

Beheersmaatregelen m.b.t. encryptie (versleuteling)

- De gemeente gebruikt encryptie conform PKI-overheid standaard. [14]
- Versleuteling vindt plaats conform ‘best practices’ (de stand der techniek), waarbij geldt dat de vereiste encryptie sterker is naarmate gegevens gevoeliger zijn.
- Intern dataverkeer (‘machine to machine’) wordt conform classificatie beveiligd met certificaten.
- Beveiligingscertificaten worden centraal beheerd.

Beheersmaatregelen m.b.t. netwerken

- Het fysieke (bekabelde) netwerk is niet toegankelijk voor onbeheerde apparatuur.
- Het netwerk is waar mogelijk gesegmenteerd (organisatie onderdelen, gebruikers en systemen zijn logisch gescheiden). Tussen segmenten met verschillende beschermingsniveaus worden access control lists (ACL’s) geïmplementeerd.
- 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.
- Alle apparatuur die is verbonden met het netwerk van de gemeente moet kunnen worden geïdentificeerd.

Beheersmaatregelen m.b.t. mobiel werken

- Beveiligingsmaatregelen hebben betrekking op zowel door de gemeente verstrekte middelen als privé-apparatuur ('bring your own device' (BYOD)). Op privé-apparatuur waarmee verbinding wordt gemaakt met het netwerk is de gemeente bevoegd om beveiligingsinstellingen af te dwingen. Dit betreft onder meer: controle op wachtwoord, encryptie, aanwezigheid van malware, etc. Het gebruik van privé-apparatuur waarop beveiligingsinstellingen zijn verwijderd ('jail break', '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 soft-

14 Public Key Infrastructure voor de overheid waarborgt op basis van Nederlandse wetgeving de betrouwbaarheid van informatie-uitwisseling via e-mail, websites of andere gegevensuitwisseling.

ware'). De beveiligingsinstellingen, zoals bedoeld in bovenstaande regel, zijn uitsluitend bedoeld ter bescherming van informatie en integriteit van het 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 privémiddelen en privébestanden. Hiervoor wordt een regeling ontwikkeld.

Beheersmaatregelen m.b.t. back-up en recovery
- In opdracht van de eigenaar van data, maakt het team Informatievoorziening reservekopieën 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.
- 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.

Beheersmaatregelen m.b.t. informatie-uitwisseling
- Voor het gebruik van informatie gelden de rechten en plichten zoals vastgelegd in de diverse documenten, zoals de CAO, geheimhoudingsverklaring, huisregels.
- Digitale documenten van de gemeente Lingewaard waar burgers en bedrijven rechten aan kunnen ontlenen, maken gebruik van PKI Overheid certificaten voor tekenen en/of encryptie. Hiervoor wordt een richtlijn PKI en certificaten opgesteld.
- Er is een (spam) filter geactiveerd voor inkomende e-mail berichten.
- Informatie-uitwisseling voldoet aan standaarden zoals beschreven door het forum standaardisatie, waaronder in ieder geval:
  - DNSSEC: Domeinnaambeveiliging
  - TLS: Beveiligde verbinding
  - DKIM: Anti-Phishing
  - SPF: Anti-Phishing
  - DMARC: Anti-Phishing

Beheersmaatregelen m.b.t. software ontwikkeling en onderhoud
- Applicaties worden door derden ontwikkeld en getest o.b.v. landelijke richtlijnen voor beveiliging, zoals de richtlijnen voor beveiliging van webapplicaties.[15] Er wordt ten minste getest op bekende kwetsbaarheden zoals vastgelegd in de OWASP top 10 voor webapplicaties. [16]
- Web applicaties worden voor de in productie name onder meer getest op invoer van gegevens (grenswaarden, format, inconsistentie, SQL injectie, cross site scripting, etc.).
- De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen (bijvoorbeeld door checksums).
- Alleen gegevens die noodzakelijk zijn voor de taak worden verzameld en beheerd (doelbinding), rekening houdend met beveiligingseisen (classificatie).
- Technische kwetsbaarheden worden regulier met een minimum van 12 keer per jaar gerepareerd door 'patchen' van software, of 'ad hoc' bij acute dreiging. Welke software wordt geüpdatet wordt bepaald door de risico's.

Beheersmaatregelen m.b.t. logging en audit trail
- Het gebruik van informatiesystemen, alsmede uitzonderingen en informatiebeveiligingsincidenten, 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.[17]
- Relevante zaken om te loggen zijn:
  - type gebeurtenis (zoals back-up/restore, reset van een wachtwoord, betreden ruimte);
  - handelingen met speciale bevoegdheden;
  - (poging tot) ongeautoriseerde toegang;
  - systeemwaarschuwingen;

15 Nationaal Cyber Security Centrum, NCSC
16 https://www.owasp.org/index.php/Main_Page
17 In sommige processen is het wettelijk verplicht of zeer gewenst dat geautoriseerde toegang wordt vastgelegd, zodat achteraf steeds kan worden vastgesteld wie toegang tot de gegevens heeft gehad.

- (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 de systeembeheerder. De bewaartermijnen zijn in overeenstemming met de wettelijke eisen.

Overige technische beheersmaatregelen

- Alle gegevens anders dan classificatie 'geen' worden beveiligd conform beveiligingseisen in de IB-architectuur. Classificatieniveau 'laag': transportbeveiliging buiten het interne netwerk; Classificatieniveau 'midden': transportbeveiliging; Classificatieniveau 'hoog': transport en berichtbeveiliging.
- 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.
- 'Mobile code' [18] 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 online transacties worden maatregelen getroffen om onvolledige overdracht, onjuiste routing, onbevoegde wijziging, openbaarmaking, duplicatie of weergave te voorkomen.

6.4 Risico's voor het beheer van de dienstverlening door een derde

Ingeval de gemeente diensten heeft uitbesteed, is er volgens de baseline sprake van een specifieke set aan te beperken risico's in dit domein:

- 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 de keten, ook al is het beheer bij een andere partij neergelegd.

6.5 Doelstellingen voor het beheer van de dienstverlening door een derde

Conform de baseline stellen we als organisatie onszelf de volgende doelstellingen in dit domein:

- Een passend niveau van informatiebeveiliging implementeren en bijhouden en dit vastleggen in een (bewerkers)overeenkomst, contracten en/of convenanten.

18 Software die wordt uitgevoerd zonder expliciete toestemming van de gebruiker, zoals scripts (Java), Java applets, ActiveX controls en Flash animaties. Dergelijke software wordt gebruikt voor functies binnen (web)applicaties.

- 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.

6.6 Beheersmaatregelen voor het beheer van de dienstverlening door een derde

De baseline maakt onderscheid in de volgende specifieke beheersmaatregelen:

- Implementatie en uitvoering van de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de (bewerkers)overeenkomst voor dienstverlening door de derde partij.
- Controle en beoordeling van de diensten, rapporten en registraties, die door de derde partij worden geleverd.
- Er worden periodiek audits uitgevoerd.
- Beheer van wijzigingen in de dienstverlening door derden, in bijvoorbeeld bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging.
- In de met de derde partij overeengekomen SLA voor dienstverlening is aandacht besteed aan informatiebeveiliging.
- In de met de derde partij overeengekomen dat de toegang tot de ICT-voorzieningen en/of de informatievoorziening (bestanden, gegevens) door derden geregeld door kaders aan te geven voor de toegang tot ICT-voorzieningen. 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.

6.7 Risico's in de behandeling van media

Volgens de baseline is er sprake van een specifieke set aan te beperken risico's in dit domein:

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

6.8 Doelstellingen in de behandeling van media

Conform de baseline stellen we als organisatie onszelf de volgende doelstellingen in dit domein:

- Voorkomen van onbevoegde openbaarmaking, modificatie, verwijdering of vernietiging van informatie en bedrijfsmiddelen.
- Media worden beheerst en fysiek beschermd.
- Vastgestelde procedures om documenten, opslagmedia (bijvoorbeeld USB-sticks, back-up tapes, schijven), in- en uitvoergegevens en systeemdocumentatie te beschermen tegen onbevoegde openbaarmaking, wijziging, verwijdering en vernietiging.

6.9 Beheersmaatregelen in de behandeling van media

De baseline maakt onderscheid in de volgende specifieke beheersmaatregelen:

- 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.
- 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 licentieplichtige 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, tablets en smartphones voor wanneer deze niet meer worden gebruikt.
- Encryptie op gegevens met het classificatielabel vertrouwelijk en zeer geheim.

6.10 Risico's bij de uitwisseling van informatie

Volgens de baseline is er sprake van een specifieke set aan te beperken risico's in dit domein:

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

6.11 Doelstellingen bij de uitwisseling van informatie

Conform de baseline stellen we als organisatie onszelf de volgende doelstellingen in dit domein:

- Handhaven van beveiliging van informatie en programmatuur, die wordt uitgewisseld binnen een 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 relevante wetgeving.
- Vastgestelde procedures en normen ter bescherming van informatie en fysieke media, die informatie bevatten die wordt getransporteerd.

6.12 Beheersmaatregelen bij de uitwisseling van informatie

De baseline maakt onderscheid in de volgende specifieke beheersmaatregelen:

- 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.
- 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.
- Gevoelige informatie (classificatie vertrouwelijk en zeer geheim) wordt nooit bekend gemaakt via telefoon of fax, in verband met bijvoorbeeld afluisteren.
- Bewustzijn en sociale controle om het risico op het lekken van informatie via telefoon e.d. te laten afnemen.

7 Logische toegangsbeveiliging

De identiteit van een gebruiker die toegang krijgt tot informatie dient te worden vastgesteld.[19] Logische toegang is gebaseerd op de classificatie van de informatie.

7.1 Risico's

Volgens de baseline is er sprake van een specifieke set aan te beperken risico's in dit domein:

- Wanneer toegangsbeheersing niet expliciet gebaseerd is op de Baseline Informatiebeveiliging Nederlandse Overheid (BIO) 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).

7.2 Doelstellingen

Conform de baseline stellen we als organisatie onszelf de volgende doelstellingen in dit domein:

- Beheersen van de toegang tot informatie, ICT-voorzieningen en bedrijfsprocessen op grond van bedrijfsbehoeften en beveiligingseisen.
- Beleid ten aanzien van informatieverspreiding en autorisatie is van toepassing.
- Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.

7.3 Beheersmaatregelen

De baseline maakt onderscheid in de volgende specifieke beheersmaatregelen:

<u>Beheersmaatregelen m.b.t. identificatie, authenticatie en autorisatie</u>

- De eigenaar van de data is bevoegd toegang te verlenen.
- 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.
- De gemeente maakt, waar mogelijk, gebruik van bestaande (landelijke) voorzieningen voor authenticatie, autorisatie en informatiebeveiliging (zoals: DigiD en eHerkenning).

19 Een gebruiker kan een medewerker, leverancier, burger, bedrijf, samenwerkingspartner of applicatie zijn.

- Wachtwoorden worden voor een beperkte periode toegekend (60 dagen). Wachtwoorden dienen aan eisen te voldoen, deze worden afgedwongen door het systeem. Voor medewerkers met speciale bevoegdheden (systeem en functioneel beheerders) gelden strengere eisen. [20]
- 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 (door middel van encryptie).
- Autorisatie is rol gebaseerd. Autorisaties worden toegekend via functie(s) en organisatie onderdelen.
- Toegang tot informatie met classificaties 'midden' of 'hoog' vereist 'multi-factor' authenticatie (bijv. naam/wachtwoord + token).

Beheersmaatregelen m.b.t. verlenen van externe toegang

- !de gemeente kan een externe partij toegang verlenen tot het netwerk. Hiervoor dient een procedure gemaakt en gevolgd te worden. 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 heeft het recht hierop te controleren en doet dat aan de hand van de audit trail en interne logging.
- De gemeente autoriseert en registreert de gebruikers die toegang hebben tot de Suwinet applicaties op basis van een formele proeedure waarin is opgenomen:
- Het verlenen van toegang tot de benodigde gegevens op basis van de uit te voeren functie/taken; Het uniek identificeren van elke gebruiker tot één persoon;
- Het goedkeuren van de aanvraag voor toegangsrechten door de manager of een gemandateerde; Het tijdig aanpassen of wijzigen van de autorisatie bij functiewijziging of vertrek;
- Het benaderen van de Suwi-databestanden door gebruikers mag alleen plaatsvinden via applicatieprogrammatuur (tenzij sprake is van calamiteiten).
- De controle op verleende toegangsrechten en gebruik vindt meerdere keren per jaar plaats. Dit gebeurt onder leiding van security officer Suwinet.

Beheersmaatregelen m.b.t. mobiel en thuiswerken

- Voor werken op afstand is een werkomgeving beschikbaar. Toegang wordt verleend op basis van multifactor authenticatie.
- Onbeheerde apparatuur (privé-apparaten of de 'open laptop') kan gebruik maken van draadloze toegangspunten (WiFi). Deze zijn logisch gescheiden van het bedrijfsnetwerk.
- Bedrijfsapplicaties worden bij voorkeur zo aangeboden dat er geen informatie wordt opgeslagen op het mobiele apparaat ('zero footprint'). Informatie dient te worden versleuteld bij transport en opslag conform classificatie eisen. [21]
- Voorzieningen als webmail, als ook sociale netwerk en sommige clouddiensten (Dropbox, Gmail, etc.) zijn door het lage beschermingsniveau (veelal alleen naam en wachtwoord, het ontbreken van versleuteling) niet geschikt voor het delen van vertrouwelijke en geheime informatie.

Organisatorische beheersmaatregelen

- Toetsing op het informatiebeveiligingsbeleid is onderdeel van de toets voor projecten met een ICT-component en onderdeel van de project start en eind architectuur (PSA en PEA[22]).
- Projecten met een hoog risicoprofiel vallen onder toezicht van het team Informatievoorziening. Toetsing op architectuur en informatiebeveiliging is hier onderdeel van.
- Projectmandaten worden ten behoeve van behandeling in overleg (onder meer) voorzien van een advies op informatiebeveiliging.
- In het programma van eisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen worden ook relevante beveiligingseisen opgenomen.

Specifieke beheersmaatregelen voor Suwinet

- De gemeente is verantwoordelijk voor het beheer van de toegang tot Suwinet. Autorisatie van medewerkers moet plaatsvinden met behulp van een schriftelijk vastgelegde procedure waarin functies aan autorisaties - en in het verlengde daarvan aan Suwinet-rollen - worden gekoppeld. Concreet gaat het om het aanwezig zijn van een autorisatieprocedure en een autorisatiematrix die onderdeel uitmaakt van de procedure. Uit de autorisatiematrix blijkt dat de organisatie heeft nagedacht over welke functionarissen welke informatie via Suwinet mogen raadplegen, met andere woorden een opzet van de wijze waarop de organisatie de accounts en rollen toekent. Door

20 Het wachtwoordbeleid is uitgewerkt in het wachtwoord beleids document van de gemeente.

21 Separaat document

22 Dit zijn Prince2 termen, zie hiervoor de projectmanagement methodiek Prince2

een uitdraai uit Suwinet hiermee te vergelijken kan de organisatie controleren of de daadwerkelijk uitgereikte accounts en rollen overeenkomen met de in opzet bedachte accounts en rollen.

- De autorisatieprocedure moet ervoor zorgen dat alle gebruikers uniek identificeerbaar zijn. Groepsautorisaties mogen dus niet worden afgegeven. Hierdoor kunnen gebruikers persoonlijk worden aangesproken op hun gebruik van Suwinet. Door aan te geven welke persoon welke functie(s) uitoefent, kan op een gestandaardiseerde en controleerbare wijze de autorisatie voor een persoon binnen Suwinet worden verleend en gecontroleerd. Het toekennen van rollen in Suwinet moet volgens een logische procedure plaats te vinden. Uit de autorisatieprocedure moet duidelijk worden op basis van welke afwegingen, welke medewerker welke gegevens mag zien.
- In de autorisatieprocedure moeten alle stappen in het autorisatieproces aanwezig, helder beschreven en toegewezen zijn aan bevoegde functionarissen binnen de organisatie.
- Van belang is dat het accountbestand meerdere keren (minimaal twee keer) per jaar wordt gecontroleerd en dat aansluitend inactieve accounts worden verwijderd. Om dit te kunnen aantonen is een schriftelijke vastlegging van zowel de procedure als de uitvoering van de controles belangrijk. Of er sprake is van een goed werkend accountbeheer wordt in beginsel over een periode van een jaar bekeken. Dit gebeurt op basis van maandelijkse gegevens van het BKWI naar het percentage inactieve accounts en naar het percentage geblokkeerde accounts bij de organisatie. Het BKWI verstaat onder een inactieve account een account waarmee niet tenminste 1x is ingelogd in een maand en onder een geblokkeerde account een account dat meer dan 90 dagen niet is gebruikt of waarmee 5x foutief is ingelogd.
- Een combinatie van een hoog percentage geblokkeerde accounts samen met een hoog percentage niet actieve accounts is een indicatie van een niet goed werkend accountbeheer en vormt een reden tot nadere vragen aan de gemeente. Als richtsnoer wordt gehanteerd dat bij meer dan 80% actieve accounts er goed gebruik wordt gemaakt van Suwinet. Bij 60% tot 80% wordt het twijfelachtig en bij minder dan 60% lijkt er echt iets aan de hand te zijn.
- Ook is het belangrijk dat zware rollen beperkt zijn uitgedeeld. Dit zijn de rollen waarvan het BKWI aangeeft dat het “risicovolle autorisaties” betreft. Beperkt betekent dat aan een klein percentage medewerkers van de gemeente deze rollen zijn toebedeeld. Het te ruim verstrekken van zware autorisaties vergroot het risico op onrechtmatige raadplegingen van de bestanden, omdat het voor een medewerker eenvoudiger is om - zonder te beschikken over een BSN gegevens van personen te raadplegen. Hierbij wordt gekeken naar de verhouding aantal accounts/accounts met zware rollen en de verhouding medewerkers sociale dienst/sociale recherche. Concreet wordt naar de volgende zware rollen gekeken: G018 (LRD/GBA zoeken), G030 (LRD/GBA zoeken uitgebreid) en G021/R1920 (RDW+ Fraude). Van belang is dat per functie (en per toegekende zware rol) moet worden gemotiveerd waarom er één of meerdere zware rollen zijn toegekend en dan met name waarom het noodzakelijk (proportioneel en subsidiair) is voor de uitoefening van de werkzaamheden. Voorts zijn aanvullende controles noodzakelijk.
- Medewerkers die belast zijn met de uitvoering van de wettelijke taken die vallen onder de Participatiewet, IOAW en IOAZ hebben na autorisatie toegang tot Suwinet. Daarnaast heeft slechts een zeer beperkte groep toegang tot Suwinet: de gemeentelijke belastingdeurwaarders, burgerzaken of de regionale meld- en coördinatiefunctie voortijdig schoolverlaten. Voor deze groep moet een apart contract worden afgesloten met het BKWI. Gebruik van Suwinet door overige functionarissen zoals WMO-medewerkers, medewerkers parkeerbeheer of andere hiervoor niet genoemde medewerkers is niet toegestaan.

8 Verwerving, ontwikkeling en onderhoud van informatiesystemen

8.1 Risico’s

Volgens de baseline is er sprake van een specifieke set aan te beperken risico’s in dit domein:

- Als bij de verwerving van nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen geen eisen omtrent informatiebeveiliging worden opgenomen, kan afbreuk worden gedaan aan de beschikbaarheid, vertrouwelijkheid, integriteit en controleerbaarheid van de gegevensverwerking.
- Als gegevens die worden ingevoerd niet worden gevalideerd bestaat de kans dat deze gegevens onjuist en ongeschikt zijn.

8.2 Doelstellingen

Conform de baseline stellen we als organisatie onszelf de volgende doelstellingen in dit domein:

- Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen;
- Voorkomen van fouten, verlies, onbevoegde modificatie of misbruik van informatie in toepassingen.
- Er behoren validatiecontroles te worden opgenomen in toepassingen om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen te ontdekken.

- Er behoren eisen te worden vastgesteld, en geschikte beheersmaatregelen te worden vastgesteld en geïmplementeerd, voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.
- Gegevensuitvoer uit een toepassing behoort te worden gevalideerd, om te bewerkstelligen dat de verwerking van opgeslagen gegevens op de juiste manier plaatsvindt en geschikt is gezien de omstandigheden.
- Het beschermen van de vertrouwelijkheid, authenticiteit of integriteit van informatie met behulp van cryptografische middelen.
- Het bewerkstelligen van een voldoende mate van beveiliging van systeembestanden.
- Beveiliging van toepassingsprogrammatuur en -informatie handhaven.
- Risico's verminderen als gevolg van benutting van gepubliceerde technische kwetsbaarheden.

8.3 Beheersmaatregelen

De baseline maakt onderscheid in de volgende specifieke beheersmaatregelen:

Beheersmaatregelen m.b.t. de analyse en specificatie van beveiligingseisen

- In projecten worden een beveiligingsrisicoanalyse en maatregelbepaling opgenomen als onderdeel van het ontwerp. Ook bij wijzigingen worden de veiligheidsconsequenties meegenomen;
- In standaarden voor analyse, ontwikkeling en testen van informatiesystemen wordt structureel aandacht besteed aan beveiligingsaspecten. Waar mogelijk wordt gebruikt gemaakt van bestaande richtlijnen (bijv. secure codingguidelines[23])
- Bij aanschaf van producten wordt een proces gevolgd waarbij beveiliging een onderdeel is van de specificatie.
- Waar het gaat om beveiligingsrelevante producten wordt de keuze voor een bepaald product verantwoord onderbouwd.
- Voor beveiliging worden componenten gebruikt die aantoonbaar voldoen aan geaccepteerde beveiligingscriteria zoals NBV[24] goedkeuring of certificering volgens ISO/IEC 15408 (common criteria).
- Er is expliciet aandacht voor leveranciers accounts, hardcoded wachtwoorden en mogelijke ‘achterdeurtjes’.

Beheersmaatregelen m.b.t. de correcte verwerking in toepassingen

- Er moeten controles worden uitgevoerd op de invoer van gegevens. Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen, toevoegen van parameters (SQL-injection) en inconsistentie van gegevens.
- Er bestaan voldoende mogelijkheden om reeds ingevoerde gegevens te kunnen corrigeren door er gegevens aan te kunnen toevoegen.
- Het informatiesysteem moet functies bevatten waarmee vastgesteld kan worden of gegevens correct verwerkt zijn. Hiermee wordt een geautomatiseerde controle bedoeld waarmee (duidelijke) transactie- en verwerkingsfouten kunnen worden gedetecteerd.
- Stapelen van fouten wordt voorkomen door toepassing van ‘noodstop’ mechanismen.
- Verwerkingen zijn bij voorkeur herstelbaar zodat bij het optreden van fouten en/of wegraken van informatie dit hersteld kan worden door het opnieuw verwerken van de informatie.
- De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen (bijv. door checksums).
- Bij uitvoer van gegevens wordt gegarandeerd dat deze met het juiste niveau van vertrouwelijkheid beschikbaar gesteld worden (bijv. beveiligd printen).
- Alleen gegevens die noodzakelijk zijn voor de doeleinden van de gebruiker worden uitgevoerd (need-to-know).

Beheersmaatregelen m.b.t. cryptografie

- De gebruikte cryptografische algoritmen voor versleuteling zijn als open standaard gedocumenteerd en zijn door onafhankelijke betrouwbare deskundigen getoetst.
- Bij de inzet van cryptografische producten volgt een afweging van de risico’s aangaande locaties, processen en behandelende partijen.
- [A]De cryptografische beveiligingsvoorzieningen en componenten voldoen aan algemeen gangbare beveiligingscriteria (zoals FIPS 140-2 en waar mogelijk NBV).
- In het sleutelbeheer is minimaal aandacht besteed aan het proces, de actoren en hun verantwoordelijkheden.

23)*Voor voorbeelden van secure coding guidelines, zie http://www.cert.org/secure-coding/ of bijvoorbeeld ook OWASP*

24)*NBV: Nationaal Bureau voor Verbindingsbeveiliging, onderdeel van het ministerie van BZK.*

- De geldigheidsduur van cryptografische sleutels wordt bepaald aan de hand van de beoogde toepassing en is vastgelegd in het cryptografisch beleid.
- De vertrouwelijkheid van cryptografische sleutels dient te zijn gewaarborgd tijdens generatie, gebruik, transport en opslag van de sleutels.
- Er is een procedure vastgesteld waarin is bepaald hoe wordt omgegaan met gecompromitteerde sleutels.
- [A]Bij voorkeur is sleutelmanagement ingericht volgens PKI Overheid.

Beheersmaatregelen m.b.t. systeembestanden
- Alleen geautoriseerd personeel kan functies en software installeren of activeren.
- Programmatuur behoort pas te worden geïnstalleerd op een productieomgeving na een succesvolle test en acceptatie.
- Geïnstalleerde programmatuur, configuraties en documentatie worden bijgehouden in een configuratiedatabase.
- Er worden alleen door de leverancier[25] onderhouden (versies van) software gebruikt.
- Van updates wordt een log bijgehouden.
- Er is een rollbackstrategie.

Beheersmaatregelen m.b.t. de bescherming van testdata
- Het gebruik van kopieën van operationele databases voor testgegevens wordt vermeden. Indien toch noodzakelijk, worden de gegevens zoveel mogelijk geanonimiseerd en na de test zorgvuldig verwijderd.

Beheersmaatregelen m.b.t. het doorvoeren van wijzigingen
- Er is aantoonbaar wijzigingsmanagement ingericht volgens gangbare best practices zoals ITIL[26] en voor applicaties ASL.
- Van aanpassingen (zoals updates) aan softwarematige componenten van de technische infrastructuur wordt vastgesteld dat deze de juiste werking van de technische componenten niet in gevaar brengen.
- Bij het instellen van besturingsprogrammatuur en programmapakketten wordt uitgegaan van de aanwijzingen van de leverancier.

Beheersmaatregelen m.b.t. het uitlekken van informatie
- Op het grensvlak van een vertrouwde en een onvertrouwde omgeving vindt content-scanning plaats. [27]
- Er dient een proces te zijn om te melden dat (persoons) informatie is uitgelekt

Beheersmaatregelen m.b.t. technische kwetsbaarheden
- Er is een proces ingericht voor het beheer van technische kwetsbaarheden; dit omvat minimaal het melden van incidenten aan de Informatiebeveiligingsdienst, periodieke penetratietests, risicoanalyses van kwetsbaarheden en patching.
- Van softwarematige voorzieningen van de technische infrastructuur kan (bij voorkeur geautomatiseerd) gecontroleerd worden of de laatste updates (patches) in zijn doorgevoerd. Het doorvoeren van een update vindt niet geautomatiseerd plaats, tenzij hier speciale afspraken over zijn met de leverancier.
- Indien een patch beschikbaar is, dienen de risico's verbonden met de installatie van de patch te worden geëvalueerd (de risico's verbonden met de kwetsbaarheid dienen vergeleken te worden met de risico's van het installeren van de patch).
- [A]Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiligings-updates/patches moeten worden ingepland bij de eerst volgende onderhoudsronde.
- Indien nog geen patch beschikbaar is dient gehandeld te worden volgens het advies van de Informatiebeveiligingsdienst of een andere CERT zoals bijvoorbeeld het NCSC.

9 Beveiligingsincidenten

9.1 Risico's
Volgens de baseline is er sprake van een specifieke set aan te beperken risico's in dit domein:

25)*Dit kan ook een interne leverancier zijn.*

26)*Information Technology Infrastructure Library, zie http://www.itil-officialsite.com*

27)*Het gaat hier dan om informatie die zich daar voor leent. Encrypted informatie is niet zondermeer te scannen.*

- 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.

9.2 Doelstellingen

Conform de baseline stellen we als organisatie onszelf de volgende doelstellingen in dit domein:

- Bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden, die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.
- Formele procedures voor rapportage van gebeurtenissen en escalatie. Alle werknemers, ingehuurd personeel en externe gebruikers zijn op de hoogte van deze procedures voor het rapporteren van de verschillende soorten gebeurtenissen en zwakke plekken die invloed kunnen hebben op de beveiliging van de bedrijfsmiddelen.
- Er is een verplichte meldingssystematiek in werking om alle informatiebeveiligingsgebeurtenissen en zwakke plekken zo snel mogelijk te rapporteren aan de aangewezen contactpersoon

9.3 Beheersmaatregelen

De baseline maakt onderscheid in de volgende specifieke beheersmaatregelen:

Beheersmaatregelen m.b.t. melding en registratie

- De medewerker dient geconstateerde of vermoede beveiligingslekken en beveiligingsincidenten direct te melden bij de functionaris informatiebeveiliging van de gemeente.
- Beveiligingsincidenten die worden gemeld bij de service desk, worden als zodanig geregistreerd en voorgelegd aan de security functionaris binnen het team Informatievoorziening. Voor afhandeling geldt de reguliere rapportage en escalatielijn.
- Afhankelijk van de ernst van een incident is er een meldplicht bij het Autoriteit Persoonsgegevens vanaf 1 januari 2016. [28]
- Ernstige incidenten, waarbij een alarmfase (zie onder) in werking treedt, worden opgenomen in de kwartaalrapportage van de CISO.

Beheersmaatregelen m.b.t. alarmering

- Bij grote beveiligingsincidenten wordt gehandeld en opgeschaald volgens de GRIP structuur.

Alarm fase	Kenmerk	Impact	Opschaling	Bijzonderheden
1	Lokaal incident bij één afdeling.	Oplosbaar probleem: bronbestrijding.	In beginsel niet. Probleem wordt opgelost door het team Informatievoorziening.	Melding aan de CISO
2	Incident bij meer dan één organisatie onderdeel	Nog steeds een geïsoleerd probleem: bron - + effectbestrijding.	In beginsel niet. Probleem wordt opgelost door het team Informatievoorziening.	Melding aan de CISO. Melding bij IBD indien nodig. Interne communicatie is optioneel.
3	Concernbreed incident (en mogelijk andere organisaties)	Impact op dienstverlening wordt echt ervaren.	Kernteam komt bij elkaar. Afhankelijk van het incident (impact) wordt geëscaleerd. Bestuur, CIO en management worden geïnformeerd.	Melding aan de CISO. Melding bij IBD (indien nodig) afdeling Interne (en externe) communicatie is vereist.
4	Incident is concern overstijgend (landelijk)	Impact op dienstverlening is manifest.	Mogelijk treedt de GRIP structuur in werking (GRIP Rijk). Het kernteam is dan in beginsel adviserend en voert desgewenst coördinatie (binnen het ICT domein).	Er is sprake van landelijke opschaling via de technische lijn (IBD à NCSC) of via de maatschappelijke lijn (Nationaal Crisis Centrum).

Beheersmaatregelen m.b.t. de opschaling conform de GRIP-structuur

28 *De WBP is hierop aangepast en wordt per 1-1-2016 van krachy. Per 25 mei 2018 geldt hiervoor de Europese verordening AVG.*

Opschaling is cruciaal bij een ramp of crisis. De zogeheten GRIP-structuur speelt daarbij een belangrijke rol. Opschaling vindt plaats op basis van de ernst en omvang van de gebeurtenis. Bij opschaling kunnen de verantwoordelijkheden en bevoegdheden wijzigen. Feitelijk richt de procedure zich op het zoeken naar het meest geschikte afstemmingsniveau.

Bij dagelijkse incidenten handelen de diensten zelf de zaken af. In sommige gevallen vinden één of meer partijen het handig en verstandig ter plaatse afstemming te organiseren en te formaliseren. Dat noemen we GRIP-1: een situatie waarvoor een Commando Plaats Incident (CoPI) wordt ingericht.

Als de situatie wat omvangrijker is en er buiten de plaats van het incident ook maatregelen nodig zijn (bijvoorbeeld ten aanzien van de afvoer van gewonden of een dreigende rookwolk), kan worden opgeschaald naar GRIP-2. Naast het CoPI wordt dan een operationeel team gevormd; meestal op regionaal niveau onder de noemer ROT (Regionaal Operationeel Team). Dit team biedt ondersteuning aan het CoPI.

Situaties waarbij er sprake is van (dreigende) maatschappelijke onrust, komen in aanmerking voor GRIP-3. In deze situaties komt de burgemeester in beeld. Hij of zij laat zich ondersteunen door een gemeentelijk beleidsteam (GBT) met vertegenwoordigers van de belangrijkste betrokken organisaties.

Omdat niet elke ramp of crisis zich aan de gemeentegrenzen houdt, is er ook nog een GRIP-4. Dan gaat het om situaties waarin de ramp of crisis de grenzen van een gemeente overstijgt (of als de betreffende gemeente de situatie niet alleen aankan). In zo'n situatie, zo is in de wet bepaald, krijgt de voorzitter van de veiligheidsregio de leiding en wordt er een regionaal beleidsteam (RBT) gevormd.

Wanneer bij een incident of de vrees daarvoor meerdere veiligheidsregio's betrokken zijn, kunnen de voorzitters van deze veiligheidsregio's in gezamenlijkheid opschalen naar GRIP 5. De bronregio neemt in principe de coördinerende rol op zich. De voorzitter van de bronregio neemt niet de bevoegdheden van de overige betrokken voorzitters veiligheidsregio over.

Wanneer de nationale veiligheid in het geding is en er behoefte is aan sturing door het Rijk kan de Ministeriële Commissie Crisisbeheersing (MCCb) GRIP Rijk afkondigen. GRIP Rijk kan van kracht zijn in combinatie met GRIP 1 t/m 5 of zonder dat er sprake is van opschaling in de veiligheidsregio.

10 Bedrijfscontinuïteit

10.1 Risico's

Volgens de baseline is er sprake van een specifieke set aan te beperken risico's in dit domein:

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

10.2 Doelstellingen

Conform de baseline stellen we als organisatie onszelf de volgende doelstellingen in dit domein:

- Onderbreken van bedrijfsactiviteiten tegengaan en kritische bedrijfsprocessen beschermen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.
- Een adequaat beheerproces van bedrijfscontinuïteit om de uitwerking op de organisatie, veroorzaakt door het verlies van informatie en het herstellen daarvan tot een aanvaardbaar niveau te beperken.
- Informatiebeveiliging is een integraal onderdeel van het totale bedrijfscontinuïteitsproces en andere beheerprocessen binnen de organisatie.

10.3 Beheersmaatregelen

De baseline maakt onderscheid in de volgende specifieke beheersmaatregelen:

- De organisatie voert een business impactanalyse uit. Afhankelijk van de bevindingen worden vervolgacties gepland. De gemeente heeft een eigen plan voor Business Continuity Management (BCM) (bedrijfscontinuïteitsbeheer). In de continuïteitsplannen wordt minimaal aandacht besteed aan:
  - risico's;
  - identificatie van essentiële procedures voor bedrijfscontinuïteit;
  - 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 of testen gehouden om het plan te toetsen (opzet, bestaan en werking). Aan de hand van de resultaten wordt het plan bijgesteld en wordt de organisatie bijgeschoold.

10.4 Beleidsuitgangspunten

Er zijn voor de belangrijkste processen en systemen continuïteits-/uitwijkplannen welke door middel van een beheerst proces tot stand komen. Continuïteitsplannen moeten regelmatig worden getest en actueel worden gehouden.

Figuur 4:• BCM Cyclus

11 Naleving

11.1 Doelstelling

Conform de baseline stellen we als organisatie onszelf de volgende doelstellingen in dit domein:

- Voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van beveiligingseisen.

11.2 Beheersmaatregelen

Organisatorische beheersmaatregelen

- Het verbeteren van de kwaliteit van informatieveiligheid is een continu proces en onderdeel van alle processen waarin wordt gewerkt met gevoelige informatie. Informatieveiligheid is een kwaliteitskenmerk van het primaire proces, waarop het management van elke afdeling stuurt. De kwaliteit wordt gemeten aan:
  - de mate waarin een volledige set aan maatregelen is geïmplementeerd, gebaseerd op vastgesteld beleid;
  - efficiency en 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.
- Het team Informatievoorziening en externe hosting providers 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 Type 1 of Type 2 verklaring).
- Naleving van regels vergt in toenemende mate ook externe verantwoording, bijvoorbeeld voor het gebruik van DigiD, SUWI, BAG en BRP. Aanvullend op dit Informatiebeveiligingsbeleid gelden daarom specifieke normen voor specifieke organisatie onderdelen. [29]
- Periodiek wordt de kwaliteit van informatieveiligheid in opdracht van de CIO onderzocht door auditors en door onafhankelijke externen (bijvoorbeeld door middel van 'penetratietesten').

29 *Door de VNG en BZK wordt gestreefd naar een uniform audit-kader om de verantwoordingslast zo veel mogelijk te beperken.*

Jaarlijks worden diverse audits, assessments en zelfevaluaties gepland. De bevindingen worden door de CISO gebruikt voor de verdere verbetering van de informatieveiligheid.
- In de P&C cyclus wordt door de CISO gerapporteerd over informatieveiligheid aan de hand van de Verklaring Van Toepasselijkheid (= VVT).
- Er wordt een beveiligingsdocumentatiedossier door de CISO aangelegd en onderhouden. Dit dossier bevat alle relevante verplichte en niet verplichte documenten waaruit blijkt of kan worden aangetoond dat aan de specifieke beveiligingseisen is voldaan is voor de diverse audits, assessments en zelfevaluaties.

Wettelijke beheersmaatregelen
- Een overzicht van relevante wet en regelgeving is te vinden bij 15.1.1 Identificatie van toepasselijke wetgeving en contractuele verplichtingen. Zo is het gebruik van persoonsgegevens geregeld in de Wet Bescherming Persoonsgegevens.
- Voor elk type registratie wordt de bewaartermijn, het opslagmedium en eventuele vernietiging bepaald in overeenstemming met wet, regelgeving, contractuele verplichtingen en bedrijfsmatige eisen. 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 mogelijk op rusten, niet worden geschonden.

Beheersmaatregelen m.b.t. Suwinet
- Organisaties en werkwijzen veranderen continu. Dit kan van invloed zijn op de wijze waarop Suwinet wordt gebruikt. Daarom is het van belang om minimaal jaarlijks het algemene informatiebeveiligingsbeleid en het beveiligingsplan van het Suwinet te evalueren en na te gaan of het informatiebeveiligingsbeleid en het beveiligingsplan nog steeds voldoen aan de beveiligingseisen en –randvoorwaarden. Ook is de vraag relevant of risico's voldoende gereduceerd worden. Wanneer dat nodig is leidt de evaluatie tot aanpassing (actualisatie) van het informatiebeveiligingsbeleid en het beveiligingsplan.
- De controle op verleende toegangsrechten en gebruik vindt meerdere keren per jaar plaats. Zeker voor de zogenaamde zware rollen is de periodieke controle op uitgave van rechten en gebruik van die rollen belangrijk. Bij geconstateerde afwijkingen waarbij sprake is van onregelmatigheden zal de gemeente corrigerende maatregelen moeten nemen. Afhankelijk van de soort onregelmatigheden zal de maatregel variëren van beperking van toegangsrechten tot disciplinaire maatregelen bij geconstateerd misbruik van persoonsgegevens.
- Interne controle en analyse kan op verschillende wijzen worden vormgegeven. In de lichtste variant bestaat deze uit het op hoofdlijnen analyseren van het gebruik en in een zware variant worden de opvragingen per gebruiker structureel op rechtmatigheid beoordeeld. De norm kan dan ook op verschillende wijzen worden uitgelegd en toegepast. Het gebruik van Suwinet moet tot op accountniveau (steekproefsgewijs) worden gecontroleerd.. Het alleen controleren door middel van de generieke rapportages kan voldoende zijn maar geeft geen zicht op individuele opvragingen. Voor het onderzoek wordt gebruik gemaakt van een aantal zoeksleutels anders dan op BSN. Wanneer binnen de gemeente opvallend vaak gebruik wordt gemaakt van dit soort zoeksleutels en de organisatie de controle uitsluitend heeft gebaseerd op basis van een generieke rapportage van het BKWI, dan wordt dit als onvoldoende beoordeeld. De gemeente moet beter zicht hebben op het gebruik van Suwinet door individuele medewerkers om oneigenlijk gebruik vroegtijdig te signaleren en te voorkomen. Het BKWI biedt maandelijks een generieke rapportage aan, waarin geaggregeerde en geanonimiseerde gegevens staan. Dit is een handvat bij de controle. Ook het opvragen van specifieke rapportages bij het BKWI is van belang. Een specifieke rapportage kan - in tegenstelling tot een generieke - gegevens bevatten over individuele medewerkers en/of cliënten.
- Van de gemeente wordt verwacht dat deze minimaal twee keer per jaar een generieke rapportage opvraagt bij het BKWI, dat er een procedure is aan de hand waarvan de generieke rapportages worden beoordeeld en dat er rapportages aanwezig zijn waaruit blijkt dat de gemeente deze controles heeft uitgevoerd. Deze rapporteert aan security officer Suwinet.

Aldus vastgesteld door burgemeester en wethouders van de gemeente Lingewaard op 17 augustus 2021,

Mevrouw P.T.A.M Kalfs, burgemeester

de heer I.P. van der Valk, secretaris