gemeente Hollands Kroon

GEMEENTEBLAD

Officiële uitgave van de gemeente Hollands Kroon

Nr. 101838

6 april

2021

Informatiebeveiligingsbeleid 2020 - 2023

Inleiding en samenvatting

1. 1. Inleiding
Voor u ligt het beleidsdocument informatiebeveiliging 2020 - 2023 van de gemeente Hollands Kroon dat richting geeft voor het verder vormgeven en borgen van informatiebeveiliging in de gemeentelijke organisatie. Het beleid bevat algemene kaders, uitgangspunten en managementafspraken tussen het college van B&W en de directie die moeten worden nagekomen.

Gemeente Hollands Kroon wil in alle opzichten een betrouwbare partner zijn. Respect, vertrouwen, contact, bevlogenheid, lef en innovatie zijn de kernwaarden in het doen en laten van alle medewerkers van Hollands Kroon. Een betrouwbare informatievoorziening waarbij de informatie van inwoners wordt beschermd en de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens is geborgd, is hier onlosmakelijk mee verbonden. Niet alleen kan een inadequate beveiliging leiden tot beschadiging van het vertrouwen, maar ook kan de privacy van de inwoner geschaad worden als bijvoorbeeld privéinformatie openbaar wordt of identiteitsgegevens worden misbruikt.

Gemeente Hollands Kroon onderkent in de bedrijfsprocessen aspecten van informatiebeveiliging die bewaakt en gecontroleerd dienen te worden; om zo 'in control' te zijn en daarover op professionele wijze verantwoording af te leggen. De zelfsturende teams spelen een cruciale rol bij het uitvoeren van dit beleid. Zo maken de teams een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente hebben, van de risico's die de gemeente hiermee loopt en van welke van deze risico's onacceptabel hoog zijn.
Dit document legt de basis voor informatiebeveiliging binnen de gemeente. Het BIO (1) normenkader is vastgesteld als basis voor de gemeente en is daarnaast van toepassing op rijksdienst, provincies en waterschappen. Wel is er de mogelijkheid voor afweging door middel van het 'pas toe of leg uit' principe. Dit beleid is naast de BIO in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving, zoals de basisregistraties, Suwi, Paspoorten en ID-bewijzen, maar ook de archiefwet en de Algemene Verordening Gegevensbescherming.
De gemeente waarborgt dat het beleid regelmatig wordt herzien of aangepast op organisatorische veranderingen en technologische ontwikkelingen. Dit om inwoners, partners, bedrijven en de interne organisatie van dienst te zijn en daarbij de informatiebeveiligingsaspecten te continueren en waar mogelijk te verbeteren.

1. De baseline informatiebeveiliging overheid is een instrument waarmee gemeenten in staat zijn om te meten of de organisatie ín control' is op het gebied van informatiebeveiliging.

Hollands Kroon stemt de bedrijfsvoering inzake informatiebeveiliging af op de norm NEN-EN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO).

Het beleid houdt rekening met onder andere:
- De internationale norm voor informatiebeveiliging (NEN-EN-ISO/IEC 27001:2017).(2)
- De Code voor informatiebeveiliging (NEN/ISO 27002) (3).
- Eisen gesteld door derden aan de dienst- en productlevering.
- Baseline informatiebeveiliging overheid (BIO) aangevuld met eigen kaders die door het directie of college specifiek voor Hollands Kroon zijn vastgesteld.
- Eisen voortkomende uit van toepassing zijnde wet- en regelgeving,

waaronder:
- artikel 213a van de gemeentewet;
- de RODIN-richtlijnen voor digitale archivering en volledige substitutie.
- de beveiligingseisen en -richtlijnen voor:
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Basisadministratie Persoonsgegevens en Reisdocumenten (BRP)
- Basisregistraties Adressen en Gebouwen (BAG)
- Basisregistraties Grootschalige Topografie (BGT)

- Basisregistratie Ondergrond (BRO)
- Basisregistratie personen (BRP)
- ICT-beveiligingsrichtlijnen voor webapplicaties (DigiD)
- Paspoorten en Nederlandse Identiteitskaarten (PNIK)
- Paspoort Uitvoeringsregeling Nederland (PUN)
- Regelement rijbewijzen
- Wet structuur uitvoeringsorganisatie werk en inkomen (Suwi)

Om de uitgangspunten op een efficiënte en effectieve wijze te beheren, zijn de bijbehorende normen, controle en maatregelen geregistreerd in een 'Informatiebeveiligings-managementsysteem' (hierna ISMS) (4)zie hoofdstuk 3.4.

2. Opgesteld door technische subcommissie ISO/IEC/JTC 1/SC 27 information security van de internationale organisatie voor standaardisatie (ISO) en het international electrotechnical commision (IEC) en is overgenomen als EN ISO/IEC 27001:2017 (ISO 27001).
3. Informatietechnologie - Beveiligingstechnieken – Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging EN ISO/IEC 27001: 2017 (ISO 27002).
4. ISMS staat voor Information Security Management System.

1.1.1. Doelstelling
Het overkoepelend doel van informatiebeveiliging is het handhaven van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Informatie is in onze samenleving een kostbaar goed dat des te meer zichtbaar wordt als we ons realiseren dat geen enkel dienstverlenend of zakelijk proces uitgevoerd kan worden zonder informatie. Besturing van processen gaat immers altijd op basis van informatie en informatiebeveiliging is daarbij onvermijdelijk. Om te voorkomen dat informatie en informatiesystemen te licht of te zwaar worden beveiligd, vormt risicomanagement een belangrijk onderdeel in dit afwegingsproces voor het treffen van passende beveiligingsmaatregelen. Daarnaast worden de volgende doelen nagestreefd:
- het garanderen van correcte en veilige informatievoorziening;
- het beschermen van kritieke bedrijfsprocessen;
- het beschermen en correct verwerken van persoonsgegevens van inwoners en medewerkers;
- het minimaliseren van risico's;
- het adequaat reageren op incidenten;
- het bereiken van informatiebeveiligingsbewustzijn bij medewerkers, bestuur en alle andere bij de gemeentelijke organisatie betrokken medewerkers, zoals inhuurkrachten, stagiaires en dienstverleners;
- het inbedden van het component informatiebeveiliging in de werkzaamheden van alle organisatieonderdelen;
- het 'in control' zijn op alle informatiebeveiligingsmaatregelen die genomen zijn en die nog nodig zijn, verankerd in een PDCA-cyclus (5) met aansluiting bij de Planning en Control (P&C) cyclus;
- het waarborgen van de naleving van dit beleid.

5 PDCA staat voor plan, do, check, act. Uitleg van de PDCA-cyclus in hoofdstuk 3.4

1.1.2. Bestuurlijke aandacht en de 10 principes voor informatiebeveiliging
Informatiebeveiliging is al vanaf 2014 onder de aandacht van de VNG met als doel de bewustwording op dit onderwerp bij gemeenten op de bestuurlijke agenda te zetten. Destijds is begonnen met de introductie van de Baseline Informatiebeveiliging Gemeenten (BIG) aangevuld met het vanaf 2017 jaarlijks afleggen van verantwoording in de vorm van een collegeverklaring over informatiebeveiliging voor Suwinet, DigiD en de BRP voorzien van een Assurance verklaring van een externe IT-auditor. Inmiddels is de opvolger van de BIG geïntroduceerd, te weten de Baseline Informatiebeveiliging Overheid (BIO). Dit normenkader is van toepassing op alle overheidslagen en is vanaf 2020 van kracht.

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder zichzelf oplegt.
De principes zijn als volgt;

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook de aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.

7. Informatiebeveiliging kost geld.
8. Onzekerheden dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

De principes gaan vooral over de rol van het bestuur bij het borgen van Informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp Informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.
Alle medewerkers van de gemeente Hollands Kroon hebben de verantwoording tot naleving van dit beleid en opvolging van de maatregelen die voortvloeien uit dit beleid. Identificatie van incidenten of het niet voldoen aan het gestelde in dit beleid dient gemeld te worden aan de CISO (6). Alle medewerkers worden actief geïnformeerd over dit beleid en worden verwacht kennis te nemen van de inhoud.

6. Chief information security officer

1.1.3. Informatiebeveiliging als pijler voor privacybescherming
Vanaf 25 mei 2018 is de AVG (7) van kracht en één van de pijlers waarop deze verordening drijft is informatiebeveiliging. De AVG vereist namelijk dat sprake moet zijn van passende organisatorische en technische beveiligingsmaatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Wat passend is vloeit voort uit het risico dat een verwerking van persoonsgegevens met zich meebrengt rekening houdend met de stand van de techniek, de uitvoeringskosten, de aard en omvang van de verwerking(8). Dit vereist een nauwe samenwerking en afstemming tussen het informatiebeveiligings- en het privacy domein. Voor de privacybescherming is overigens een afzonderlijk beleidsdocument vastgesteld.

1.2. Samenvatting
Met het beleidsdocument informatiebeveiliging 2020 – 2023 geeft het college van B&W de kaders en uitgangspunten aan voor het vormgeven en onderhouden van informatiebeveiliging. De uitwerking van dit beleid naar de organisatie ligt bij de directie en de proceseigenaren. De proceseigenaren sturen op risico's, bepalen welke beveiligingsmaatregelen nodig zijn, draagt dit uit naar hun organisatieonderdelen,

7. Algemene Verordening Gegevensbescherming
8. Art 32 AVG

ondersteunen en bewaken de uitvoering ervan en legt aantoonbaar verantwoording af. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen).
Naast dit beleid behoort de gemeente ook te voldoen aan alle wetgeving waarbij rekening gehouden moet worden met informatiebeveiliging zoals de BRP(9) , PUN, SUWI, BAG, BGT, de archiefwet, de AVG en de wet openbaarheid van bestuur (WOB). De Baseline Informatiebeveiliging Overheid (BIO) is het normenkader voor informatiebeveiliging waaraan de gemeente zich conformeert en biedt volop ruimte voor risicoafweging en prioritering voor verbetering.
Waar nodig kan aanvullend beleid worden gedefinieerd op onderwerpen die in dit beleidsdocument in algemene zin zijn geraakt zoals bijvoorbeeld: Toegangsbeleid, wachtwoordbeleid en beleid rond het beheer en veilig gebruik van mobiele apparaten.
Samenvattend:
1. Het college van B&W is eindverantwoordelijk voor de informatiebeveiliging.
2. De directie is verantwoordelijk voor de inrichting en werking van de beveiligingsorganisatie en legt periodiek op een aantoonbare wijze verantwoording af.
3. De directie zorgt ervoor dat voor elk werkproces een proceseigenaar is benoemd. Een proceseigenaar is in het geval van Hollands Kroon een zelfsturend team.
4. Een proceseigenaar is verantwoordelijk voor de informatiebeveiliging van een werkproces inclusief de daaraan gerelateerde informatiesystemen.
5. Een proceseigenaar stelt op basis van een risicoafweging de beveiligingseisen vast voor het werkproces.
6. Op basis van de beveiligingseisen kiest, implementeert en draagt de proceseigenaar de beveiligingsmaatregelen uit.
7. Proceseigenaren leggen periodiek op een aantoonbare wijze verantwoording af over de beveiliging van hun werkprocessen.
8. De CISO ondersteunt de organisatie bij het bewaken en verhogen van de informatieveiligheid en rapporteert hierover periodiek aan de directie en het college van B&W. De CISO onderhoudt de

contacten met de IBD (10) en is voor de organisatie centraal aanspreekpunt voor informatiebeveiliging.
9. Een managementsysteem voor informatiebeveiliging (ISMS) gebaseerd op een plan-do-check-act cyclus (PDCA-cyclus) wordt ingezet als strategisch instrument om:
a. grip te houden op de veelheid aan activiteiten in het kader van informatiebeveiliging, om
b. aan te tonen dat aan gestelde beveiligingseisen wordt voldaan en om
c. daarover aantoonbaar verantwoording te kunnen afleggen.
10. Risicomanagement rondom informatiebeveiliging wordt verder uitgerold op zowel organisatie-, proces- als systeemniveau met als doel te komen tot een evenwichtige balans tussen beveiligingsrisico's en beveiligingsmaatregelen.
11. De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen passend te kunnen beveiligen volgens de wijze gesteld in dit beleid.
12. Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures en richtlijnen voor zover relevant voor hun werkzaamheden.
13. 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 bij de CISO.

(9) BRP staat voor Basisregistratie Personen, PUN staat voor Paspoort uitvoeringsregeling Nederland, SUWI staat voor Wet structuur uitvoeringsorganisatie werk en inkomen, BAG staat voor Basisregistratie adressen en gebouwen en BGT staat voor Basisregistratie Grootschalige Topologie.
(10) Informatiebeveiligingsdienst voor gemeenten

Dit beleidsdocument wordt minimaal één keer per 3 jaar of zodra zich belangrijke wijzigingen voordoen herzien. Het informatiebeveiligingsbeleid van Hollands Kroon is bindend voor iedereen die voor de gemeente werkt of bestuurlijke verantwoordelijkheid draagt.

Alle medewerkers van de gemeente Hollands Kroon hebben de verantwoording tot naleving van dit beleid en opvolging van de maatregelen die voortvloeien uit dit beleid. Identificatie van incidenten of het niet voldoen aan het gestelde in dit beleid dient gemeld te worden aan de CISO.
Alle medewerkers worden actief geïnformeerd over dit beleid en worden verwacht kennis te nemen van de inhoud.
Dit beleidsdocument treedt in werking na vaststelling door het college van B&W. Hiermee komt het oude informatiebeveiligingsbeleid van 2018 te vervallen.

Informatiebeveiliging

2.1 . Visie op informatiebeveiliging

De komende jaren pakt Hollands Kroon door op het verder verhogen van informatieveiligheid en het professionaliseren van de informatiebeveiligingsfunctie in de organisatie. Dat vereist een integrale aanpak, goed opdrachtgeverschap, onderlinge samenwerking en risicobewustzijn waarbij ieder bedrijfsonderdeel betrokken is. De nadruk komt hierdoor te liggen op de governance rond informatiebeveiliging. Ook de BIO haakt hierop in door de verantwoordelijkheid voor informatiebeveiliging in de organisatie nadrukkelijk neer te leggen bij het bestuur en proceseigenaren. Deze verantwoordelijkheid moet ervoor zorgen dat de risico's op het niveau van werkprocessen/informatiesystemen in beeld zijn en dat daar passende beveiligingsmaatregelen voor genomen worden. Risicomanagement wordt hiervoor als middel ingezet. Ook het periodiek afleggen van verantwoording over de risicoafweging en over de effectieve werking van beveiligingsmaatregelen aan de raad komt nadrukkelijk te liggen bij het bestuur en de proceseigenaren en is mede van belang voor het gestelde vertrouwen in de ketensamenwerking binnen de overheid en ketenpartners.

2.2. Definitie en bescherming van informatiebeveiliging

Informatiebeveiliging is het proces van vaststellen van de vereiste beveiliging van informatiesystemen in termen van beschikbaarheid, integriteit en vertrouwelijkheid alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.
Het begrip informatiebeveiliging heeft aldus betrekking op:
- Beschikbaarheid: het zorgdragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- Integriteit: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;

- Vertrouwelijkheid: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

Dit tabel dient als hulpmiddel te worden gebruikt om informatie en de daar bijbehorende classificatie vast te stellen.

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

Het toekennen van classificatieniveaus aan data en/of informatiesystemen is van groot belang, omdat daarmee het (vereiste) beschermingsniveau kenbaar gemaakt wordt. Aan de hand hiervan kan worden bepaald welke beveiligingseisen gelden en welke maatregelen moeten worden genomen. Dit is bijvoorbeeld relevant voor beheerders die lang niet altijd bekend zijn met de inhoud en dus de waarde van data, maar worden geacht adequate beschermingsmaatregelen te treffen. De volgende factoren oefenen invloed uit op de te nemen beveiligingsmaatregelen:
Beleidsuitgangspunten, architectuurprincipes, beveiligingseisen (en hoe deze te interpreteren).

Classificatieniveaus zijn afgeleid van de waarde van data en het belang van het bedrijfsproces waarin deze data een rol speelt. Stel daarom vast wat het belang is van de bedrijfsvoeringprocessen voor de organisatie en hoe deze worden ondersteund door de ICT-voorzieningen. 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.

Classificatie vindt plaats door de kritieke processen van de gemeente te inventariseren aan de hand van: verstoring of uitval van het proces, systeem, eigenaar, gegevens, hardware. Hierbij wordt een link gelegd met de toegepaste informatiemiddelen en informatiesystemen per proces.

2.3. Reikwijdte en afbakening

De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente en externe partijen, voor zowel het gebruik als het beheer daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte systemen, applicaties. Informatiebeveiliging is meer dan alleen de geautomatiseerde informatiesystemen en ICT-infrastructuur. Het gaat om alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, DVD, beeldscherm etc.) en alle informatie verwerkende systemen (de programmatuur, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen) maar vooral ook mensen en processen.

2.4. Grondslagen

De Baseline Informatiebeveiliging Overheid (BIO) geldt als leidraad voor het verder vormgeven van informatiebeveiliging. Een toelichting op dit normenkader is terug te vinden in hoofdstuk 4 van dit beleidsdocument.
Dit beleidsdocument is algemeen van opzet. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen. Hierbij geldt specifieke wet- en regelgeving waar altijd aan voldaan moet worden, zoals de basisregistratie personen (BRP), paspoort uitvoeringsregeling Nederland (PUN), de wet structuur uitvoeringsorganisatie werk en inkomen (SUWI), DigiD, de

basisregistratie adressen en gebouwen (BAG), de basisregistratie grootschalige topologie (BGT), de archiefwet, de algemene verordening gegevensbescherming (AVG) en de wet openbaarheid van bestuur (WOB).
Indien hogere beveiligingseisen worden gesteld vanuit bepaalde kerntaken op grond van wet- en regelgeving dan worden deze eisen geïmplementeerd.
Waar nodig kan aanvullende beleid worden gedefinieerd op onderwerpen die in dit beleidsdocument in algemene zin zijn geraakt.

2.5. Uitgangspunten
Dit beleid hanteert de volgende uitgangspunten:
1. Een betrouwbare informatievoorziening vormt een essentiële succesfactor voor een efficiënte en effectieve bedrijfsvoering. Omdat Hollands Kroon onderdeel uitmaakt van de totale federatieve overheid en ook verbonden is met andere ketenpartijen, heeft een onveilige situatie bij de Hollands Kroon direct gevolgen voor de veiligheid van andere overheden of partijen.
2. Informatiebeveiliging moet bij voorkeur informatiebeveiligingsincidenten voorkomen, respectievelijk de effecten van het optreden van incidenten beperken.
3. Informatiebeveiliging is niet vanzelfsprekend en moet georganiseerd worden. Het vergroten van het bewustzijn en acceptatie van medewerkers over informatiebeveiliging vraagt continue aandacht van de gemeentesecretaris en het lijnmanagement.
4. De informatiebeveiligingstaken worden als integraal onderdeel van de dagelijkse bedrijfsvoering in de organisatie belegd.
5. Risicomanagement rondom informatiebeveiliging wordt verder uitgerold op zowel organisatie-, proces- als systeemniveau met als doel te komen tot een evenwichtige balans tussen beveiligingsrisico's en beveiligingsmaatregelen.
6. De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen passend te kunnen beveiligen volgens de wijze gesteld in dit beleid.
7. Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures en richtlijnen voor zover relevant voor hun functie.
8. 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.
9. Minimaal een keer per 3 jaar of zodra zich belangrijke wijzigingen voordoen wordt het beleidsdocument informatiebeveiliging geactualiseerd.

2.6. Risicobenadering
De insteek van risicomanagement in het kader van de BIO is dat er cyclisch en methodisch vanuit een PDCA-cyclus wordt omgegaan met informatiebeveiliging. Daarbij hanteert de BIO 3 basisbeveiligingsniveaus (BBN).
- Informatiesystemen op BBN1 niveau zijn systemen waarvoor het BBN2 niveau te zwaar wordt gezien. De nadruk voor BBN1 ligt op wat voor de overheid minimaal verwacht mag worden.
- Voor informatiesystemen binnen de overheid vormt BNN2 het uitgangspunt. Er is dan sprake van het verwerken vertrouwelijke informatie of de veiligheid van andere systemen is afhankelijk van de veiligheid van het eigen systeem of dat beveiligingsincidenten leiden tot bestuurlijke commotie.
- BBN3 is van toepassing op gerubriceerde informatie Departementaal Vertrouwelijk dan wel vergelijkbaar vertrouwelijk bij andere overheidslagen, waarbij weerstand tegen statelijke actoren of vergelijkbare dreigingen (denk aan criminele organisaties) nodig is.

Beveiligingsmaatregelen worden getroffen op basis van een toets (GAP-analyse (11)) op de BIO (12) controls en maatregelen. Indien een proces of informatiesysteem privacy of security gevoelig is, kan het zijn dat er aanvullende maatregelen nodig zijn. Hiervoor inventariseert de procesverantwoordelijke (13) de kwetsbaarheid van zijn/haar werkproces en de dreigingen die kunnen leiden tot een beveiligingsincident, rekening houdend met de bescherming eisen van de informatie.
Het risico is de kans op beveiligingsincidenten en de impact daarvan op het werkproces. Deze wordt bepaald de procesverantwoordelijke.

De BIO heeft een werkwijze die gericht is op risicomanagement. Er dient gewerkt te worden volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt in dat men op voorhand keuzes en afwegingen maakt of informatie in bestaande en nieuwe processen voldoende beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid (BIV). De BIV-classificatie is al reeds toegelicht in hoofdstuk 2.2. Aan de hand van deze classificatie wordt het basisbeveiligingsniveau (BBN) bepaald. Is het beveiligingsniveau hoog dan wordt geadviseerd een diepgaande risicoanalyse uit te voeren.

(11) Het doel van de GAP-analyse is om te controleren of en in welke mate de maatregelen uit de BIO geïmplementeerd zijn bij de gemeente die het onderzoek uitvoert of laat uitvoeren. De GAP-analyse (opgesteld door de IBD) bevat alle maatregelen uit de BIO met daarbij controlevragen. De GAP-analyse is een methode om een vergelijking te maken tussen een huidige situatie en de gewenste situatie.
(12) De BIO kent een normenkader waarmee gemeenten in staat zijn om te meten of de organisatie 'in control' is op het gebied van informatiebeveiliging. De Gap-analyse is het instrument waarmee dit wordt gedaan.
(13) Procesverantwoordelijke zijn de zelfsturende teams.

2.7. Afleggen verantwoording
In alle bedrijfsprocessen zijn aspecten van informatiebeveiliging die bewaakt en gecontroleerd dienen te worden; om zo 'in control' te zijn en daarover op professionele wijze verantwoording af te leggen. Gemeente Hollands Kroon onderkent dit. De zelfsturende teams spelen een cruciale rol bij het uitvoeren van dit beleid. Zo maken de zelfsturende teams een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente hebben, van de risico's die de gemeente hiermee loopt en van welke van de risico's onacceptabel hoog zijn.
Gemeenten hebben verder te maken met aanvullende specifieke wetgeving waarvan onderdelen bij ENSIA(14) worden uitgevraagd voor de jaarlijkse verticale en horizontale verantwoording. Het gaat hierbij om wetgeving voor de basisregistraties, Suwi, DigiD en de PUN. De ENSIA-coördinator en CISO leggen verantwoording af over de ENSIA-systematiek.

(14) ENSIA = Eenduidige Normatiek Single Information Audit en is een gezamenlijk project van BZK, de VNG, gemeenten en SZW.

2.8. Ketensamenwerking
Ingeval sprake is van samenwerking binnen de overheid of met ketenpartners waarbij sprake is van uitwisseling van informatie dan zijn nadere schriftelijke afspraken gemaakt over verantwoordelijkheden en het treffen van passende beveiligingsmaatregelen.

Beveiligingsorganisatie

3. 1. Interne organisatie
Om informatiebeveiliging te beheren en blijvend te borgen in de gemeentelijke organisatie is een goed werkende interne organisatie voor informatiebeveiliging nodig. Daarbij horen duidelijke afspraken over de behorende verantwoordelijkheden, taken en rollen die ook als zodanig worden nagekomen. Het gaat hier aldus over de governance rond informatiebeveiliging waarbij onderlinge samenwerking/afstemming bepalend is voor het succes.

Dit beleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau. Dit informatiebeveiligingsbeleid beschrijft op strategisch niveau de informatiebeveiliging. Dit zal vertaald worden in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt en concreet gemaakt in het informatiebeveiligingsplan dat vastgesteld wordt door de directie. Dit wordt gedaan op basis van input van de zelfsturende teams, de FG de CISO, het dreigingsbeeld van de IBD en de uitkomsten van ENSIA. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid wordt gevraagd.

3.2. Verantwoordelijkheden
Het college van B&W is eindverantwoordelijk voor de informatiebeveiliging binnen de organisatie en stelt kaders op voor informatiebeveiliging op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders. Het college van B&W stimuleert de directie en proceseigenaren om passende beveiligingsmaatregelen te treffen binnen de vastgestelde beleidskaders.
De directie is eindverantwoordelijk voor de inrichting en werking van de beveiligingsorganisatie en:
- Stuurt de organisatie aan op beveiligingsrisico's;
- Controleert of de getroffen maatregelen overeenstemmen met de beveiligingseisen en of deze voldoende bescherming bieden;
- Wijst voor elk werkproces/informatiesysteem een proceseigenaar aan.
- Evalueert periodiek de beleidskaders en stelt waar nodig bij;
- Legt aantoonbaar verantwoording af over het gevoerde beleid.

De proceseigenaar is verantwoordelijk voor de integrale beveiliging van de werkproces(sen) en daaraan gerelateerde informatiesystemen. De proceseigenaar:

- Stelt op basis van een expliciete risicoafweging de beveiligingseisen vast voor het werkproces en daaraan gerelateerde informatiesystemen;
- Kiest en implementeert op basis van beveiligingseisen de beveiligingsmaatregelen en draagt deze uit;
- Legt aantoonbaar verantwoording af over de beveiliging van het werkproces;
- Stuurt op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en bewustzijn);
- Meldt incidenten en rapporteert in hoeverre werkprocessen/informatiesystemen voldoen aan het informatiebeveiligingsbeleid van de gemeente.

De teams die verantwoordelijk zijn voor de bedrijfsvoering zijn verantwoordelijk voor de uitvoering van:

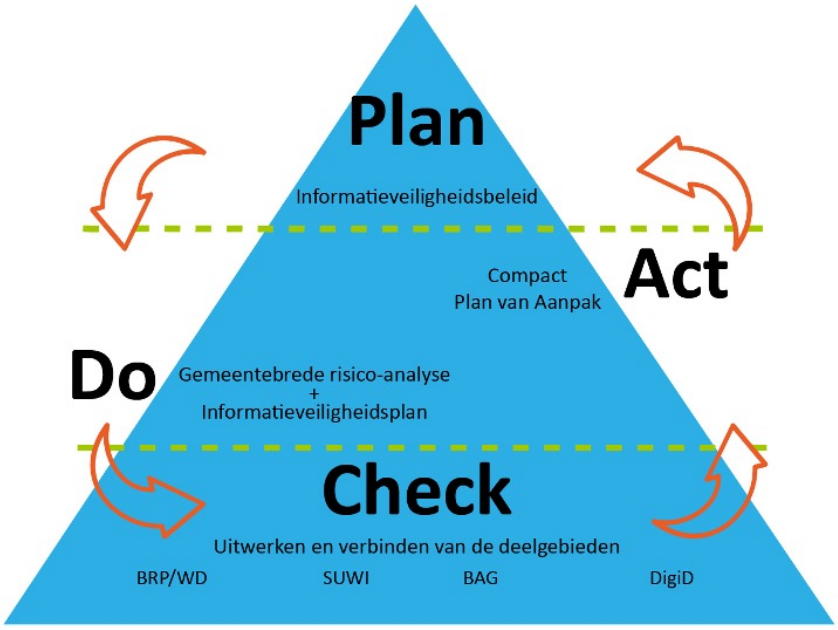
- De beveiliging van de informatievoorziening en implementatie van beveiligingsmaatregelen die voortvloeien uit de beveiligingseisen en bijbehorende risicoanalyse.
- Alle beheeraspecten van informatiebeveiliging die betrekking hebben op ICT-aangelegenheden zoals incident- en probleemmanagement, configuratie- en wijzigingsbeheer, logging van activiteiten en back-up & recovery;
- Maatregelen gericht op beveiliging van personeel zoals screening, geheimhoudings-verklaringen en awareness programma's;
- Maatregelen gericht op beveiliging van gebouwen, publieke en werkruimte van de gemeente;

3.3. Taken en rollen

Het college van B&W stelt formeel het informatiebeveiligingsbeleid vast. Het college delegeert de uitvoering hiervan en informeert de raad periodiek over dit thema. Binnen het college van B&W valt informatiebeveiliging onder de portefeuille van een van de portefeuillehouders. De directie adviseert het college van B&W formeel over het vast te stellen beleid.
De directie geeft sturing aan de uitvoering van het informatiebeveiligingsbeleid en ziet erop toe dat naleving van dit beleid plaatsvindt. De directie zorgt dat voor elk werkproces een proceseigenaar is benoemd die verantwoordelijk is voor de informatiebeveiliging van het werkproces.
De CISO ondersteunt de directie bij de coördinerende en adviserende taken die voortvloeien uit het informatiebeveiligingsbeleid, faciliteert waar nodig de proceseigenaren bij het implementeren van beveiligingsmaatregelen, onderhoudt het managementsysteem voor informatiebeveiliging (ISMS), de contacten met de proceseigenaren en met de IBD en is het centraal aanspreekpunt van de gemeente voor informatiebeveiliging. De CISO is eveneens voor het onderdeel BIO, coördinator voor ENSIA dat als doel heeft het jaarlijks verantwoordingsproces bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijk P&C-cyclus.
Controlerende taken op het gebied van informatiebeveiliging liggen zoveel mogelijk bij team Effect (VIC).

3.4. Managementsysteem voor informatiebeveiliging (ISMS)

De gemeente maakt gebruik van een managementsysteem voor informatiebeveiliging (ISMS) om het interne beheersingsproces te ondersteunen rondom informatiebeveiliging gebaseerd op een plan-do-check-act cyclus (PDCA-cyclus) met bijbehorende rapportages. De CISO is belast met het beheer van dit systeem. Het ISMS is een integraal kwaliteitssysteem van informatiebeveiliging conform ISO 27001:2017 en is in lijn met de operationele procedures van Hollands Kroon en aan de relevante landelijke en Europese wet- en regelgeving. Het ISMS bevat een informatie-beveiligingsmanagementproces dat is ingericht op basis van een PDCA-cyclus (Plan, Do, Check, Act). Door middel van het doorlopen van de PDCA-cyclus wordt gemonitord of de genomen beheersmaatregelen nog effectief zijn en zich nieuwe of andere risico's voordoen die nog niet (voldoende) beheerst worden. Het zorgt er dus voor dat een passend beveiligingsniveau wordt gehandhaafd.



Dit betekent concreet het volgende:

- Jaarlijks wordt een plan opgesteld voor het verbeteren van de informatiebeveiliging. Dit plan wordt formeel vastgesteld;
- De proceseigenaren treffen maatregelen om de beveiligingsrisico's te verminderen en om compliant te zijn aan wet- regelgeving, landelijke normen en de BIO;
- De CISO stelt jaarlijks vast welke (rest-) risico's er zijn door middel van een risicoanalyse;
- Er wordt periodiek door de zelfsturende teams zelfevaluaites en/of interne/externe audits uitgevoerd voor de BRP, PNIK, BAG, BGT en Suwi en eventueel andere toekomstige wettelijke normenkaders;
- De zelfsturende teams evalueren jaarlijks dit beleid en stellen een verbeterplan op naar aanleiding van een uitgevoerde interne/externe audit.

Baseline Informatiebeveiliging Overheid (BIO)

4. 1. Inleiding

De BIO beoogt de beveiliging van informatie(systemen) bij alle bestuurslagen en bestuursorganen van de overheid te bevorderen, zodat alle overheidslagen erop kunnen vertrouwen dat onderling uitgewisselde gegevens, in lijn met wet- en regelgeving, passend beveiligd zijn. De BIO helpt het bestuur en proceseigenaren bij het nemen van hun verantwoordelijkheden ten aanzien van informatiebeveiliging. Vanaf 2020 is de BIO van kracht voor alle overheidslagen waarbij gemeenten zich in 2019 hadden kunnen voorbereiden op de overgang van BIG naar BIO.
De BIO richt zich nadrukkelijk op een stevig gefundeerde governance waarbij de directie verantwoordelijk is voor de beveiligingsorganisatie. De proceseigenaren zijn ieder verantwoordelijk voor informatiebeveiliging voor zover dat hun werkprocessen raakt. Dan gaat het zowel over het werkproces, de (direct) betrokken medewerkers als de ondersteunende informatiesystemen. Het beveiligen van informatie is geen eenmalige zaak, maar een proces waarbij steeds de PDCA-cyclus wordt doorlopen voorzien van de daarbij behorende managementrapportages. Om te voorkomen dat informatie en informatiesystemen te licht of te zwaar worden beveiligd, vormt risicomanagement een belangrijk onderdeel in dit proces. De CISO ondersteunt de directie, het college en de proceseigenaren in het realiseren en onderhouden van het gewenste beveiligingsniveau.

4. 2. Toelichting BIO

De BIO bevat de volgende hoofdstukindeling:

- H5: Informatiebeveiligingsbeleid
- H6: Organiseren van informatiebeveiliging

- H7: Veilig personeel
- H8: Beheer van bedrijfsmiddelen
- H9: Toegangsbeveiliging
- H10: Cryptografie
- H11: Fysieke beveiliging en beveiliging van de omgeving
- H12: Beveiliging bedrijfsvoering
- H13: Communicatiebeveiliging
- H14: Acquisitie, ontwikkeling en onderhoud van informatiesystemen
- H15: Leveranciersrelaties
- H16: Beheer van informatiebeveiligingsincidenten
- H17: Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
- H18: Naleving

Een toelichting op deze onderwerpen waaraan voldaan moet worden is opgenomen in de volgende paragrafen.

4.2. 1. Informatiebeveiligingsbeleid
Het informatiebeveiligingsbeleid is een document en 'doet' op zich nog niets. Het is een communicatiemiddel naar alle betrokkenen en bevat naast kaders en uitgangspunten managementafspraken tussen het college van B&W en de directie met als doel richting te geven aan het vormgeven van informatiebeveiliging in de gemeentelijke organisatie. Zonder beleid neemt de kans op onvoorspelbare resultaten toe. Het is van belang dat het beleid periodiek beoordeeld wordt om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.

4.2. 2. Organiseren van informatiebeveiliging
Dit onderdeel zoomt in op een beheerkader om de implementatie en uitvoering van informatiebeveiliging binnen de organisatie te initiëren en te beheersen. Een interne organisatie van informatiebeveiliging met een evenwichtige verdeling van taken en verantwoordelijkheden is daarvoor nodig. Conflicterende taken en verantwoordelijkheden worden zoveel mogelijk vermeden om de kans op onbedoeld of onbevoegd wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.
Onder deze noemer valt ook het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur dat steeds meer zijn intrede doet.

4.2. 3. Veilig personeel
Met veilig personeel wordt bedoeld dat er waarborgen zijn dat voorafgaand aan het dienstverband medewerkers en contractanten hun verantwoordelijkheid begrijpen en geschikt zijn voor de rollen waarvoor zij in aanmerking komen. Het gaat dan om maatregelen gericht op screening en arbeidsvoorwaarden. Tijdens het dienstverband behoren medewerkers en contractanten bewust te zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze na te komen. Instructies, gedragsregels en bewustwordingsprogramma's spelen hier een belangrijke rol. Bij het beëindigen van een dienstverband ligt de nadruk op het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband.

4.2.4. Beheer van de bedrijfsmiddelen
De organisatie moet weten welke bedrijfsmiddelen gebruikt worden, wie verantwoordelijk is voor de beveiliging (proceseigenaar) van deze middelen en welk beveiligingsniveau voor elk bedrijfsmiddel van toepassing is. Dit vereist inventarisatie, classificatie en passende bescherming van bedrijfsmiddelen in overeenstemming met het belang ervan voor de organisatie. Ook het aanvaardbaar gebruikmaken van bedrijfsmiddelen door het personeel valt hieronder. Onzorgvuldig gebruik van bedrijfsmiddelen zoals verwijderbare media kan immers leiden tot grote beveiligingsincidenten.

4.2.5. Toegangsbeveiliging
De toegang tot informatie en informatie verwerkende faciliteiten behoort te worden beperkt tot datgene wat noodzakelijk is. Het gaat dan om de toegang tot het netwerk van de gemeente, netwerkdiensten en informatiesystemen. Dat vereist naast toegangsbeleid ook beheer van toegangsrechten om toegang voor bevoegde gebruikers te bewerkstelligen en onbevoegde toegang tot systemen en diensten te voorkomen en waar nodig gebruik te maken van een beveiligde inlogprocedure. Gebruikers zijn verantwoordelijk voor het beschermen van hun authenticatie-informatie zoals wachtwoorden.

4.2.6. Cryptografie
Ter bescherming van informatie is het gebruik van cryptografie (15) een effectieve maatregel. Aan het gebruik van cryptografie kleven echter risico's zoals

a. het verlies van sleutels waardoor versleutelde data niet meer in leesbare vorm teruggezet kunnen worden of
b. het gebruik van zwakke sleutels waardoor versleutelde data door onbevoegden alsnog in leesbare vorm teruggezet kunnen worden. Voor correct en doeltreffend gebruik van cryptografie is beleid nodig om aan te geven wanneer cryptografie wordt ingezet en in welke vorm, wie verantwoordelijk is en hoe het beheer en gebruik van cryptografie geregeld moet worden. Het gebruik van verplichte PKI-overheid certificaten valt hieronder.

4.2.7. Fysieke beveiliging en beveiliging van de omgeving
Fysieke beveiliging richt zich op het voorkomen van onbevoegde fysieke toegang tot (gebieden rondom) gebouwen, kantoren, ruimte en faciliteiten. Daarnaast richt de fysieke beveiliging zich op het voorkomen van verlies, schade, diefstal of het compromitteren van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie.

4.2.8. Beveiliging bedrijfsvoering
Een correcte en beveiligde bediening van informatie verwerkende faciliteiten behoort te zijn gewaarborgd waaronder de installatie van operationele software. Dit raakt voor een groot deel de dagelijkse ICT-faciliteiten die nodig zijn voor een continue bedrijfsvoering. Voorts zijn waarborgen nodig dat informatie en informatie verwerkende faciliteiten zijn beschermd tegen malware en dat er goed werkende back-up voorzieningen zijn tegen verlies van gegevens. Het vastleggen van alle relevante gebeurtenissen (logging) en verzamelen van bewijs bij storingen of beveiligingsincidenten zijn noodzakelijk om te monitoren en om achteraf (gerichte) controles te kunnen uitvoeren of om fouten/storingen sneller te herstellen.

4.2.9. Communicatiebeveiliging
Communicatiebeveiliging gaat over het waarborgen van de bescherming van informatie in netwerken en de ondersteunende informatie verwerkende faciliteiten. Denk hierbij aan al het dataverkeer dat over het netwerk gaat maar ook aan het handhaven van de beveiliging van informatie die wordt uitgewisseld in de organisatie en met externe partijen. Voor het gebruik van gemeentelijke informatie gelden de rechten en plichten zoals vastgelegd in het CAR-UWO, huisregels, integriteitsverklaring, belofte of eed.

(15) Versleutelen van informatie

4.2.10. Acquisitie, ontwikkeling en onderhoud van informatiesystemen
Beveiligingseisen voor informatiebeveiliging behoort standaard onderdeel te zijn in het kader van acquisitie. Informatiebeveiliging waaronder 'privacy by designtechnieken' behoort een vast onderdeel te zijn in het inkoopproces als het gaat om de aanschaf van informatie verwerkende faciliteiten. Bij de ontwikkeling, implementatie (denk aan projectmanagement) en onderhoud van informatiesystemen behoort informatiebeveiliging eveneens een vast onderdeel te zijn. Daarnaast behoren er waarborgen te zijn voor het beschermen van gegevens die voor testdoeleinden worden gebruikt. Daarbij geldt vanuit de privacywetgeving dat het testen met persoonsgegevens niet is toegestaan.

4.2.11. Leveranciersrelaties
Met leveranciers die toegang (moeten) hebben tot informatie en informatie verwerkende faciliteiten van de gemeente behoren beveiligingseisen te worden overeengekomen en gedocumenteerd om de bescherming van bedrijfsmiddelen te waarborgen. Dit speelt bij offerteaanvragen en contractmanagement waarbij informatie(voorziening) een rol speelt evenals bij het handhaven van de gemaakte beveiligingsafspraken. Hiervoor bestaat de GIBIT als gemeenschappelijke inkoopvoorwaarde bij IT.

Als er gebruik wordt gemaakt van bedrijfsmiddelen die toegankelijk zijn voor of uitbesteed zijn aan leveranciers. Dan is het voor de beveiliging noodzakelijk dat er een verwerkersovereenkomst wordt overlegd waarin de leverancier aantoont dat zij voldoen aan alle informatiebeveiligingseisen. Indien het een nieuwe leverancier betreft dan dient dit meegenomen te worden in het inkooptraject, waarbij tevens een risicoafweging wordt gemaakt. Het beveiligingsbeleid van de leverancier moet dezelfde garanties geven als het beveiligingsbeleid van Hollands Kroon en/of dat past bij het product of dienst.

4.2.12. Beheer van informatiebeveiligingsincidenten
Dit onderdeel richt zich op het bewerkstelligen van een consistente en doeltreffende aanpak van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging. Procedures voor onder meer incidentenbestrijding en -herstel met vermelding van taken en verantwoordelijkheden en rapportages van informatiebeveiligingsgebeurtenissen zijn hierbij essentieel. Hier ligt ook een duidelijke relatie met datalekken voor zover het gaat om persoonsgegevens.

Als er sprake is van een datalek dan dient deze direct gemeld te worden bij de CISO d.m.v. het melding registratiesysteem. Deze wordt opgepakt en voorgelegd aan een securityoverleg. Voor afhandeling geldt er een rapportage en escalatielijn volgens het incidentmeldingen beheerplan.
Voorbeelden van data/beveiligingslekken en beveiligingsincidenten zullen via voorlichting en communicatie in het kader van bewustwording duidelijk gemaakt moeten worden. Daarnaast kan er van incidenten geleerd worden om de kans van optreden in de toekomst te verminderen.
Er is sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Hierbij kan gedacht worden aan bijvoorbeeld het kwijtraken van een USB-Stick of externe harde schijf, een verkeerd verstuurde e-mail, diefstal van een laptop of telefoon of aan inbraak van een hacker. Een beveiligingslek is een zwakke plek als gevolg van een menselijke fout of een zwakker plek in het systeem (hard- of software), die functies toelaat die niet toegestaan zijn, of onbevoegden toegang tot gegevens of functies verschaft. Beveiligingslekken kunnen berusten op programmeerfouten, ontwerpfouten of verkeerde configuraties. Hierbij heeft ICT een rol maar ook de functioneel beheerder die de toegang tot de systemen/data autoriseren en kunnen monitoren.

4.2.13. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
Bedrijfscontinuïteitsbeheer is van belang om onderbreking van bedrijfsactiviteiten tegen te gaan en vitale bedrijfsprocessen te beschermen tegen de gevolgen van een omvangrijke storing in de bedrijfsvoering of een crisis of een ramp om tijdig herstel te bewerkstelligen. De organisatie behoort in dat kader de eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties vast te stellen. Deze kunnen anders zijn dan onder normale uitvoeringsomstandigheden. Voorts behoren processen, procedures en beheersmaatregelen te worden vastgesteld, gedocumenteerd, geïmplementeerd en te worden gehandhaafd om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen. Periodieke verificatie, beoordeling en evaluatie van deze geïmplementeerde beheersmaatregelen behoort plaats te vinden om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.

4.2.14. Naleving
Dit onderdeel is gericht op het voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen. Hieronder vallen ook de licenties en intellectuele eigendomsrechten en naleving van de privacywetgeving.
Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.
Het verbeteren van de kwaliteit van informatieveiligheid is een continu proces en onderdeel van alle gemeentelijk processen waarin wordt gewerkt met gevoelige informatie. Informatieveiligheid is een kwaliteitskenmerk van het primaire proces, waar continu op gestuurd moet worden. Deze 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 informatiebeveiliging het bereiken van de strategische doeleinden ondersteunt.

Periodieke beoordelingen zijn nodig om (aantoonbaar) te verzekeren dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie. Een goed werkend managementsysteem voor informatiebeveiliging (ISMS) gebaseerd op een PDCA-cyclus draagt hiertoe aan bij.