Informatiebeveiligingsbeleid

gemeente Lisse

november 2017

Inhoud

1 Inleiding

Gemeenten zijn voor steeds meer beleidsterreinen verantwoordelijk. In vrijwel alle gevallen wordt daarbij gebruik gemaakt van de mogelijkheden van informatie-uitwisseling. Door informatie te delen en processen te optimaliseren kan onder meer de dienstverlening beter georganiseerd worden, de veiligheid van burgers worden verbeterd en meer mensen aan het werk komen. Ook voor de decentralisatie van taken op gebied van werk, jeugdzorg en AWBZ wisselen we onderling en met diverse ketenpartners informatie uit.

Naast de uitvoering van werkzaamheden op de hiervoor genoemde gebieden, wordt ook onze rol van 'gegevensbeschermer' belangrijker. De media om ons heen maken steeds vaker melding van hackers, ransomware, virussen, identiteitfraude, et cetera; bedreigingen, die de uitvoering van onze maatschappelijke rol meer en meer in gevaar brengen. Als professionele organisatie is het dus noodzakelijk dat we ook de beveiliging van informatie(systemen) professioneel organiseren.

Dit document geeft algemene beleidsuitgangspunten over informatiebeveiliging, bedoeld voor de gemeenten Hillegom, Lisse en Teylingen en de werkorganisatie HLTsamen. De Informatie-beveiligingsdienst (IBD) zorgde voor het format, gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Dit beleidsdocument wordt vastgesteld door de afzonderlijke colleges van de drie gemeenten en het bestuur van de werkorganisatie HLTsamen. Het beleid vormt de basis van een gedegen opzet en verdere uitwerking van de informatiebeveiliging. Directie en management zijn verantwoordelijk voor verdere uitwerking en concretisering van het beleid; de adviseur informatiebeveiliging (CISO) van HLTsamen ondersteunt hierbij. De colleges en het bestuur van HLTsamen worden periodiek over de uitwerking van het beleid gerapporteerd.

Informatiebeveiliging

Informatiebeveiliging is de verzamelnaam voor de processen die ingericht worden om de betrouwbaarheid van gemeentelijke 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 zorgdragen voor het beschikbaar zijn van informatie en informatie-verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- Integriteit / betrouwbaarheid: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- Vertrouwelijkheid / exclusiviteit: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

Reikwijdte en afbakening informatiebeveiliging

Informatiebeveiliging is veel meer dan ICT, computers en automatisering. Het gaat om:

- *alle* uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis),
- *alle* mogelijke informatiedragers (papier, digitaal, foto/film, CD/DVD, beeldscherm, etc.) en
- *alle* informatie-verwerkende systemen (programmatuur, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen).

En daarnaast gaat het vooral ook om 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.

2 Informatiebeveiligingsbeleid Hillegom, Lisse, Teylingen en HLTsamen

De drie colleges en bestuur & management van HLTsamen spelen een cruciale rol bij de opzet en uitvoering van (informatie)beveiligingsbeleid. De colleges verstrekken opdracht om aanvullend beleid en procedures op te (laten) stellen en adequate (beveiligings)-maatregelen te treffen. Naar aanleiding daarvan, wordt een inschatting gemaakt van:

- het belang dat de verschillende delen van de informatievoorziening voor de organisatie hebben,
- de risico's die hiermee gelopen worden en
- welke van deze risico's onacceptabel hoog zijn.

Op basis hiervan werkt het management dit beleid voor informatiebeveiliging verder uit, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Bestuur en management van HLTsamen geven duidelijke richting aan informatiebeveiliging. Zij laten zien dat zij informatiebeveiliging ondersteunen en zich hierbij betrokken voelen. Dit doen ze, door het uitbrengen en handhaven van (aanvullend) informatiebeveiligingsbeleid dat van toepassing is op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de organisatie en de relevante landelijke en Europese wet- en regelgeving.

De organisatie 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 Basisregistratie Personen (BRP), Structuur uitvoeringsorganisatie Werk en Inkomen (SUWI), Basisregistratie Adressen en Gebouwen (BAG), Paspoortuitvoeringsregeling (PUN) en archiefwet.
- Er is een gemeenschappelijk normenkader, met als basis de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
- Het bestuur van HLTsamen stelt dit normenkader vast, waarbij er ruimte is voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.
- Bij de totstandkoming van het beleid heeft afstemming plaats gevonden met het project 'Integrale veiligheid'. Ook in de vervolgstappen vindt deze afstemming plaats.

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

1. Alle informatie en informatiesystemen zijn van kritiek en vitaal belang voor de HLT-organisatie. De verantwoordelijkheid voor informatiebeveiliging ligt bij het (lijn)management, met de colleges van B&W van de drie gemeenten en het bestuur van HLTsamen als eindverantwoordelijken. De verantwoordelijkheden voor de bescherming van gegevens en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd.
2. Door periodieke controles, organisatie-brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen HLTsamen. Het informatiebeveiligings*beleid* vormt samen met het informatiebeveiligings*plan* het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatie-breed 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 managementsysteem van informatiebeveiliging.
4. De adviseur informatiebeveiliging / Chief Informationsecurity Officer (CISO) ondersteunt vanuit een *onafhankelijke* positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover.
5. HLTsamen 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 worden vastgelegd en vastgesteld. Alle medewerkers worden getraind in het gebruik van de van belang zijnde 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.

3 Uitgangspunten informatiebeveiliging Hillegom, Lisse, Teylingen en HLTsamen

Het belang van informatie(veiligheid)

Informatie is een belangrijk bedrijfsmiddel voor de drie gemeenten en HLTsamen. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben. Incidenten hebben mogelijk negatieve gevolgen voor burgers, bedrijven, partners en/of de eigen organisatie met mogelijk ook politieke consequenties. Informatie*veiligheid* is daarom van groot belang; informatie*beveiliging* is het proces dat dit belang dient.

Visie

> Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de organisatie en vormt de basis voor het beschermen van rechten van burgers en bedrijven.[1] Dit vereist een integrale aanpak, waarin iedere manager verantwoordelijk is voor de veiligheid en beveiliging van minimaal zijn/haar eigen organisatieonderdeel en processen. Het succes van beveiligen en daarmee de mate van betrouwbaarheid hangt voornamelijk af van houding en gedrag van ieder individuele medewerker. Activiteiten rond beveiliging en veiligheid moeten daarom voor een belangrijk deel hierop gericht zijn.

Het proces van informatiebeveiliging is primair gericht op bescherming van gemeentelijke informatie, maar is tegelijkertijd een zogenaamde '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, et cetera). Het gaat ook niet alleen over ICT: verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid.[2]

Doelstelling

Dit informatiebeveiligingsbeleid is het kader voor passende organisatorische en technische maatregelen, ter bescherming van gemeentelijke informatie. Ook draagt het beleid ertoe bij, dat de organisatie kan voldoen aan relevante wet- en regelgeving en het legt voor HLTsamen de basis om 'in control' te zijn en daarover op professionele wijze verantwoording af te leggen. In control betekent in dit verband:

- de organisatie weet waar ze aan moet voldoen,
- de organisatie weet welke maatregelen genomen zijn,
- er is een SMART (Specifiek, Meetbaar, Acceptabel, Realistisch, Tijdsgebonden) planning van de maatregelen die nog niet genomen zijn en
- dit geheel is verankerd in de PDCA (Plan, Do, Check, Act)-cyclus.

[1] Met betrouwbaarheid wordt bedoeld: 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 HLT Samen verricht.

Uitgangspunten

- Het informatiebeveiligingsbeleid van de drie gemeenten en HLTsamen is in lijn met het algemene beleid van de organisatie en de relevante landelijke en Europese wet- en regelgeving.[3]
- Het beleid is gebaseerd op de Code voor Informatiebeveiliging (NEN/ISO 27002) en de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
- Het (algemene) informatiebeveiligingsbeleid wordt vastgesteld door de drie colleges van B&W en het bestuur van HLTsamen. De HLT-directie herijkt dit beleid periodiek.

Risicobenadering

De aanpak van informatiebeveiliging in HLTsamen is 'risk based'. Dat wil zeggen, dat beveiligings-maatregelen worden getroffen op basis van een toets - de GAP-analyse - tegen de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) van VNG/KING. Indien een systeem méér of zwaardere maatregelen nodig heeft, wordt een risicoanalyse uitgevoerd. Daartoe inventariseert de proces-eigenaar de kwetsbaarheid van zijn werkproces en de dreigingen die kunnen leiden tot een beveiligingsincident, rekening houdend met de beschermingseisen van de informatie. Het risico is de kans op beveiligingsincidenten en de impact daarvan op het werkproces en wordt dus bepaald door de proceseigenaar, oftewel: **risico = kans x impact**.

Doelgroepen

Het gemeentelijk informatiebeveiligingsbeleid is bedoeld voor alle in- en externe medewerkers van de gemeentelijke organisaties en de werkorganisatie HLTsamen. In het onderstaande schema staan de verschillende functies/groepen en hun rol binnen de informatiebeveiliging.

Doelgroep	Relevantie voor IB-beleid
Colleges van B&W en het bestuur van HLTsamen	Integraal (eind)verantwoordelijk
Bestuur HLTsamen	Stelt waar nodig nader beleid vast
Directie HLTsamen	Stelt nader beleid en plannen op en implementeert
Domein- en teammanagers	Sturen op informatieveiligheid en naleving
Medewerkers	Gedrag en naleving
Gegevenseigenaren	Classificatie: bepalen van beschermingseisen van informatie
Beleidmakers	Planvorming binnen informatiebeveiligingskaders
IB-functionarissen	Dagelijkse coördinatie van IB
Juridische Zaken	Privacy – Functionaris gegevensbescherming
Personeelszaken	Arbeidsvoorwaardelijke zaken
Facilitaire zaken	Fysieke toegangsbeveiliging
ICT-diensten (en -ontwikkelaars)	Technische beveiliging
Functioneel beheerders	Informatiebeveiliging binnen vakgebied en -toepassing
Auditors en controller	Onafhankelijke toetsing
Leveranciers en ketenpartners	Compliancy (voldoen aan gestelde eisen)

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

Scope

De scope van dit beleid omvat:

- alle gemeentelijke processen,
- onderliggende informatiesystemen,
- informatie en gegevens van de organisatie en externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Dit beleid is een algemene basis. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen.[4]

Uitwerking

Na vaststelling van dit informatiebeveiligings*beleid* stelt het HLT-bestuur nadere kaders vast. De uitwerking hiervan wordt vastgelegd in één of meerdere informatiebeveiligings*plan(nen)*. Zo'n plan is de basis voor de PDCA-cylus (Plan Do Check Act). Beleid en uitvoering dienen steeds met elkaar in overeenstemming te blijven, zodat informatiebeveiliging een vast onderdeel in de organisatie blijft.

De te nemen maatregelen moeten worden afgestemd op de risico's. Hierbij moet rekening 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 afzwakken van de risico's disproportioneel hoog zijn. Kort gezegd: risico's en tegenmaatregelen dienen in balans te zijn.

Middelen

Bij de uitwerking van dit beleid doen zich dus ongetwijfeld situaties voor, waarin (aanvullende) beveiligingsmaatregelen genomen moeten worden. Omdat het beeld rond de uitgangssituatie (nulmeting) nog niet compleet is, is op dit moment geen indicatie van die *extra* middelen te geven. Vooralsnog maken we gebruik van bestaande formatie en budget. Bij verdere uitwerking van het plan worden risico-analyses en afwegingen gemaakt; hierbij dienen ook de beschikbare middelen te worden meegenomen. Indien deze voor de betreffende maatregel(s) ontoereikend zijn, dan wordt een voorstel voor de benodigde aanvulling gedaan.

Gebruik

Dit informatiebeveiligingsbeleid en de nog op te stellen informatiebeveiligingsplannen kunnen worden gebruikt voor diverse audits en toetsingen op dit gebied. Per specifiek onderdeel, zoals de Basisregistratie Personen (BRP), moet aanvullend beleid worden vastgesteld. Voor elke interne of externe audit worden het betreffende, vastgestelde informatiebeveiligingsbeleid en het bijbehorende informatiebeveiligingsplan als basis genomen. Door de PDCA-cyclus wordt actualisatie gewaarborgd.

[4] Bijvoorbeeld SUWI (Structuur Uitvoeringsorganisatie Werk en Inkomen) en gemeentelijke basisregistraties.

Werking

Dit informatiebeveiligingsbeleid treedt in werking na vaststelling door het college van B&W van Lisse; het komt in de plaats van het 'Informatiebeveiligingsbeleid 2013-2015' dat op 26-03-2013 werd vastgesteld.

4 Organisatie van de informatiebeveiliging

4.1 Interne organisatie

Risico

Verantwoordelijkheden en bijbehorende activiteiten, procedures en instrumenten moeten expliciet belegd worden. Gebeurt dit niet, dan kan het daadwerkelijk en structureel uitvoeren en borgen van de beheersmaatregelen een probleem worden. Hierdoor kunnen belangen van burgers, bedrijven en (keten) partners geschaad worden.

Doelstellingen

- Beheren van de informatiebeveiliging binnen de organisaties.
- Vaststellen van het beheerkader om de implementatie van informatiebeveiliging in de organisatie te initiëren en te beheersen.
- Goedkeuring door de colleges en het bestuur van HLTsamen van het (algemene) informatiebeveiligingsbeleid.
- Toewijzing van de rollen.
- Coördinatie en beoordeling van de implementatie van het beleid binnen de organisatie.

Verantwoordelijkheden

- De drie colleges van Burgemeester en Wethouders:
  - integraal verantwoordelijk voor de beveiliging van informatie binnen de werkprocessen van de gemeenten én HLTsamen;
  - vaststellen beleid voor informatiebeveiliging op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders.
- Het bestuur van HLTsamen:
  - verantwoordelijk voor nadere kaderstelling waar nodig;
  - periodiek evalueren en eventueel bijstellen van beleidskaders.
- De directie van HLTsamen:
  - verantwoordelijk voor sturing op concernrisico's;
  - opstellen en implementeren nader beleid en plannen;
  - controleren of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden.
- Het managementteam van HLTsamen:
  - verantwoordelijk voor de integrale beveiliging van de verschillende organisatieonderdelen;
  - vaststellen betrouwbaarheidseisen voor de informatiesystemen (classificatie), op basis van een expliciete risicoafweging.
- De domein-/teammanagers:
  - verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
  - controleren of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden;
  - sturen op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn);
  - rapporteren over compliance aan wet- en regelgeving en algemeen beleid van HLTsamen in de managementrapportages.

- Het domein Bedrijfsvoering:
  - verantwoordelijk voor beveiliging van de informatievoorziening en implementatie van beveiligingsmaatregelen, die voortvloeien uit betrouwbaarheidseisen (classificaties);
  - verantwoordelijk voor alle beheeraspecten van informatiebeveiliging, zoals ICT-securitymanagement, incident- en problemmanagement, facilitaire en personele zaken;
  - verzorgen van logging, monitoring en rapportage;
  - leveren van beveiligingsadviezen aan klanten.

4.2 Taken en rollen

- De colleges van Hillegom, Lisse en Teylingen en het bestuur van HLTsamen stellen het (algemene) informatiebeveiligingsbeleid vast. De uitvoering van het beleid moet gecontroleerd worden. Zowel de colleges als het bestuur van HLTsamen als de gemeenteraden (controlefunctie) kunnen opdracht geven om dit te (laten) controleren. De directie van HLTsamen adviseert de colleges en het bestuur van HLTsamen over het vast te stellen beleid.
- De domeinmanager Bedrijfsvoering geeft, in zijn rol als Chief Information Officer (CIO), namens de directie op dagelijkse basis invulling aan zijn sturende rol. Hij doet dit door besluitvorming in de directie voor te bereiden en toe te zien op de uitvoering ervan. De informatiebeveiligingstaken die hieruit voortvloeien zijn belegd bij de Adviseur Informatiebeveiliging / Chief Information Security Officer (CISO) en de beleidsmedewerker Informatisering en Beveiliging / Information Security Officer (ISO).
- De CISO adviseert gevraagd en ongevraagd over informatiebeveiliging én verzorgt de jaarlijkse rapportages aan de colleges over de stand van zaken. Ook de coördinatie van de informatiebeveiliging is belegd bij de CISO. Uitvoerende taken worden zoveel mogelijk belegd bij de teammanagers; zij rapporteren aan de CISO. De CISO rapporteert twee keer per jaar (concern-breed) aan bestuur en directie over het functioneren van de informatiebeveiliging.
- De ISO is werkzaam op het operationele niveau binnen de organisatie. De werkzaamheden van de ISO beslaan onder meer het uitvoeren van de informatiebeveiligingsafspraken van de CISO met het management. Tevens werkt hij samen met de 'Chief' tijdens het opstellen van het beleid. Hierbij valt te denken aan het maken van risico-analyses, het opstellen van minimum veiligheidseisen en het digitaal rechercheren.
- De Functionaris Gegevensbescherming (FG) van het team Juridische Zaken richt zich meer specifiek op (gebruik en beveiliging van) persoonsgegevens.
- In het team Automatisering is een Security-Functionaris (SF) aangewezen voor dagelijks beheer van technische informatiebeveiligingsaspecten. Deze functionaris rapporteert aan de CISO.
- Ook in de overige teams worden medewerkers aangewezen, die namens het team contactpersoon voor de informatiebeveiliging zijn. De tijdsbesteding zal in praktijk afhankelijk zijn van de mate van gebruik van (vertrouwelijke) gegevens in het team.

4.3 De CISO

De rol van Chief InformationSecurity Officer (CISO) werd al een aantal keren genoemd. Deze, voor HLTsamen nieuwe rol, is cruciaal in het gehele speelveld van de informatiebeveiliging. Om die reden wordt hier nader op ingegaan.

De CISO moet - op basis van de algemeen aanvaarde standaard: de BIG - zorgdragen voor een samenhangend pakket van maatregelen ter waarborging van de beschikbaarheid, integriteit en

vertrouwelijkheid van de informatie binnen de organisatie. Sleutelbegrippen daarbij zijn risicoanalyse, oog voor de bedrijfsvoering en in achtneming van de wettelijke voorschriften.

Deze meer beleidsmatig gerichte functie heeft als belangrijkste doel om binnen de gemeente voldoende organisatorische beveiligingsmaatregelen te initiëren en wel zodanig dat de technische beveiligingsmaatregelen ook daadwerkelijk effectief zijn. Met andere woorden, er dient zorg gedragen te worden voor samenhang tussen de technische en organisatorische maatregelen.

Het betreft een verbijzonderde functie, waarbij direct aan het College van B&W en de directie gerapporteerd kan worden. In de HLTsamen-organisatie is de functie gepositioneerd binnen het team Informatiebeleid en -beheer. Door de in het beleid opgenomen opdracht(en) wordt een zekere, voor de functie noodzakelijke, onafhankelijkheid ten opzichte van de 'gewone' lijnfuncties gegarandeerd.

De taken en verantwoordelijkheden van de CISO zijn als volgt samen te vatten:

- Verantwoordelijk voor het opstellen, bijstellen, vernieuwen en herzien van het informatiebeveiligingsbeleid en de daaruit voortvloeiende informatie(beveiligings)plannen.
- Optreden als adviseur informatiebeveiliging (voor het management) bij nieuwe ICT-voorzieningen en bij ingrijpende veranderingen in de ICT-infrastructuur.
- Adviseren van het (lijn)management bij de uitwerking van het informatiebeveiligingsbeleid in informatiebeveiligingsplannen voor hun verantwoordelijkheidsgebieden en bij de implementatie van deze plannen.
- Initiëren of laten uitvoeren van periodieke beveiligingsaudits, risico-, afhankelijkheids- en kwetsbaarheidsanalyses.
- Coördineren en adviseren bij beveiligingsincidenten en zo nodig optreden bij calamiteiten.
- Opzetten en initiëren van (periodieke) informatiebeveiligingsbewustzijnsprogramma's en adviseren over voorlichting en training van gebruikers in het correct omgaan met informatie(systemen).
- Projecten leiden die als doel hebben beveiligingsmaatregelen te implementeren of de kwaliteit van de beveiliging op langere termijn te handhaven en waar nodig te verbeteren.
- Controleren van de werking en naleving van het informatiebeveiligingsbeleid en daaruit voortvloeiende maatregelen.
- Periodiek rapporteren van beveiligingsincidenten en de afhandeling daarvan aan de portefeuillehouder.

4.4 Functioneel overleg

De CISO stelt een organisatie voor van beveiliging-gerelateerde functionarissen binnen HLTsamen, de beveiligingscommissie. Hij organiseert drie maal per jaar een (security)overleg met dit gremium en zit dit ook voor. De commissie heeft binnen HLTsamen een adviesfunctie richting MT, directie en bestuur en richt zich met name op beleid. Ook adviseert de commissie over tactisch/strategische kwesties binnen de informatiebeveiliging.
Het onderwerp Informatiebeveiliging dient verder een regelmatig terugkerend item te zijn op de agenda van het managementteam, zodat er sturing kan plaatsvinden op de uitgevoerde en uit te voeren activiteiten.

4.5 Externe partijen

- Informatiebeveiligingsbeleid, landelijke normen en wet- en regelgeving gelden ook voor de externe partijen (leveranciers, ketenpartners) waarmee we samenwerken en informatie uitwisselen.[5] Ook voor hen geldt hierbij het beginsel 'pas toe of leg uit'.
- Bij contractuele overeenkomsten gelden in beginsel altijd de Algemene Inkoop Voorwaarden voor leveringen en diensten Hillegom, Lisse en Teylingen (AIV), alsmede de Gemeentelijke Inkoopvoorwaarden bij IT (GIbIT), waarin onder meer geheimhouding en aansprakelijkheid is geregeld. Afwijkingen op de AIV en GIbIT dienen te worden getoetst aan het informatie-beveiligingsbeleid. 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.[6]
- Voor het tot stand brengen van datakoppelingen met externe partijen, geldt naast generiek informatiebeveiligingsbeleid een specifieke procedure, met als doel risicobeheersing.
- Voor externe hosting van data en/of services gelden naast generiek informatiebeveiligings-beleid de richtlijnen voor cloud-computing. De organisatie is gehouden aan:
  - regels omtrent grensoverschrijdend dataverkeer;
  - toezicht op naleving van regels door de externe partij(en);
  - hoogste beveiligingseisen voor bijzondere categorieën gegevens;[7]
  - melding bij de Autoriteit Persoonsgegevens (AP) bij doorgifte van persoonsgegevens naar derde landen (buiten de EU).

4.6 ICT crisisbeheersing en landelijke samenwerking

Voor interne crisisbeheersing dient een kernteam Informatiebeveiliging geïnstalleerd te zijn, bestaande uit:

- de CISO en de ISO,
- de functionaris gegevensbescherming (FG) van het team Juridische Zaken,
- de Security-Functionaris van het team Automatisering,
- relevante experts en
- een medewerker van het team Communicatie.

De werkwijze dient te zijn vastgelegd.

HLTsamen participeert in relevante landelijke platforms en onderhoudt contacten met andere sectoraal georganiseerde informatiebeveiligings-platforms.

4.7 PDCA

Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging.[8] Deze kwaliteitscyclus is hieronder beschreven.

- Plan: de cyclus start met informatiebeveiligingsbeleid, gebaseerd op wet- en regelgeving, landelijke normen zoals de BIG en best practices. Dit beleid wordt uitgewerkt in regels voor onder meer informatiegebruik, bedrijfscontinuïteit en naleving (informatiebeveiligingsplan).

[5] Beleidsregels voor externe partijen zijn beschreven in de Baseline Informatiebeveiliging Nederlandse Gemeenten.
[6] Hiervoor kan gebruik worden gemaakt van een 'third party mededeling' (TPM) of een ISAE 3402-verklaring.
[7] 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
[8] NEN/ISO 27001

Planning geschiedt op jaarlijkse basis en wordt indien nodig tussentijds bijgesteld. Domein- dan wel teamspecifieke activiteiten worden bij voorkeur opgenomen in domein- of teamspecifieke plannen.

- Do: het beleidskader is de basis voor risicomanagement, uitvoering van (technische) maatregelen en bevordering van 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 de controle (buiten het primaire proces) door een auditor.[9] Dit heeft het karakter van een steekproef. Jaarlijks worden meerdere van dergelijke onderzoeken uitgevoerd. Bevindingen worden opgenomen in de rapportage door de CISO.
- Act: De cyclus is rond met de uitvoering van verbeteracties o.b.v. check en (eventueel) externe controle. De cyclus is een continu proces, waarbij de bevindingen van controles input vormen voor de jaarplanning en beveiligingsplannen. De bevindingen worden in beginsel gerapporteerd aan de directie; voor ingrijpende verbeteracties wordt een verbetervoorstel gedaan.

[9] Van onder meer de accountant, rijksoverheid (voor bijv. basisregistraties) en gemeentelijke auditors (intern).

5 Onderwerpen van beveiliging

5.1 Verantwoordelijkheid voor bedrijfsmiddelen

Risico's

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

Doelstellingen

- 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.

5.2 Classificatie van informatie

Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen t.a.v. processen en informatiesystemen, worden beveiligingsclassificaties gebruikt. Classificatie maakt het vereiste beschermingsniveau zichtbaar en maakt direct duidelijk welke maatregelen nodig zijn. Er wordt geclassificeerd op drie betrouwbaarheidsaspecten van informatie: beschikbaarheid, integriteit (juistheid, volledigheid) en vertrouwelijkheid.

Risico's

- 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.
- Onjuiste classificatie kan leiden tot desinvestering (bij te hoge classificatie).

Doelstellingen

- Classificatie van informatie is ingericht, zodat de noodzaak van bescherming is aangegeven.
- Informatie krijgt hierdoor het juiste niveau van bescherming.
- De noodzaak voor aparte verwerkingsmaatregelen is gecommuniceerd.

5.3 Beveiliging van personeel

Risico

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.

Doelstellingen

- Werknemers, ingehuurd personeel en externe gebruikers begrijpen hun verantwoordelijkheden en zijn geschikt voor de rol die ze (gaan) innemen.
- De verantwoordelijkheden ten aanzien van beveiliging is vóór het dienstverband vastgelegd in passende functiebeschrijvingen en in de arbeidsvoorwaarden.
- Er is een procedure beschikbaar waarin beschreven wordt of en hoe kandidaten voor een aanstelling, ingehuurd personeel en externe gebruikers vooraf worden gecheckt.

5.4 Fysieke beveiliging en beveiliging van de omgeving

Risico's

- Onbevoegde toegang tot kritieke systemen of waardevolle informatie. Bij het ontbreken van registratie zijn incidenten bovendien niet herleidbaar tot individuen.
- Niet-medewerkers krijgen toegang tot de panden.
- Toegang tot informatie die vertrouwelijk of geheim is.
- Niet veilig verwijderen of hergebruiken van ICT-apparatuur.
- Verlies van, schade aan of diefstal van apparatuur.

Doelstellingen

- Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van de locaties en de informatie van de organisatie en bedrijfsmiddelen.
- Het voorkomen van onderbreking van de bedrijfsactiviteiten.
- Goed beschermde en beveiligde ICT-voorzieningen (met kritieke of gevoelige bedrijfsactiviteiten) 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.

5.5 Beveiliging van apparatuur en informatie

Risico's

- Het ontbreken van documentatie kan leiden tot fouten, niet-uniforme wijze van gegevensinvoer, of in geval de beheerder/bediener uitvalt, tot problemen rondom de continuïteit.
- Onjuiste autorisaties kunnen leiden tot foutieve handelingen, fraude en verduistering.
- Het niet uitvoeren en vastleggen van technische en functionele applicatietesten en/of de resultaten hiervan, kan in bepaalde omstandigheden (tijdsdruk, vakantieperiodes, etc.) leiden tot een verhoogd risico van uitval of gegevensverlies.
- Bij uitbesteding van beheer van systemen en gegevens aan een derde partij, kan ook informatie van HLTsamen op straat komen te liggen. De HLT-organisatie *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 antivirusbescherming bij medewerkers thuis leidt tot hogere beveiligingsrisico's.

Doelstellingen

- Waarborgen van een correcte en veilige bediening van ICT-voorzieningen.
- Vastgestelde verantwoordelijkheden en procedures voor beheer en bediening van alle ICT-voorzieningen. Dit betreft ook geschikte bedieningsinstructies.
- Systeem van functiescheiding toegepast (waar nodig), om het risico van nalatigheid of opzettelijk misbruik te verminderen.

5.6 Beheer van de dienstverlening door een derde partij

Risico

HLTsamen 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 organisatie op straat komen te liggen. HLTsamen heeft hierbij een regiefunctie en blijft verantwoordelijk voor de informatiebeveiliging van haar gegevens in dat deel van de keten, waarbij het beheer bij een andere partij ligt.

Doelstelling

- Een passend niveau van informatiebeveiliging implementeren en bijhouden en dit vastleggen in (bewerkers)overeenkomsten, contracten en/of convenanten.
- De HLT-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 voldoet aan alle eisen, die met de derde partij zijn overeengekomen.

5.7 Behandeling van media

Risico

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

Doelstellingen

- 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.

5.8 Uitwisseling van informatie

Risico

Bij verlies of diefstal van bijvoorbeeld laptops, USB-sticks, tablets of smartphones kan informatie in verkeerde handen komen.

Doelstelling

- Een formeel uitwisselingsbeleid m.b.t. de uitwisseling van informatie en programmatuur tussen de HLT-organisatie en externe partijen, dat in lijn is met de uitwisselings-overeenkomsten en relevante wetgeving.
- Vastgestelde procedures en normen ter bescherming van informatie en fysieke, te transporteren media (die informatie bevatten).

5.9 Logische toegangsbeveiliging

De identiteit van een gebruiker die toegang krijgt tot gemeentelijke informatie dient te worden vastgesteld.[10] Logische toegang is gebaseerd op de classificatie van de informatie.

Risico's:

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

Doelstelling

Beheersing van de toegang tot informatie, ICT-voorzieningen en bedrijfsprocessen op grond van bedrijfsbehoeften en beveiligingseisen.

5.10 Beveiligingsincidenten

Risico's

Als incidenten niet geregistreerd worden, is niet duidelijk waar en wanneer er zich incidenten voordoen of hebben voorgedaan. Op deze wijze kan er geen lering worden getrokken uit deze incidenten, zodat deze in de toekomst voorkomen kunnen worden.

Doelstelling

- Bewerkstelligen dat informatiebeveiligingsgebeurtenissen en -zwakheden, die verband houden
- met informatiesystemen zodanig kenbaar worden gemaakt dat 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 zwakheden die invloed kunnen hebben op de beveiliging van de bedrijfsmiddelen.
- Er is een meldingssystematiek in werking om alle informatiebeveiligingsgebeurtenissen en zwakke plekken zo snel mogelijk te rapporteren aan de aangewezen contactpersoon.

[10] Een gebruiker kan een medewerker, leverancier, burger, bedrijf, samenwerkingspartner of applicatie zijn.

5.11 Bedrijfscontinuïteit

Het is belangrijk dat de de continuïteit van de dienstverlening en de bedrijfsvoering van en door HLTsamen gewaarborgd wordt.

Risico's

- Als er weinig of geen invulling gegeven wordt aan continuïteitsplanning, is er in geval er zich een calamiteit voordoet, naast een vals gevoel van veiligheid ook grote kans op ad hoc maatregelen.
- Het uitvallen van medewerkers (ziekte, sterven, ontslag) kan een reële bedreiging zijn.

Doelstellingen

- Voorkomen van onderbreking van bedrijfsactiviteiten.
- Beschermen van kritische bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen.
- Bewerkstelligen van tijdig herstel als verstoringen optreden.

6 Naleving

De vastgestelde procedures, contracten en afspraken moeten worden nageleefd. Er moet aantoonbaar gewerkt worden binnen de vastgestelde kaders, plannen en de geldende wet- en regelgeving.

Risico's

- Het afgesproken kader wordt een papieren tijger.
- Afspraken en uitvoering komen niet met elkaar overeen, processen worden niet gevolgd.
- Niet naleven van wettelijke eisen, waardoor ook burgers, bedrijven en ketenpartners schade kunnen oplopen.

Doelstellingen

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

6.1 Organisatorische aspecten

Het verbeteren van de kwaliteit van informatieveiligheid is een continu proces en onderdeel van alle gemeentelijke processen waarin wordt gewerkt met gevoelige informatie. Informatieveiligheid is een kwaliteitskenmerk van het primaire proces, waarop het management van elk domein en team 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 bestuur en directie voor het toezicht op de uitvoering van het informatie-beveiligingsbeleid. De CISO legt een beveiligingsdocumentatiedossier aan en onderhoudt dit. Het bevat alle relevante verplichte en niet verplichte documenten, waaruit blijkt of kan worden aangetoond dat aan de specifieke beveiligingseisen is voldaan.

Periodiek wordt de kwaliteit van informatieveiligheid onderzocht, ook door onafhankelijke externen. De bevindingen worden gebruikt voor de verdere verbetering van de informatieveiligheid.

In de P&C-cyclus wordt gerapporteerd over informatieveiligheid aan de hand van het 'in control' statement.

6.2 (Wettelijke) kaders

Een overzicht van relevante wet- en regelgeving is te vinden bij KING. Zo is het gebruik van persoonsgegevens bijvoorbeeld geregeld in de Wet Bescherming Persoonsgegevens, maar zijn ook de (europese) Privacy verordening en de Wet meldplicht Datalekken van invloed.

7 Relevante documenten en bronnen

7.1 Intern

- Algemene Inkoopvoorwaarden voor leveringen en diensten Hillegom, Lisse en Teylingen (AIV)
- Gemeentelijke Inkoopvoorwaarden bij IT (GIbIT)

7.2 Extern

- NEN/ISO 27001 (2005) en 27002 (Code voor Informatiebeveiliging) (2007)
- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
- CBP richtsnoeren 'beveiliging van persoonsgegevens', 2013: http://www.cbpweb.nl/Pages/pb_20130219_richtsnoeren-beveiliging-persoonsgegevens.aspx
- GEMMA: https://www.kinggemeenten.nl/secties/gemma/gemma
- Voorbeeld Informatiebeveiligingsbeleid gemeenten, IBD, 2013.

8 Begrippen- en afkortingenoverzicht

AP (Autoriteit Persoonsgegevens) houdt toezicht op gebruik van persoonsgegevens door organisaties.

Archiefwet beschrijft hoe overheidsorganisaties moeten omgaan met de archieven die zij vormen.

BAG (Basisregistratie Adressen en Gebouwen) bevat gemeentelijke basisgegevens van alle adressen en gebouwen in een gemeente. Kopieën van al deze gegevens zijn verzameld in een Landelijke Voorziening (BAG LV). Het Kadaster beheert de BAG LV en stelt de gegevens beschikbaar aan organisaties met een publieke taak, instellingen, bedrijven en particulieren. De Minister van IenM is verantwoordelijk voor de BAG

BIG (Baseline Informatiebeveiliging Nederlandse Gemeenten) is het normenkader dat de beschikbaarheid, integriteit en vertrouwelijkheid van gemeentelijke informatie(systemen) bevordert. De BIG is een richtlijn die een totaalpakket aan informatiebeveiligingscontrols en -maatregelen omvat, die voor iedere gemeente noodzakelijk is om te implementeren.

BRP (Basisregistratie Personen) is dé basisregistratie voor persoonsgegevens binnen het stelsel van basisregistraties. De hele Nederlandse overheid gebruikt de gegevens die in de BRP worden geregistreerd.

CIO (Chief Information Officer) is de functionaris die verantwoordelijk is voor de informatievoorziening. ICT, de bedrijfstrategie, de organisatie zijn daarbij belangrijke aandachtsgebieden voor de CIO. De CIO heeft een steeds belangrijker rol binnen de organisatie bij het formuleren van strategische doelen.

CISO (Chief InformationSecurity Officer) heeft de touwtjes in handen als het gaat om *alle* aspecten van de informatiebeveiliging van de organisatie (coördinator/adviseur).

Classificeren is een passend beschermingsniveau bepalen, oftewel *die* maatregelen nemen die aansluiten bij de waarde van het te beschermen object.

Code voor Informatiebeveiliging beschrijft normen en maatregelen, die van belang zijn voor het realiseren van een afdoende niveau van informatiebeveiliging. De Code wordt uitgebracht door het Nederlands Normalisatie-instituut (NEN).

FG (Functionaris Gegevensbescherming) houdt binnen de organisatie toezicht op de toepassing en naleving van de Wet bescherming persoonsgegevens (Wbp).

Gap-analyse is een methode om een vergelijking te maken tussen een bestaande en een gewenste situatie.

IBD (Informatiebeveiligingsdienst) voor gemeenten is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING). De

IBD richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC).

Informatievoorziening is het geheel aan infrastructurele hulpmiddelen, applicaties, gegevensverzamelingen en organisatorische inrichtingen dat dient voor het aan gebruikers verstrekken van informatie.

ISO (InformationSecurity Officer) is de functionaris die binnen de informatiebeveiliging werkzaam is op het operationele niveau van de organisatie.

PUN (Paspoortuitvoeringsregeling) Regeling van de Minister voor Grote Steden- en Integratiebeleid van 7 september 2001, houdende regels in verband met de verstrekking van reisdocumenten door de burgemeesters.

SUWI (Structuur uitvoeringsorganisatie Werk en Inkomen) In de Wet SUWI is geregeld hoe de structuur met betrekking tot de uitvoering van taken inzake de arbeidsvoorziening en de sociale verzekeringswetten is vormgegeven. De wet bepaalt ook hoe de verschillende uitvoeringsorganen, het Uitvoeringsinstituut werknemersverzekeringen (UWV), de Sociale verzekeringsbank (SVB) en de Gemeenten samenwerken.