Informatiebeveiligingsbeleid Heemstede

Definitieve versie

April 2013

Verseonnummer 607112

Inhoudsopgave

Deel 1: Beleidskaders informatiebeveiliging

1. Inleiding

Als Gemeente Heemstede kunnen we niet om informatiebeveiliging heen. Informatiesystemen vormen immers het zenuwstelsel van onze organisatie en van de (keten)partners waarmee we zaken doen. Deze systemen kunnen alleen goed functioneren wanneer we de beveiliging ervan op orde hebben, dat wil zeggen: wanneer wij ervoor zorgen dat de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie gewaarborgd is en blijft.

2. Definities en belang van informatiebeveiliging

De kwaliteit van de informatievoorziening wordt voornamelijk gedefinieerd in termen van **beschikbaarheid, integriteit en vertrouwelijkheid**. Om de gegevens en informatiesystemen waarover we beschikken, op deze gebieden te kunnen beschermen is het noodzakelijk een informatiebeveiligingsbeleid te hebben.
We beschouwen informatiebeveiliging als het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie binnen de organisatie. Hierbij worden deze termen als volgt gedefinieerd:

- ***Beschikbaarheid*** betekent dat informatie(systemen) beschikbaar zijn op de juiste momenten. Hierdoor hebben burgers en bedrijven toegang tot onze website en toegang tot voor hen relevante informatie en hebben medewerkers toegang tot relevante informatie om hun werk en hun dienstverlening richting onze burgers en bedrijven ongestoord voort te zetten.
- ***Integriteit*** betekent het waarborgen van de correctheid en de volledigheid van de informatieverwerking. Voor een efficiënte en effectieve bedrijfsvoering is het voor de Gemeente Heemstede van belang dat de correcte informatie tijdig aanwezig is in de systemen. Maar ook dat zelfs na een bepaalde periode de correctheid en de volledigheid van informatie eenvoudig gecontroleerd kan worden (=controleerbaarheid).
- ***Vertrouwelijkheid*** betekent dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn. Voor de Gemeente Heemstede is het van belang dat vertrouwelijke informatie zoals de persoonsgegevens van burgers en gegevens van bedrijven niet toegankelijk is voor onbevoegden.

Dit informatiebeveiligingsbeleid richt zich niet alleen op de geautomatiseerde gegevensverwerking door middel van ICT-voorzieningen, maar uitdrukkelijk ook op de bescherming van niet geautomatiseerde gegevens (zoals fysieke documenten) en bedrijfseigendommen.

3. Doelstelling van informatiebeveiliging

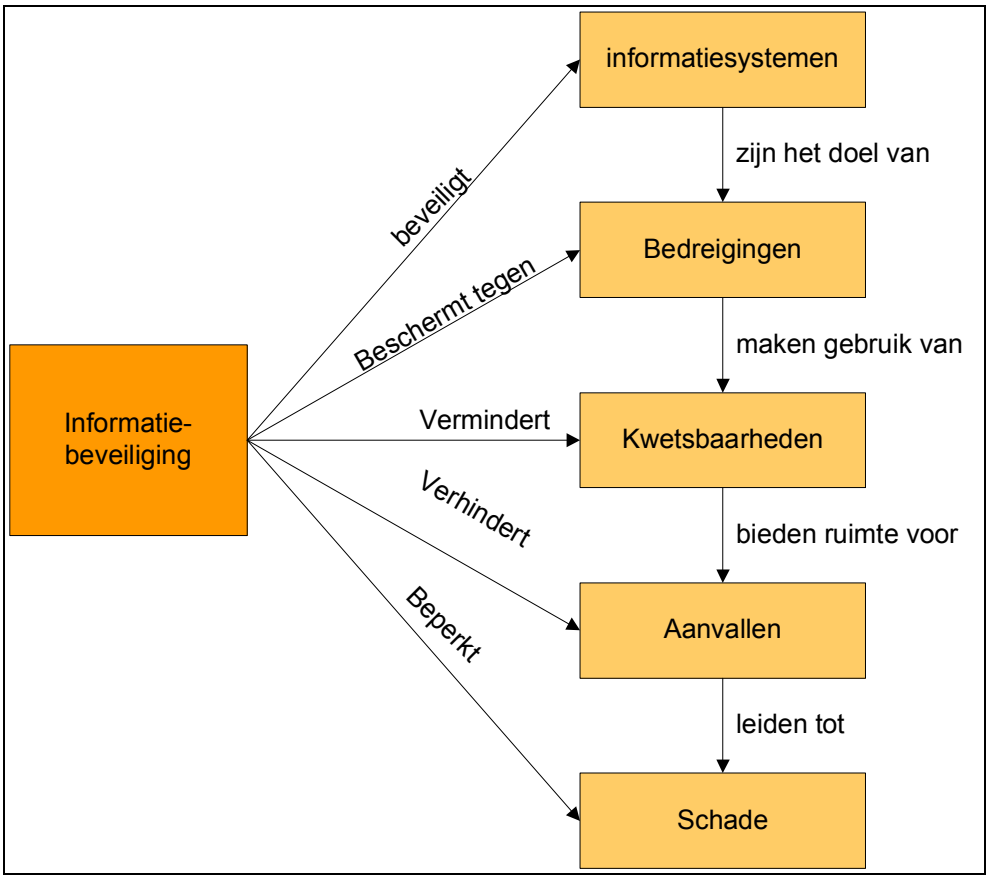
Dit document is de leidraad voor de aansturing en coördinatie van de verschillende beveiligingsprocessen binnen de Gemeente Heemstede. Het uiteindelijke doel is het inrichten van een set van beveiligingsmaatregelen, gericht op risicobeheersing. De risicobronnen waar de informatie en informatievoorziening van de Gemeente Heemstede aan zijn blootgesteld komen onder andere voort uit:

- de door de organisatie gewenste functionaliteit;
- de gebruikers van de informatiesystemen;
- de kwetsbaarheden van de ICT-infrastructuur;
- externe oorzaken (bijvoorbeeld inbraak, ongeoorloofd gebruik, vernieling)
- externe oorzaken (natuurgeweld, maar ook technische calamiteiten zoals brand en lekkage).

Het doel van informatiebeveiliging binnen de Gemeente Heemstede is om te allen tijde een adequate set van maatregelen te hebben getroffen om de risico's die de hiervoor genoemde risicobronnen met zich meebrengen te beperken c.q. de gevolgschade te beperken. Niet alleen het treffen van fysieke, procedurele, organisatorische en technische maatregelen is van belang, ook de controle op naleving is essentieel. Hierbij wordt rekening gehouden met het volwassenheidsniveau van de organisatie en de beschikbare middelen.

Zonder goede informatie kunnen we niet werken, want de primaire en ondersteunende processen van de Gemeente Heemstede zijn in hoge mate afhankelijk van een adequate informatievoorziening en betrouwbare informatiesystemen. Zonder beveiligde informatie kan de Gemeente Heemstede bloot staan aan imagoschade. Met andere woorden informatie is voor ons een belangrijk bedrijfsmiddel dat op gepaste wijze beschermd moet worden.

Dit informatiebeveiligingsbeleid is er op gericht de beschikbaarheid, de integriteit en de vertrouwelijkheid van de (geautomatiseerde) gegevensverwerking binnen de Gemeente Heemstede en de (geautomatiseerde) uitwisseling van gegevens tussen de Gemeente Heemstede en derden te waarborgen. Om die beheersbare en betrouwbare informatievoorziening te realiseren is het van belang een aantal gemeenschappelijke uitgangspunten te hanteren en deze uit te dragen.

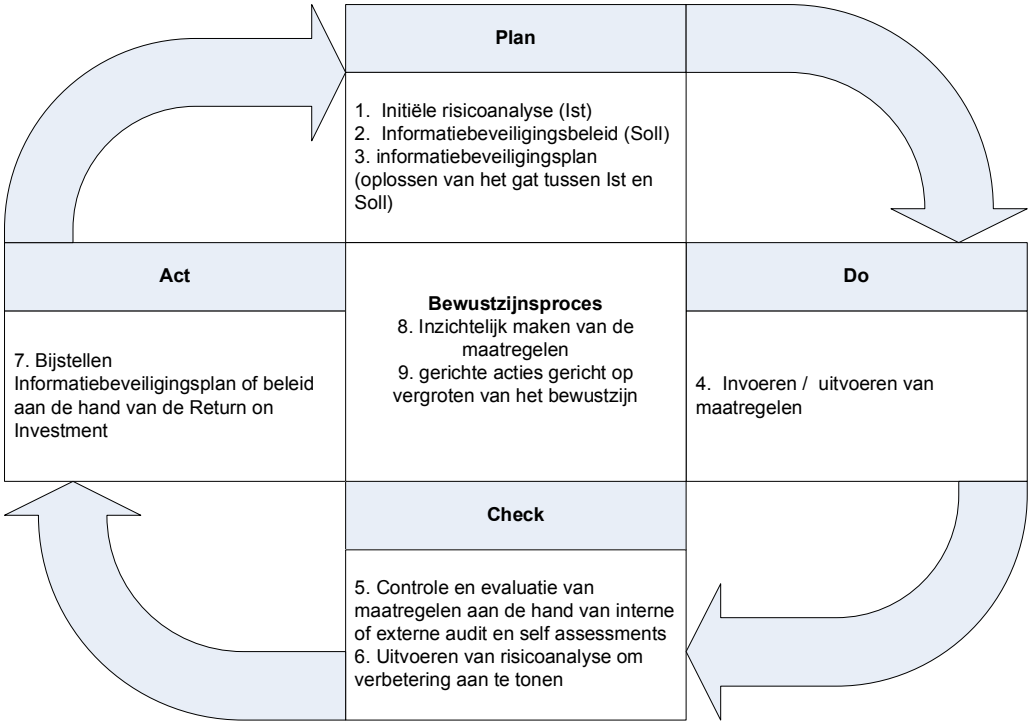


Het informatiebeveiligingsbeleid heeft als doel om de betrouwbare werking van de (geautomatiseerde) uitwisseling van informatie van de Gemeente Heemstede inzichtelijk te maken en daar waar nodig maatregelen aan te geven tegen een brede waaier van bedreigingen waaronder verstoringen en inbreuken en zo de continuïteit van de Gemeente Heemstede op dit gebied te verzekeren en maximaal bij te dragen tot goede resultaten. Informatieveiligheid wordt bereikt door de implementatie van een reeks beleidsmaatregelen of controles (hardware en software functies, processen, procedures, organisatie structuren). Deze moeten uitgewerkt worden om de veiligheidsdoelstellingen van de Gemeente Heemstede in te vullen.

Het informatiebeveiligingsbeleid moet steunen op een lagenmodel (zie volgend hoofdstuk) waar verschillende maatregelen complementair aan elkaar zijn. De veiligheid die bereikt kan worden met technische middelen is slechts één van de lagen. Deze middelen moeten aangevuld worden met een doeltreffend managementsysteem en met de noodzakelijk processen. Cruciaal voor een goede informatiebeveiliging is de deelname van alle medewerkers binnen de Gemeente Heemstede.

4. Organisatie van informatiebeveiliging

- Binnen de Gemeente Heemstede is een beheerkader vastgesteld om de implementatie van informatiebeveiliging in de organisatie te initiëren en te beheersen.
- Het informatiebeveiligingsbeleid is door het College van B&W vastgesteld en wordt door het Directie Team van de Gemeente Heemstede uitgevoerd, waarbij beveiligingsrollen zijn toegewezen en de implementatie van de beveiligingsmaatregelen binnen de Gemeente Heemstede door het Directie Team wordt gecoördineerd en beoordeeld.
- Omdat de IT-voorzieningen continu onderhevig zijn aan veranderingen, is Informatiebeveiliging binnen de Gemeente Heemstede een continu (verbeter)proces.
- Het informatiebeveiligingsproces doorloopt de zogenaamde Deming Cyclus die de fases Plan, Do, Check en Act bevat. De uit te voeren werkzaamheden zijn als volgt te plaatsen in de cyclus:



- Ten aanzien van risico's die voort komen uit de risicoanalyse heeft de Gemeente Heemstede per risico één van de volgende strategieën gekozen om deze te verkleinen:
  - Treat the risk (reduceren): verkleinen van het risico door middel van het nemen van informatiebeveiligingsmaatregelen.
  - Take the risk (accepteren): het risico is zo klein dat de gevolgen acceptabel zijn.
  - Terminate the risk (vermijden): wanneer er een groot risico bestaat voor een bedrijfsactiviteit die weinig tot geen toegevoegde waarde heeft dan wordt deze bedrijfsactiviteit indien mogelijk gestaakt.
  - Transfer the risk (delen/overdragen): overhevelen van het risico naar een derde partij door middel van uitbesteding of het afsluiten van verzekeringen.

- De correcte uitvoering van informatiebeveiliging wordt minimaal jaarlijks door een externe partij beoordeeld.

Het informatiebeveiligingsbeleid is onderdeel van het Informatiebeveiliging raamwerk van de Gemeente Heemstede. Dit raamwerk bestaat uit drie hiërarchische niveaus.

Op het hoogste niveau wordt het informatiebeveiligingsbeleid gedefinieerd. De uitgangspunten in dit beleid worden beïnvloed door algemeen geldende standaarden en normen alsmede de wettelijke bepalingen waaraan de Gemeente Heemstede onderhevig is. Daarnaast wordt het beleid ingevuld op basis van randvoorwaarden zoals het algemene bedrijfsbeleid en mogelijke geldende externe normen. Het gaat hier om algemeen geldende richtlijnen, niet om op specifieke informatiesystemen gerichte maatregelen.

Op het tweede niveau worden de beveiligingsmaatregelen beschreven als uitwerking van de doelstellingen in het informatiebeveiligingsbeleid Het gaat hierbij om zowel organisatorische als om technische beveiligingsmaatregelen. Deze kunnen gedefinieerd zijn voor de informatiebeveiliging in het algemeen of voor specifieke informatiesystemen.

Op het laagste niveau zijn de procedures en werkinstructies gedefinieerd die bestaan uit dagelijkse beheersactiviteiten met betrekking tot de informatiebeveiliging.

Het is van essentieel belang te realiseren dat het informatiebeveiligingsbeleid in algemene termen uitspraken doet over beveiligingsaspecten. Het geeft via richtlijnen dwingend richting aan de implementatie van een adequaat beveiligingsniveau voor alle (geautomatiseerde) informatie. Maatregelen op systeemniveau komen in het beleid niet aan de orde.

Subjecten van het informatiebeveiligingsbeleid

Alle personeelsleden in loondienst van de Gemeente Heemstede en alle externe krachten die tijdelijk of voor onbepaalde duur bij de Gemeente Heemstede tewerkgesteld zijn of voor de Gemeente Heemstede werkzaamheden verrichten (bijv. onderaannemers, consultants, leveranciers, …) dienen

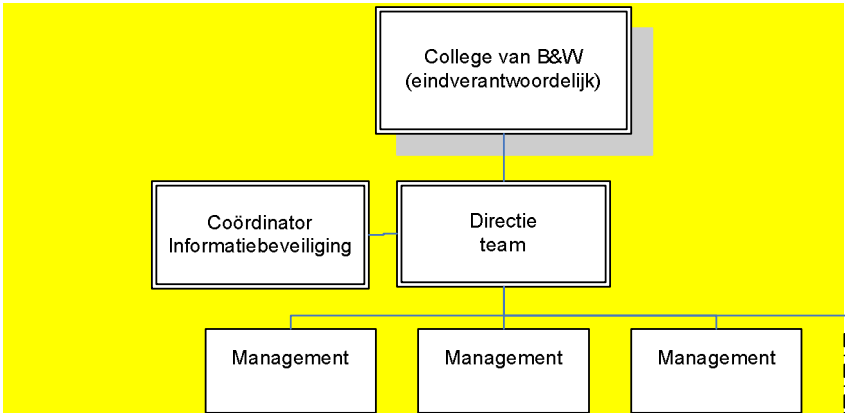
overeenkomstig het beveiligingsbeleid te handelen en zijn dus verantwoordelijk voor het toepassen van het beveiligingsbeleid binnen hun verantwoordelijkheidsgebied.

Objecten van het informatiebeveiligingsbeleid

Het beveiligingsbeleid geldt voor alle informatie, hetzij mondeling, hetzij geschreven, geprint of elektronisch opgeslagen, die eigendom is van, in bewaring is bij of gebruikt wordt door welk gedeelte van de Gemeente Heemstede dan ook. Het beveiligingsbeleid geldt ook voor alle (tijdelijke) dragers gebruikt in het creëren, verwerken, versturen sorteren, gebruiken of controleren van gegevens en informatie.

5. Taken, bevoegdheden en verantwoordelijkheden

Binnen de Gemeente Heemstede worden de volgende functies ten aanzien van informatiebeveiliging onderscheiden:



Het **College van B&W** van de Gemeente Heemstede is eindverantwoordelijk voor alle informatiebeveiligingsaangelegenheden. Het **Directieteam** ondersteunt informatiebeveiliging door duidelijk richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor informatiebeveiliging toe te kennen en te erkennen.

Het ***Management*** van elke afdeling van de Gemeente Heemstede is en blijft onverkort verantwoordelijk voor de beveiliging en voor de kwaliteit van de informatie en informatiesystemen voor eigen gebruik en de aan anderen geleverde informatie en informatiediensten. De uitvoering van sommige beveiligingsactiviteiten van een afdeling kan door het management zijn gedelegeerd aan de **Coördinator Informatiebeveiliging**.

Daarnaast hebben ***medewerkers***, oftewel gebruikers van informatie en informatiesystemen van de Gemeente Heemstede een eigen verantwoordelijkheid. Men is verplicht, zich te houden aan de verstrekte richtlijnen aangaande de omgang met informatie, informatieverwerking en desbetreffende bedrijfsmiddelen.

Functie	Strategisch (uitstippelen)	Tactisch (aansturing)	Operationeel (uitvoering)
Directieteam	- Goedkeuren en uitdragen informatiebeveiligingsbeleid en informatiebeveiligingsplan. - Beschikbaar stellen middelen voor implementatie van beveiligingsmaatregelen	- Aansturen coördinator informatiebeveiliging - initïeren interne- en externe audits. - Toezicht houden op informatiebeveiliging	- Naleven van informatiebeveiligingsmaatregelen
Coördinator informatiebeveiliging	- Opstellen informatiebeveiligingsbeleid - Opstellen informatiebeveiligingsplan	- uitvoeren van interne audits. - Ondersteunen bij en coördineren van externe audits - Coördineren bewustwordingsproces	- Rapporteren status informatiebeveiliging aan Directie - Naleven van beveiligingsmaatregelen.
Management	N.v.t.	- Implementeren specifieke informatiebeveiligingsmaatregelen voor de eigen afdeling. - Aansturing van medewerkers - Toezicht houden op naleving van informatiebeveiligingsmaatregelen door zijn/haar medewerkers.	- Uitvoeren van self assessments - Rapporteren status implementatie van maatregelen aan Coördinator - Naleven van beveiligingsmaatregelen.
Medewerkers	N.v.t.	N.v.t.	Naleven van beveiligingsmaatregelen.

6. Doelgroepen

Informatiebeveiliging en daarmee ook dit informatiebeveiligingsbeleid geldt voor alle medewerkers (ook uitzend- en inhuurkrachten) van de Gemeente Heemstede. Kortom allen die te maken hebben met het verwerken van informatie. Het informatiebeveiligingsbeleid heeft als functie richting te geven aan informatiebeveiliging. Daarom worden in dit beleid de grondhouding en de basisprincipes van de Gemeente Heemstede ten aanzien van informatiebeveiliging beschreven. Dit document is tevens gericht op alle overige belanghebbenden van de Gemeente Heemstede, zoals burgers, bedrijven en leveranciers van goederen en diensten om op die manier duidelijk te maken wat de basisprincipes en -eisen zijn ten aanzien van informatiebeveiliging. Indien bij samenwerking met derden sprake is van uitwisseling van informatie, waarvan de Gemeente Heemstede eigenaar of beheerder is, dient informatiebeveiliging een onderdeel te zijn de samenwerkingsovereenkomst en mag deze niet strijdig zijn met het informatiebeveiligingsbeleid van de Gemeente Heemstede.

Het informatiebeveiligingsbeleid is locatie onafhankelijk. Indien een medewerker, zakelijke relatie of leverancier of derde zich op een locatie bevindt buiten het Raadhuis van de Gemeente Heemstede, maar wel met informatie of informatievoorziening (denk aan onderhoud in het veld, thuiswerken en/of webmail) van de Gemeente Heemstede werkt, dient men dit beleid te respecteren.

7. Van toepassing zijnde Wet- en regelgeving

Behalve de interne eisen die de Gemeente Heemstede aan informatiebeveiliging stelt, zijn er wettelijke eisen gesteld aan de beveiliging van gegevens en informatiesystemen. Voorbeelden hiervan zijn te vinden in:

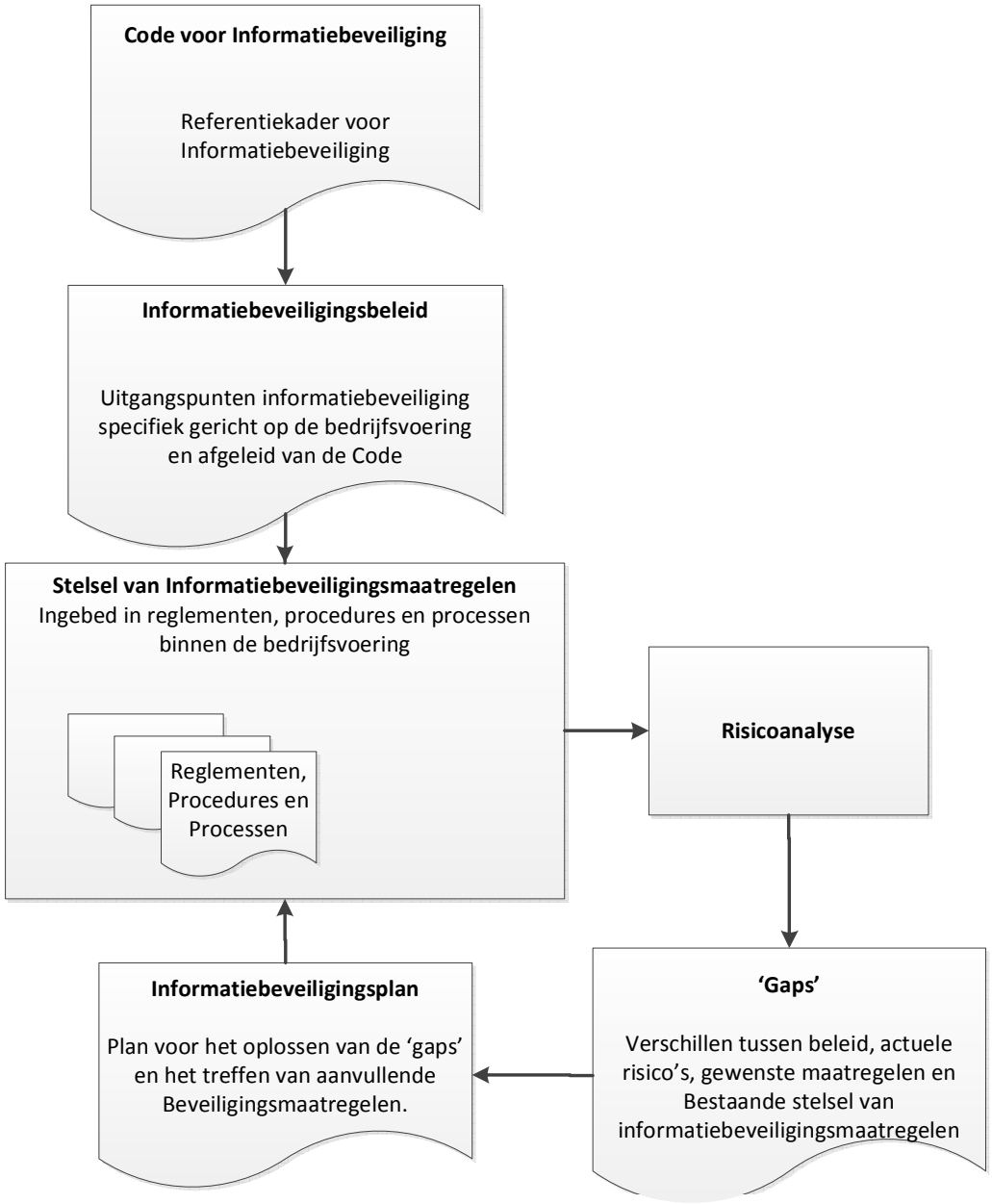
- de Wet Bescherming Persoonsgegevens (WBP) gaat in op de bescherming van persoonsgegevens in gestructureerde gegevensverwerkingen. De Gemeente Heemstede dient volgens deze wet ervoor zorg te dragen dat persoonsgegevens van burgers, bedrijven, medewerkers, leveranciers en overige belanghebbenden worden beschermd tegen onrechtmatige verwerking van of onbevoegde toegang tot deze gegevens.
- de Wet Computercriminaliteit II. Deze wet gaan in op computergerelateerde strafbare handelingen. De Gemeente Heemstede dient door middel van adequate informatiebeveiligingsmaatregelen ervoor te zorgen dat deze wet door medewerkers van de Gemeente Heemstede of door derden waarvoor de Gemeente Heemstede verantwoordelijk is niet wordt overtreden.
- Daarnaast zijn er gemeente specifieke vereisten van de Wet GBA, de wet BAG, de richtlijnen voor SUWInet.
- Maar ook het Burgerlijk Wetboek, de Telecommunicatiewet, de Auteurswet, de Wet op de Jaarrekening, de Archiefwet en het Wetboek van Strafvordering, etc…. bevatten in het algemeen een resultaatverplichting tot een passend niveau van informatiebeveiliging.

8. Gebruikte normen en standaarden

Binnen de Gemeente Heemstede wordt de Code voor Informatiebeveiliging (NEN-ISO/IEC 27002:2007) als norm gehanteerd voor het implementeren van informatiebeveiliging.

9. Relaties met overige documentatie

Het informatiebeveiligingsbeleid wordt door middel van een informatiebeveiligingsplan geoperationaliseerd. Dit betekent dat de concrete uitvoering van dit beleid door middel van het implementeren van informatiebeveiligingsmaatregelen is beschreven in het informatiebeveiligingsplan. In het informatiebeveiligingsplan wordt beschreven welke maatregelen ingevoerd moeten worden, op welke manier, door wie en binnen welk tijdsbestek. Indien van toepassing worden activiteiten uit het informatiebeveiligingsplan verder uitgewerkt in afzonderlijke projectplannen. In onderstaand figuur is de samenhang grafisch weergegeven.



10. Benodigde middelen

De Gemeente Heemstede stelt ieder jaar een begroting op, waarin de benodigde middelen voor informatiebeveiliging beschikbaar worden gesteld. Het budget wordt beschikbaar gesteld aan de hand van de in het informatiebeveiligingsplan gedefinieerde activiteiten.

Deel 2: Doelstellingen en beleidsuitgangspunten voor informatiebeveiliging

In dit hoofdstuk wordt per beveiligingscategorie uit de Code voor Informatiebeveiliging uiteengezet wat voor de Gemeente Heemstede de doelstelling en de uitgangspunten zijn voor de te treffen maatregelen.

1. Beveiligingsbeleid

1.1 Informatiebeveiligingsbeleid

Doelstelling:
Het Directie Team van de Gemeente Heemstede zal richting geven aan en ondersteuning bieden voor informatiebeveiliging in overeenstemming met de bedrijfsmatige eisen en relevante wetten en voorschriften.

Uitgangspunten:
- Door het uitbrengen van dit informatiebeveiligingsbeleid geeft het College uitdrukking aan het belang dat zij hecht aan informatiebeveiliging en demonstreert zij dat zij dit beleid van harte ondersteunt
- Dit informatiebeveiligingsbeleid zal het Directie Team handhaven en daarmee geeft het Directie Team tegelijkertijd een duidelijke beleidsrichting aan in overeenstemming met de bedrijfsdoelstellingen en demonstreert zij dat zij informatiebeveiliging ondersteunt.

2. Organisatie van informatiebeveiliging

2.1 Interne organisatie

Doelstelling:
Beheren van de informatiebeveiliging binnen de Gemeente Heemstede, waarbij de continuïteit van informatiebeveiliging wordt geborgd in de organisatie en in de processen.

Uitgangspunten:
- Het College van B&W van de Gemeente Heemstede heeft een beheerkader vastgesteld om de implementatie van informatiebeveiliging in de organisatie te initiëren en te beheersen.
- Het College van B&W van de Gemeente Heemstede heeft het informatiebeveiligingsbeleid goedgekeurd, en de uitvoering bij het Directie Team belegd.
- Het Directie Team heeft vervolgens beveiligingsrollen toegewezen, tevens coördineert en beoordeelt het Directie Team de implementatie van de beveiliging binnen de organisatie.

2.2 Externe partijen

Doelstelling:

Conformiteit van ons gemeentelijk IB beleid door externe partijen borgen middels leveranciersmanagement en de daarbij behorende contracten, SLA's en eventuele bewerkingsovereenkomsten.

Uitgangspunten:

- De beveiliging van de informatie en IT voorzieningen van de Gemeente Heemstede wordt zo minimaal mogelijk beïnvloed door het invoeren van nieuwe (of vernieuwde) producten of diensten van externe partijen.
- Elke toegang tot de IT-voorzieningen en het verwerken en communiceren van informatie door externe partijen wordt door de Gemeente Heemstede beheerst
- Met externe partijen waarmee wordt samengewerkt, zijn zo nodig overeenkomsten afgesloten waarin van toepassing zijnde beveiligingsrichtlijnen zijn opgenomen.

3. Beheer van bedrijfsmiddelen

3.1 Verantwoordelijkheid voor bedrijfsmiddelen

Doelstelling:

Bereiken en handhaven van een adequate bescherming van *)bedrijfsmiddelen van de Gemeente Heemstede.

Uitgangspunten:

- Alle bedrijfsmiddelen zijn verantwoord en aan een 'eigenaar' toegewezen.
- Voor alle bedrijfsmiddelen is vastgelegd wie verantwoordelijk is voor het handhaven van geschikte beheersmaatregelen. Deze verantwoordelijkheid kan zijn gedelegeerd, maar de eigenaar blijft verantwoordelijk voor een goede bescherming van de bedrijfsmiddelen.

*) onder bedrijfsmiddelen worden o.a. verstaan, apparatuur zoals: PC's, laptops, tablets, smartphones, en servers, maar ook applicaties zoals CIPERS, Verseon, Civision, WIZ, etc.

3.2 Classificatie van informatie

Doelstelling:

Zorgen dat informatie een passend niveau van bescherming krijgt.

Uitgangspunten:

- Informatie binnen de Gemeente Heemstede is geclassificeerd om bij het verwerken van deze informatie de noodzaak, prioriteiten en verwachte graad van beveiliging te kunnen aangeven.

- de Gemeente Heemstede beschikt over een informatie classificatieschema dat wordt gebruikt om adequate niveaus van bescherming te definiëren en de noodzaak voor aparte verwerkingsmaatregelen te communiceren.

4. Beveiliging van personeel

4.1 Voorafgaand aan het dienstverband

Doelstelling:

Zorgen dat werknemers, in te huren personeel en gebruikers van externe partijen hun verantwoordelijkheden begrijpen om daardoor het risico van diefstal, fraude of misbruik van faciliteiten te verminderen.

Uitgangspunten:

- De verantwoordelijkheid voor (informatie)beveiliging is voorafgaand aan het dienstverband vastgelegd in passende functiebeschrijvingen en opgenomen in de ambtenaren eed.
- Kandidaten, in te huren personeel en gebruikers van externe partijen worden op, door P&O bepaalde, passende wijze gescreend.
- Alle werknemers, in te huren personeel en gebruikers van externe partijen die IT-voorzieningen gebruiken worden geïnformeerd over het algemeen geldende beveiligingsbeleid en over hun beveiligingsrollen en – verantwoordelijkheden.

4.2 Tijdens het dienstverband

Doelstelling:

Zorgen dat alle werknemers, in te huren personeel en gebruikers van externe partijen zich bewust zijn van bedreigingen en gevaren voor informatiebeveiliging, van hun verantwoordelijkheid en dat ze zijn toegerust om het beveiligingsbeleid van de Gemeente Heemstede in hun dagelijkse werkzaamheden uit te voeren en het risico van een menselijke fout te verminderen.

Uitgangspunten:

- Alle werknemers, al het ingehuurde personeel en alle externe medewerkers beschikken over een passend niveau van bewustwording, opleiding en training in beveiligingsprocedures en het juiste gebruik van IT-voorzieningen om mogelijke beveiligingsrisico's te minimaliseren.
- de Gemeente Heemstede kent een gestructureerd proces voor het omgaan met beveiligingsinbreuken.

4.3 Beëindiging of wijziging van dienstverband

Doelstelling:

Zorgen dat werknemers, in te huren personeel en gebruikers van externe partijen de Gemeente Heemstede volgens de richtlijnen verlaten of hun dienstverband wijzigen.

Uitgangspunten:

- de Gemeente Heemstede kent een proces om te waarborgen dat alle apparatuur wordt teruggegeven en dat alle toegangsrechten worden ingetrokken wanneer een werknemer, ingehuurde medewerker of externe gebruiker de organisatie verlaat.
- Verandering van verantwoordelijkheden en dienstverband binnen de Gemeente Heemstede wordt behandeld als zijnde beëindiging gevolgd door een nieuw dienstverband.

5 Fysieke beveiliging en beveiliging van de omgeving

5.1 Beveiligde ruimten

Doelstelling:

Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van IT voorzieningen en de daarop opgeslagen informatie van de Gemeente Heemstede.

Uitgangspunten:

- IT voorzieningen die kritieke of gevoelige bedrijfsactiviteiten ondersteunen zijn fysiek ondergebracht in beveiligde ruimten.
- Alle IT voorzieningen van de Gemeente Heemstede zijn beschermd tegen toegang door onbevoegden.
- De geboden bescherming is in overeenstemming met de vastgestelde risico's.

5.2 Beveiliging van apparatuur

Doelstelling:

Het voorkomen van onderbrekingen van de bedrijfsactiviteiten en het voorkomen van schade aan, of verlies of diefstal van apparatuur.

Uitgangspunten:

- Alle apparatuur van de Gemeente Heemstede is beschermd tegen fysieke bedreigingen en gevaren van buitenaf, zodat het risico van toegang door onbevoegden tot informatie wordt verminderd en de apparatuur wordt beschermd tegen verlies of schade en de gevolgen van diefstal.

- Apparatuur die opslagmedia bevat, behoort te worden gecontroleerd om te zorgen dat alle gevoelige gegevens en in licentie gebruikte programmatuur zijn verwijderd of veilig zijn overschreven, voordat de apparatuur wordt verwijderd.

6. Beheer van communicatie- en bedieningsprocessen

6.1 Bedieningsprocedures en verantwoordelijkheden

Doelstelling:

Het waarborgen van een correcte en veilige bediening van IT-voorzieningen.

Uitgangspunten:

- de Gemeente Heemstede heeft verantwoordelijkheden en procedures vastgesteld voor beheer en bediening van alle IT-voorzieningen. Hieronder vallen ook bedieningsinstructies en handleidingen.
- Waar van toepassing wordt functiescheiding toegepast om het risico van nalatigheid of opzettelijk misbruik van informatiesystemen te verminderen.

6.2 Beheer van de dienstverlening door een derde partij

Doelstelling:

Het implementeren en bijhouden van een passend niveau van informatiebeveiliging bij dienstverlening door een derde partij.

Uitgangspunten:

- De Gemeente Heemstede controleert de implementatie van overeenkomsten met derden, bewaakt naleving van de overeenkomsten en beheert wijzigingen om te waarborgen dat de geleverde diensten aan alle eisen betreffende informatiebeveiliging voldoen die met de derde partij zijn overeengekomen.

6.3 Beheer van wijzigingen

Doelstelling:

Het risico van systeem verstoringen tot een minimum beperken.

Uitgangspunten:

- De Gemeente Heemstede treft bij wijzigingen de nodige voorbereidingen om voldoende menscapaciteit en beschikbaarheid van IT-middelen te waarborgen.

- De Gemeente Heemstede heeft de operationele eisen aan nieuwe systemen vastgesteld gedocumenteerd en getest voordat deze systemen worden geaccepteerd en in gebruik worden genomen.

6.4 Bescherming tegen virussen en kwaadaardige programmatuur

Doelstelling:
Beschermen van de integriteit van programmatuur en informatie.

Uitgangspunten:
- de Gemeente Heemstede heeft maatregelen getroffen voor de detectie en preventie en terminatie van de verspreiding van virussen en andere kwaadaardige programmatuur.

6.5 Back-up en recovery

Doelstelling:
Handhaven van de integriteit en beschikbaarheid van informatie en IT-voorzieningen

Uitgangspunten:
- de Gemeente Heemstede heeft routineprocedures vastgesteld voor het uitvoeren van de overeengekomen back-up en recovery strategie.

6.6 Beheer van netwerkbeveiliging

Doelstelling:
Zorgen voor de bescherming van informatie in netwerken en bescherming van de ondersteunende infrastructuur.

Uitgangspunten:
- de Gemeente Heemstede heeft maatregelen getroffen voor de beveiliging van het interne netwerk.

6.7 Behandeling van media

Doelstelling:
Voorkomen van onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van bedrijfsmiddelen en onderbreking van bedrijfsactiviteiten.

Uitgangspunten:

- de Gemeente Heemstede heeft passende maatregelen getroffen om documenten, opslagmedia (bijvoorbeeld schijven, tapes, USB-sticks), en systeemdocumentatie te beschermen tegen onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging.

6.8 Uitwisseling van informatie

Doelstelling:

Handhaven van beveiliging van informatie en programmatuur die wordt uitgewisseld met derden.

Uitgangspunten:

- Iedere uitwisseling van informatie en programmatuur wordt uitgevoerd in overeenstemming met relevante wetgeving.
- de Gemeente Heemstede heeft procedures vastgesteld ter bescherming van informatie en fysieke media die informatie bevatten die wordt getransporteerd.

6.9 Diensten voor online transacties

Doelstelling:

Zorgen voor de beveiliging van diensten voor *)online transacties en veilig gebruik ervan.

Uitgangspunten:

- de Gemeente Heemstede zorgt voor passende beveiligingsmaatregelen die gepaard gaan met diensten voor online transacties.
- de Gemeente Heemstede zorgt voor passende beveiligingsmaatregelen die betrekking hebben op de integriteit en beschikbaarheid van online transacties.

6.10 Controle

Doelstelling:

Ontdekken van onbevoegde informatieverwerkingsactiviteiten.

Uitgangspunten:

- de Gemeente Heemstede controleert haar systemen en registreert informatiebeveiligings-gebeurtenissen. Hiertoe wordt gebruik gemaakt van logbestanden en storingsregistraties.
- de Gemeente Heemstede voldoet aan alle relevante wettelijke eisen die van toepassing zijn op haar controle en registratie-activiteiten.

7. Toegangsbeveiliging

7.1 Beheer van toegangsrechten van gebruikers

Doelstelling:

Toegang voor bevoegde gebruikers beheersen en onbevoegde toegang tot informatiesystemen voorkomen.

Uitgangspunten:

- Toegang tot informatie, IT-voorzieningen en bedrijfsprocessen wordt bij de Gemeente Heemstede beheerst op grond van autorisatiematrices.
- de Gemeente Heemstede heeft procedures vastgesteld voor de beheersing van toewijzing van toegangsrechten tot informatiesystemen en –diensten
- de Gemeente Heemstede heeft speciale aandacht besteed aan het toewijzen van speciale toegangsrechten waarmee gebruikers de normale beveiliging van het systeem kunnen passeren.

7.2 Verantwoordelijkheden van gebruikers

Doelstelling:

Voorkomen van onbevoegde toegang door gebruikers en beschadiging of diefstal van informatie en IT-voorzieningen.

Uitgangspunten:

- de Gemeente Heemstede informeert haar medewerkers over hun verantwoordelijkheid voor toegangsbeveiliging, vooral met betrekking tot het gebruik van wachtwoorden.
- de Gemeente Heemstede kent een ‘clear-desk’ en ‘clear-screen’-beleid om het risico van ongeoorloofde toegang of schade aan papieren, media en IT-voorzieningen te verminderen.

7.3 Mobiele apparaten en telewerken

Doelstelling:

Het zorgen voor een passende mate van informatiebeveiliging bij het gebruik van mobiele apparaten en faciliteiten voor telewerken.

Uitgangspunten:

- De vereiste bescherming bij de Gemeente Heemstede is in overeenstemming met de risico’s die verbonden zijn aan deze manier van werken.

8. Inkoop, onderhoud en ontwikkeling van informatiesystemen

8.1 Beveiligingseisen aan informatiesystemen

Doelstelling:
Zorgen dat informatiebeveiliging integraal deel uitmaakt van nieuw te ontwikkelen informatiesystemen.

Uitgangspunten:
- de Gemeente Heemstede heeft maatregelen getroffen die waarborgen dat beveiligingseisen voorafgaand aan de ontwikkeling en/of implementatie van informatiesystemen worden vastgesteld en overeengekomen.
- Tijdens de specificatie van eisen voor een project worden de van toepassing zijnde beveiligingseisen overeengekomen en gedocumenteerd als onderdeel van de randvoorwaarden rondom het nieuwe informatiesysteem.

8.2 Correcte verwerking in programmatuur

Doelstelling:
Voorkomen van fouten, verlies, onbevoegde wijziging of misbruik van informatie in programmatuur.

Uitgangspunten:
- In programmatuur zijn geschikte beheermaatregelen ingebouwd, waaronder validatie van invoergegevens, interne verwerking en uitvoergegevens.
- Indien nodig zijn, bij systemen waarop gevoelige, waardevolle of kritische informatie wordt verwerkt, aanvullende beheersmaatregelen getroffen op basis van de beveiligingseisen en een risicobeoordeling.

8.3 Cryptografische beheersmaatregelen

Doelstelling:
Beschermen van de vertrouwelijkheid, authenticiteit en integriteit van informatie met behulp van cryptografische middelen.

Uitgangspunten:
- Wanneer de vertrouwelijkheid van de gegevens binnen een (te ontwikkelen) informatiesysteem dit vereist wordt er gebruik gemaakt van cryptografische toepassingen om de gegevens te beschermen tegen onbevoegde wijziging of inzage.

8.4 Beveiliging van systeembestanden

Doelstelling:

Zorgen voor de beveiliging van systeembestanden.

Uitgangspunten:

- De broncode en systeembestanden van de binnen de Gemeente Heemstede aanwezige applicaties zijn beschermd tegen inzage door onbevoegden, beschadiging en diefstal.

8.5 Beheer van technische kwetsbaarheden

Doelstelling:

Risico's verminderen als gevolg van benutting van gepubliceerde technische kwetsbaarheden.

Uitgangspunten:

- de Gemeente Heemstede heeft het beheer van technische kwetsbaarheden op een doeltreffende, systematische en herhaalbare wijze geïmplementeerd (software patchen).

8.6 Uitlekken van informatie

Doelstelling:

Er behoort te worden voorkomen dat zich gelegenheden voordoen om informatie te laten uitlekken.

Uitgangspunten:

- de Gemeente Heemstede probeert lekken van informatie te voorkomen door onbevoegde netwerktoegang te voorkomen,
- We combineren dat met beleid en procedures om het bewustzijn te stimuleren en tegelijkertijd misbruik van informatiediensten door personeel te ontmoedigen.

9. Beheersen van informatiebeveiligingsincidenten

9.1 Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken

Doelstelling:

Zorgen dat informatiebeveiligingsgebeurtenissen en zwakheden geregistreerd worden en dat tijdig corrigerende maatregelen worden getroffen.

Uitgangspunten:

- de Gemeente Heemstede heeft een procedure opgesteld voor rapportage van gebeurtenissen en escalatie.

- Alle medewerkers, in te huren personeel en gebruikers van externe partijen zijn van deze procedure op de hoogte en zijn zich bewust van hun verplichting alle beveiligingsgebeurtenissen en zwakke plekken zo snel mogelijk te rapporteren aan de aangewezen contactpersoon.

9.2 Beheer van informatiebeveiligingsincidenten en -verbeteringen

Doelstelling:

Zorgen dat een consistente en doeltreffende benadering wordt toegepast voor het beheer van informatiebeveiligingsincidenten.

Uitgangspunten:

- de Gemeente Heemstede heeft een procedure opgesteld voor het doeltreffend behandelen van informatiebeveiligingsgebeurtenissen en zwakke plekken, zodra ze zijn gerapporteerd.
- de Gemeente Heemstede heeft een proces van continue verbetering ingericht voor het reageren op, controleren, beoordelen en beheer van informatiebeveiligingsincidenten.

10. Continuïteitsbeheer

10.1 Informatiebeveiligingsaspecten van continuïteitsbeheer

Doelstelling:

Onderbrekingen van bedrijfsactiviteiten tegengaan en kritische bedrijfsprocessen beschermen tegen de gevolgen van calamiteiten[*)] en om voor tijdig herstel te zorgen.

*) onder calamiteit wordt verstaan een omvangrijke storing in informatiesystemen of rampen

Uitgangspunten:

- De definitie van een calamiteit is duidelijk binnen de gehele organisatie.
- Calamiteiten welke de gegevenswerking kunnen bedreigen zijn geïdentificeerd.
- De Gemeente Heemstede beschikt over een continuïteitsplan waarin is beschreven welke stappen genomen dienen te worden om de continuïteit van de gegevensverwerking te waarborgen in geval van een calamiteit.
- Het calamiteitenplan wordt periodiek getest.
- De meest bedrijfskritische informatiesystemen die de primaire bedrijfsprocessen ondersteunen kennen een uitwijkplan en zijn opgenomen in genoemd continuïteitsplan.
-

11. Naleving

11.1 Naleving van wettelijke voorschriften

Doelstelling:

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

Uitgangspunten:

- Alle van toepassing zijnde wettelijke, reglementaire en contractuele vereisten zijn expliciet gespecificeerd en gedocumenteerd voor relevante informatiesystemen.
- Indien nodig wint de Gemeente Heemstede advies in over specifieke juridische eisen bij de juridisch adviseurs van de organisatie of bij externe gekwalificeerde juristen.

11.2 Naleving van beveiligingsbeleid en –normen en technische naleving

Doelstelling:

Zorgen dat systemen voldoen aan het beveiligingsbeleid en de beveiligingsnormen van de organisatie.

Uitgangspunten:

- Informatiesystemen worden regelmatig beoordeeld op naleving van beveiligingsnormen en standaarden.
- Dergelijke beoordelingen worden uitgevoerd op basis van het beveiligingsbeleid
- Technische platforms en informatiesystemen worden beoordeeld op naleving van toepasselijke normen voor de implementatie van de beveiliging en gedocumenteerde beveiligingsmaatregelen.

11.3 Zorgvuldigheid bij audits van informatiesystemen

Doelstelling:

Zorgvuldigheid bewaken bij audits van informatiesystemen en minimaliseren van eventuele verstoringen als gevolg van audits.

Uitgangspunten:

- de Gemeente Heemstede heeft beheersmaatregelen getroffen om productiesystemen te beveiligen tijdens de uitvoering van audits.

11.4 Bescherming van (vertrouwelijke) bedrijfsinformatie en bedrijfsdocumenten

Doelstelling:

Belangrijke informatie en/of registraties behoren te worden beschermd tegen verlies, vernietiging, ontvreemding en vervalsing, overeenkomstig wettelijke en regelgevende eisen, contractuele verplichtingen, projectmatige en bedrijfsmatige eisen (lees: auditability).

Uitgangspunten:

De Gemeente Heemstede heeft een (privacy) beleid voor bescherming van vertrouwelijke gegevens ontwikkeld en ingevoerd. Dit beleid is gecommuniceerd naar alle personen die betrokken zijn bij het werken met vertrouwelijke gegevens.
Naleving van dit beleid en alle relevante wetgeving voor gegevensbescherming en regelgeving vereist een passende structuur voor beheer en beveiliging. Er is een functionaris aangewezen die belast is met de bescherming van gegevens. Deze functionaris biedt ondersteuning aan managers, gebruikers en dienstverlenende bedrijven met betrekking tot hun individuele verantwoordelijkheden en de specifieke procedures die behoren te worden gevolgd.
Het toewijzen van verantwoordelijkheid voor het verwerken van vertrouwelijke informatie en het waarborgen dat medewerkers zich bewust zijn van de uitgangpunten van bescherming van gegevens is uitgevoerd in overeenstemming met de relevante wet- en regelgeving. Er zijn passende technische en organisatorische maatregelen geïmplementeerd om dergelijke vertrouwelijke gegevens te beschermen (lees: bescherming van forensisch bewijs).

Deel 3: Stelsel van Informatiebeveiligingsmaatregelen

1 Inventarisatie maatregelen

In dit hoofdstuk wordt per beveiligingscategorie uit de Code voor Informatiebeveiliging uiteengezet welke maatregelen reeds van toepassing zijn voor de Gemeente Heemstede en welke aanvullende maatregelen de Gemeente Heemstede voornemens is in de planperiode alsnog te gaan treffen.

1.1 Maatregelen afgezet tegen de norm

Allereerst is per onderdeel van de Code voor Informatiebeveiliging gekeken wat het niveau van informatiebeveiliging bij de Gemeente Heemstede is. De score is gebaseerd op de implementatierichtlijnen zoals deze in de Code zijn beschreven. In bijgaande tabel is de score per onderdeel uitgesplitst.

De score voor de Gemeente Heemstede is als volgt:

Onderwerp	% score op gesloten vragen (ja)	
1. Beveiligingsbeleid	**10 %**	
2. Organisatie van de informatiebeveiliging	*55 %*	
3. Classificatie en beheer van bedrijfsmiddelen	**40 %**	
4. Beveiligingsaspecten t.a.v. personeel	**45%**	
5. Fysieke beveiliging	85 %	
6. Beheer van communicatie en bedieningsprocessen	*62 %*	
7. Toegangsbeveiliging	75 %	
8. Ontwikkeling en onderhoud van systemen	*66 %*	
9. Beheer van informatiebeveiligingsincidenten	**40 %**	
10. Continuïteitsmanagement	**10 %**	
11. Naleving	**40 %**	

De laagste percentages geven een indicatie van de hoogste **risico's**. Tot 50% = Rood, tot 75% = oranje; boven 75% groen. Met behulp van bovenstaande tabel is de prioritering bepaald van beleidsuitgangspunten met betrekking tot informatiebeveiliging.

1.2 Maatregelen prioritering

Nu alle relevante doelstellingen voor de Gemeente Heemstede zijn beschreven (in deel 2) kan de invoering ervan in een plan worden weergegeven. Doel is om voor 31 december 2015 voor alle doelstellingen maatregelen geïmplementeerd te hebben. Dit betekent dat er een planning voor 2013, 2014 en 2015 is opgesteld waarin eerst wordt gekeken naar welke maatregelen er al (gedeeltelijk) zijn of worden uitgevoerd. Deze worden benoemd. Daarna wordt er aan de hand van de in paragraaf 1.1 beschreven scoringstabel bepaald welke maatregelen voor welke doelstellingen er als eerste worden geïmplementeerd. Als een (set van) maatregel(en) gedeeltelijk is ingevoerd wordt naar de prioriteit gekeken van het volledig invoeren van de (set van) maatregel(en) en zo bepaald wanneer het wordt uitgevoerd.

Nummer	Omschrijving	Bestaat al /gedeeltelijk	2013	2014	2015
1	Beleid	Gedeeltelijk	1		
2	Organisatie	Gedeeltelijk		2	
3	Classificatie & beheer bedrijfsmiddelen	Gedeeltelijk	3		
4	Personele beveiliging	Gedeeltelijk		4	
5	Fysieke beveiliging	Bestaat al			5
6	Beheer & Communicatie	Gedeeltelijk		6	
7	Toegangsbeveiliging	Gedeeltelijk		7	
8	Ontwikkeling & Onderhoud	Gedeeltelijk			8
9	Incidenten beheer	Gedeeltelijk	9		
10	Continuïteitsmanagement	Afwezig	10		
11	Naleving	Gedeeltelijk	11		

1.3 Informatiebeveiligingsplan (periode 2013-2015)

De maatregelen die in 2013 worden uitgevoerd zijn hieronder in een planning weergegeven.

Augustus	September	Oktober	November	December
			1.1	
3.1	3.2			
		8		
			10	
				11

BIJLAGEN

Bijlage 1: Overzicht bestaande maatregelen en nog te treffen maatregelen

(per hoofdstuk volgens de Code voor Informatiebeveiliging)

Leeswijzer: in zwart reeds aanwezige maatregelen, in blauw verwijzing naar betreffende document, in rood nog te treffen maatregelen