Informatiebeveiligingsbeleid Gemeente Groningen

In opdracht van	Aaldert van Lingen (Directeur SSC-I&S)
Status	*Concept*
Versie	0.3
Redacteur	Bas Verheijen (CISO)
Datum	21-03-2019

Versiebeheer			
Versie	***Datum***	***Wijzigingen***	***Auteur***
0.1	05-10-2018	Initiële versie, ter afstemming met Informatiebeveiligingsteam en MT-I&S.	Bas Verheijen
0.2	23-10-2018	Distributie versie, inclusief bijdrage Informatiebeveiligingsteam en MT-I&S ter afstemming Bedrijfsvoeringsoverleg (BVO) / Informatiebeveiligingsraad.	Bas Verheijen
0.3	21-03-2019	Definitieve versie distributie, inclusief bijdrage Informatiebeveiligingsraad en GMT.	Bas Verheijen
~~1.0~~	XX-03-2019	Vaststelling college van Burgemeester & Wethouders.	Bas Verheijen

Goedkeuring				
Versie	***Datum***	***Naam***	***Functie***	***Status***
~~1.0~~	XX-04-2019	Aaldert van Lingen	Directeur SSC-I&S	~~Definitief~~

Distributielijst		
Versie	***Datum***	***Naam***
0.1	05-10-2018	Interne review: - Informatiebeveiligingsteam en MT-I&S.
0.2	23-10-2018	Verwerkte reacties Informatiebeveiligingsteam en MT-I&S. Interne review: - Bedrijfsvoeringsoverleg (BVO) / Informatiebeveiligingsraad. - Groninger Management Team (GMT)
0.3	21-03-2019	College van Burgemeester & Wethouders en gemeenteraad.
~~1.0~~	XX-04-2019	Gepubliceerd op intranet als definitieve versie.

Tekenparagraaf

Organisatie	**Naam**	**Handtekening**	**Datum**
Gemeente Groningen	College B&W		XX-03-2019

De definitieve versie van het informatiebeveiligingsbeleid is aldus formeel individueel vastgesteld door de eigenaar en de gebruikersorganisaties van de ICT-infrastructuur van de gemeente Groningen (rechtstreeks door het college van Burgemeesters en Wethouders van de gemeente Groningen en indirect via de SLA's door de directies van de gebruikersorganisaties). Het is de basis voor de toewijzing van de formele rollen en de implementatie van de informatiebeveiligingsmaatregelen ter beheersing van de informatiebeveiligingsrisico's binnen ICT-infrastructuur van en door de gemeente Groningen.
Hiermee zijn de voorgaande (deel)beleidstukken komen te vervallen.
Dit geldt voor de volgende strategische en tactische beleidstukken:

- *Informatiebeveiligingsbeleid – de kaders v20140601*
- *Informatiebeveiligingsbeleid – de maatregelen v20070306*
- Alle overige onderliggende uitwerkingen van processen, procedures, werkinstructies en dergelijke blijven gelden tot dat deze één voor één zijn geactualiseerd of vervangen conform de IBD-templates en geldende BIG-eisen.

Inhoudsopgave

Inhoudsopgave 4
1 Inleiding 7
1.1 Aanleiding 7
1.2 Doel van het beleid 8
1.3 Werkingssfeer 8
1.4 Doelgroep 10
1.5 Leeswijzer 11
1.6 Samenvatting 12
2 Informatiebeveiliging 13
2.1 Begrippenkader 13
2.2 Belang van informatieveiligheid 13
2.3 Reikwijdte 14
2.4 Visie 15
2.5 Kosten en opbrengsten 15
2.5.1 Kosten 15
2.5.2 Opbrengsten 16
3 Implementeren van informatiebeveiliging 16
3.1 Gelaagdheid 16
3.2 Volwassenheid – verbeterproces 17
3.3 Invoering maatregelen 17
3.4 Status maatregelen 18
4 Procesrisicoanalyse (BIA) 18
5 Informatiebeveiligingsbeleid 20
5.1 Informatiebeveiligingsbeleid 20
5.1.1 Uitgangspunten 20
6 Organisatie van informatiebeveiliging 21
6.1 Interne organisatie 21
6.1.1 Uitgangspunten 21
6.2 Externe partijen 23
6.2.1 Uitgangspunten 23
7 Beheer van bedrijfsmiddelen 23
7.1 Verantwoordelijkheid voor bedrijfsmiddelen 23
7.1.1 Uitgangspunten 23
7.2 Classificatie van informatie en bedrijfsmiddelen 23
7.2.1 Uitgangspunten 23
8 Personele beveiliging 24
8.1 Voorafgaand aan het dienstverband 24
8.1.1 Uitgangspunten 24
8.2 Tijdens het dienstverband 24
8.2.1 Uitgangspunten 24
8.3 Beëindiging of wijziging van het dienstverband 24
8.3.1 Uitgangspunten 25
9 Fysieke beveiliging en beveiliging van de omgeving 25
9.1 Beveiligde ruimten 25
9.1.1 Uitgangspunten 25
9.2 Beveiliging van apparatuur 25
9.2.1 Uitgangspunten 25
10 Beheer van communicatie- en bedieningsprocessen 26
10.1 Bedieningsprocedures en -verantwoordelijkheden 26
10.1.1 Uitgangspunten 26
10.2 Exploitatie door een derde partij 26
10.2.1 Uitgangspunten 26
10.3 Systeemplanning en -acceptatie 26
10.3.1 Uitgangspunten 26
10.4 Bescherming tegen virussen en 'mobile code' 27

10.4.1 Uitgangspunten....27
10.5 Back-up....27
10.5.1 Uitgangspunten....27
10.6 Beheer van netwerkbeveiliging....27
10.6.1 Uitgangspunten....27
10.7 Behandeling van media....27
10.7.1 Uitgangspunten....27
10.8 Uitwisseling van informatie....28
10.8.1 Uitgangspunten....28
10.9 Diensten voor elektronische bedrijfsvoering....28
10.9.1 Uitgangspunten....28
10.10 Controle....28
10.10.1 Uitgangspunten....28
11 Toegangsbeveiliging....29
11.1 Toegangsbeleid....29
11.1.1 Uitgangspunten....29
11.2 Beheer van toegangsrechten van gebruikers....29
11.2.1 Uitgangspunten....29
11.3 Verantwoordelijkheden van gebruikers....29
11.3.1 Uitgangspunten....29
11.4 Toegangsbeheersing voor netwerken....29
11.4.1 Uitgangspunten....30
11.5 Toegangsbeveiliging voor besturingssystemen....30
11.5.1 Uitgangspunten....30
11.6 Toegangsbeheersing voor toepassingen en informatie....30
11.6.1 Uitgangspunten....30
11.7 Draagbare computers en telewerken....31
11.7.1 Uitgangspunten....31
12 Verwerving, ontwikkeling en onderhoud van informatiesystemen....31
12.1 Beveiligingseisen voor informatiesystemen....31
12.1.1 Uitgangspunten....31
12.2 Correcte verwerking in toepassingen....31
12.2.1 Uitgangspunten....31
12.3 Cryptografische beheersmaatregelen....31
12.3.1 Uitgangspunten....32
12.4 Beveiliging van systeembestanden....32
12.4.1 Uitgangspunten....32
12.5 Beveiliging bij ontwikkelings- en ondersteuningsprocessen....32
12.5.1 Uitgangspunten....32
12.6 Beheer van technische kwetsbaarheden....32
12.6.1 Uitgangspunten....32
13 Beheer van informatiebeveiligingsincidenten....33
13.1 Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken....33
13.1.1 Uitgangspunten....33
13.2 Beheer van informatiebeveiligingsincidenten en verbeteringen....33
13.2.1 Uitgangspunten....33
14 Bedrijfscontinuïteitsbeheer....33
14.1 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer....33
14.1.1 Uitgangspunten....33
15 Naleving....34
15.1 Naleving van wettelijke voorschriften....34
15.1.1 Uitgangspunten....34
15.2 Naleving van beveiligingsbeleid en -normen en technische naleving....34
15.2.1 Uitgangspunten....34
15.3 Overwegingen bij audits van informatiesystemen....34
15.3.1 Uitgangspunten....34
Bijlage 1: Overzicht van gemeente Groningen met verbonden organisaties....35

Bijlage 2: Bronnen 35
Bijlage 3: Detailuitwerking voor het informatiebeveiligingsplan 35
B3.1 Interne organisatie 35
B3.1.1 Uitgangspunten 35
B3.1.2 Verantwoordelijkheden 36
B3.2 Externe partijen 40
B3.2.1 Uitgangspunten 40

1 Inleiding

1.1 Aanleiding

De gemeente Groningen[1] is een informatie-intensieve organisatie. De randvoorwaarde voor succesvolle dienstverlening is een betrouwbare en veilige informatievoorziening. De medewerkers, van deze verschillende afdelingen en van de verbonden organisaties die gebruikmaken van deze dienstverlening, moeten beschikken over betrouwbare informatie om de klanten optimaal te kunnen helpen en adviseren. Daarnaast dient de privacy van burgers en bedrijven aantoonbaar te zijn gewaarborgd, zodat zij erop kunnen vertrouwen dat hun gegevens in goede handen zijn binnen de gemeente.

Door de steeds verdergaande samenwerking en professionalisering van de gemeente Groningen nemen de digitalisering van de interne en externe informatievoorziening en de digitale dienstverlening[2, 3] verder toe. Daarvoor worden informatiesystemen intern en extern met (een toenemend aantal) ketenpartners gekoppeld. Door deze koppelingen ontstaat een steeds complexere infrastructuur van informatiesystemen die de basis vormt voor de totale informatievoorziening. Daarmee is de gemeente Groningen afhankelijker geworden van de goede en veilige werking van deze informatievoorziening. Hoe waardevoller de informatie is, hoe belangrijker het is dat de juiste maatregelen getroffen worden om de operationele risico's [4]te beheersen.

Veel informatiesystemen zijn echter niet primair ontworpen met het oog op de veiligheid van informatie. Daarnaast is het veiligheidsniveau dat met alleen fysieke en technische middelen kan worden bereikt beperkt. Het dient daarom te worden ondersteund met passende beheerprocessen en procedures. De menselijke factor (het menselijk gedrag) vormt daarbij een belangrijke en doorslaggevende rol in het daadwerkelijk realiseren van de veiligheid van informatie in de praktijk.

De gemeente Groningen heeft zich op 29 november 2013, in de Buitengewone Algemene Ledenvergadering, gecommitteerd aan de VNG-resolutie: *Informatieveiligheid, randvoorwaarde voor professionele gemeente*.

Als eerste actie is opgenomen om een informatiebeveiligingsbeleid vast te stellen aan de hand van de *Baseline Informatiebeveiliging Nederlandse Gemeenten* (BIG[5]). In het eerder vastgestelde informatiebeveiligingsbeleid (het beleid uit 2007 dat deels is geactualiseerd in 2014) zijn de belangrijke uitgangspunten grotendeels al opgenomen.

[1] Gemeente Groningen zoals gedefinieerd in bijlage 1.
[2] Mede door de invoering van het Stelsel van Basisregistraties (Digitale Overheid).
[3] Met de 3 decentralisaties van zorgtaken naar de gemeenten is de norm NEN 7510 (eveneens gebaseerd op de marktstandaard de Code voor Informatiebeveiliging, maar dan speciaal opgesteld voor zorg-gerelateerde organisaties) ook relevant geworden.
[4] Bedreigingen zoals benoemd in de BIG (paragraaf 1.6).
[5] BIG zal worden opgevolgd door de Baseline Informatiebeveiliging Overheid (BIO) waarschijnlijk vanaf 1 januari 2020. De maatregelen daarin wijken echter beperkt af ten opzicht van de huidige BIG.

1.2 Doel van het beleid

Dit beleid legt de basis voor één gemeenschappelijke taal binnen gemeente Groningen voor alle risico's en maatregelen op het gebied van informatiebeveiliging. De intentie is niet dat alle medewerkers exact weten wat er in het informatiebeveiligingsbeleid staat. Maar iedereen moet weten dat het beleid er is, wat de belangrijkste uitgangspunten zijn en in staat zijn het beleid vanuit zijn of haar functie te gebruiken.

Het beleid vormt tevens dé basis voor het richten, inrichten en verrichten van informatiebeveiliging binnen gemeente Groningen. Daarvoor zijn *alle* algemene uitgangspunten uit de BIG overgenomen. Deze uitgangspunten hebben een sterk normerend karakter en geven richting aan de keuzes voor de maatregelen die in de BIG staan. Deze maatregelen vormen tevens de basis voor het informatiebeveiligingsplan en voor de procesrisicoanalyses (Business Impact Analyses) waarmee de gemeente Groningen invulling geeft aan de uitgangspunten in dit informatiebeveiligingsbeleid.

Dit beleid is het kader voor passende technische en organisatorische maatregelen (processen) om interne informatie te beschermen en te waarborgen, opdat de gehele gemeente Groningen voldoet aan relevante wet- en regelgeving[6].
Het vormt de paraplu die alle individuele (bestaande en nog te nemen) maatregelen tot één samenhangend geheel smeedt, zodat daarmee één gemeenschappelijk fundament wordt gevormd voor de gemeente Groningen.

1.3 Werkingssfeer

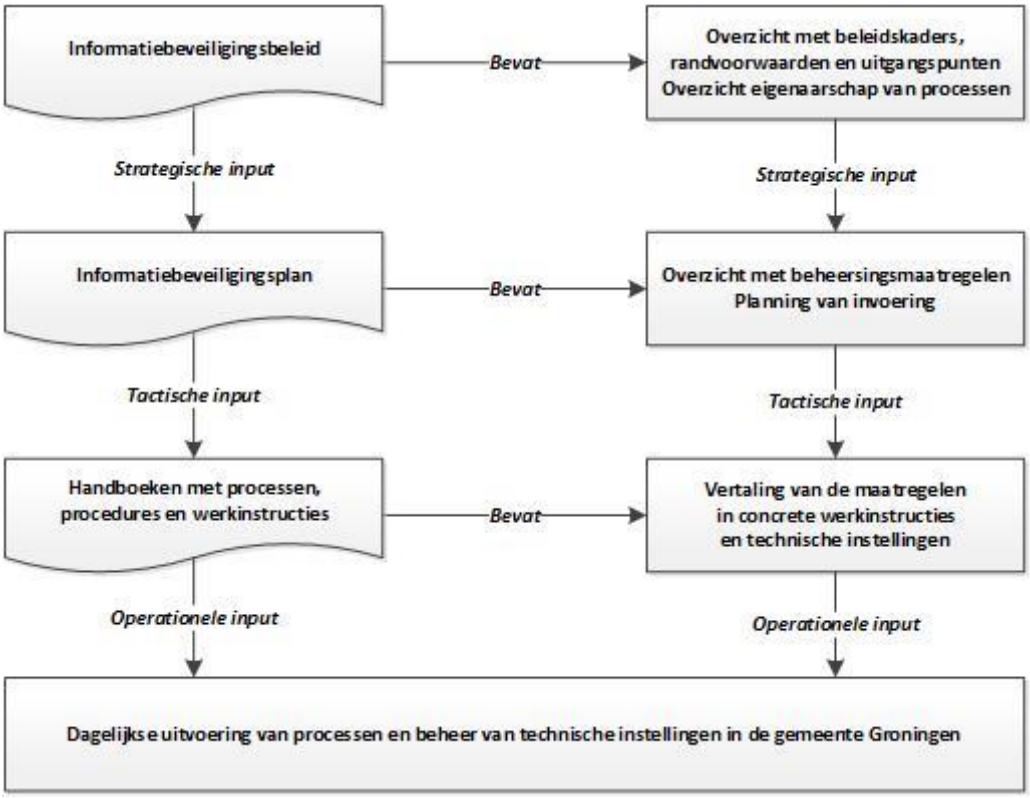
Het informatiebeveiligingsbeleid bevat de formele uitgangspunten en verwijzing naar de relevante gebieden waarop maatregelen getroffen dienen te worden om informatiebeveiligingsrisico's te kunnen mitigeren (verkleinen) en de maatregelen goed te kunnen invoeren en borgen binnen gemeente Groningen. Het beleid is van toepassing op *alle* informatie, informatieverwerkingsprocessen en systemen (hardware en software, zowel binnen de ICT-infrastructuur als daarbuiten) die wordt gebruikt door alle interne en externe medewerkers[7] van de gemeente Groningen. Daarmee vallen zowel de primaire operationele dienstverlenings-/ productieprocessen, als alle processen voor bestuurlijke en technische ondersteuning binnen de gemeente Groningen binnen het bereik van dit beleid.

Zie bijlage 1 voor de gedetailleerde lijst met alle organisaties (de gemeente Groningen, de verbonden Gemeenschappelijke Regelingen en overige gebruikersorganisaties van de ICT-infrastructuur) die zich dienen te conformeren aan het beleid. Er wordt namelijk gebruik gemaakt van informatie van de gemeente Groningen en (voor een deel van de processen) van de ICT-infrastructuur[8]. In het vervolg van dit document worden de verschillende organisaties die gebruik maken van de ICT-infrastructuur niet meer apart benoemd, maar worden deze aangeduid als *verbonden organisaties* van de gemeente Groningen of kortweg als *gemeente Groningen*. Het betreft immers een beleid dat geldt voor alle verbonden organisaties. Met gemeente Groningen wordt hier uitdrukkelijk niet alleen de organisatie gemeente Groningen bedoeld.

Het doel van dit beleid is het beheersen van risico's rond de ontwikkeling, het beheer en het gebruik van de ICT-infrastructuur, de informatiesystemen en ICT-bedrijfsmiddelen, de informatie-uitwisseling, de informatie zelf, en de gebruikers van die informatie. In het

[6] Het aantal wetten en regels over dit onderwerp is dusdanig gefragmenteerd en omvangrijk (meer dan honderd) dat er voor gekozen is, in dit beleid geen (uitputtend) overzicht met wettelijke eisen op te nemen.
[7] In dit verband is een *medewerker* iemand die werkzaam is bij of werkzaamheden verricht voor / in opdracht van de gemeente Groningen (of een verbonden organisatie) en daarbij gebruik maakt van informatie uit de informatievoorziening van de gemeente Groningen.
[8] De ICT-infrastructuur is als aangrijpingspunt genomen voor de bepaling van de reikwijdte wegens de onderlinge technische *ketenafhankelijkheid* voor informatiebeveiliging. Het beleid is uiteraard breder dan de ICT-infrastructuur van de gemeente Groningen en geldt voor alle informatie binnen de verbonden organisaties (zie bijlage 1), dus ook voor de informatie die buiten de ICT-infrastructuur wordt opgeslagen.

informatiebeveiligingsplan worden de beleidsuitgangspunten nader uitgewerkt. Op basis van de procesrisicoanalyses wordt gekozen welke concrete organisatorische en technische maatregelen noodzakelijk zijn om de informatiebeveiligingsdoelstellingen uit dit beleid te bereiken. Deze vertaling is weergegeven in onderstaande figuur 1.



Figuur 1 – Vertaling beleidsuitgangspunten naar concrete werkinstructies en instellingen

1.4 Doelgroep

Dit beleid is bedoeld voor *alle* interne en externe medewerkers binnen de gemeente Groningen. Het is vooral gericht op diegenen die betrokken zijn bij de ontwikkeling, uitvoering, sturing en naleving van het informatiebeveiligingsbeleid. De bestuurders en het management spelen een belangrijke rol bij de besluitvorming over dit onderwerp en de sturing ervan binnen de planning- & controlcyclus. Zie onderstaande tabel voor een korte toelichting van de verantwoordelijkheid per doelgroep en de hoofdstukken die relevant zijn voor de doelgroep.

Doelgroep	**Verantwoordelijkheid voor**	**Relevante hoofdstukken**
Gemeenteraad	Toezichthouden	Alle
College van B&W	Integraal bestuurlijk verantwoordelijk (kaderstelling)	Alle
Directies	Ambtelijke sturing op beleid	Alle
Lijnmanagement	Vertaling van beleid naar sturing op uitvoering van en controle op naleving informatiebeveiliging	6, 8, 10, 12, 13 en 14
Medewerkers	Implementatie, uitvoering, naleving van beleid en onderliggende procedures (sturing eigen gedrag)	7, 10, 11 en 12
Auditors (intern/extern)	Periodieke[9] onafhankelijke toetsing naleving	Alle
Beleidmakers	Opstellen beleid en toetsing procedures en uitvoering aan het informatiebeveiligingsbeleid	4, 5, 6, 10 en 12
Beveiligings-functionarissen	Dagelijkse coördinatie op uitvoering en naleving van informatiebeveiligingsbeleid	Alle
Eigenaren (proces, applicatie/systeem, informatie)	Classificatie van processen, applicaties/systemen en informatie	7, 10, 11 en 12
Communicatie	Vrijgave van (publieke) informatie	Alle
Facilitaire zaken	Fysieke beveiliging en toegang	9
ICT-beheer en -ontwikkeling (SSC)	Technische beveiliging	6, 7, 9, 10, 11, 12 en 13
Inkoop & contractbeheer	Inkoopvoorwaarden, toetsing in contractbeheer	6.2, 8, 10.2, 12.1, 13 en 15
Juridische zaken	Interpretatie wet- en regelgeving, onder andere verantwoordelijkheidsvraagstukken omtrent privacy, meldplicht datalekken (AVG)	8, 10, 13 en 15
Personeelszaken	Arbeidsvoorwaarden, procedures voor instroom, doorstroom en uitstroom van medewerkers	8
Financiële zaken	Begroting en verantwoording integriteit van financiële informatie	11, 12 en 13
Leveranciers en ketenpartners	Gemeente Groningen ondersteunen om compliant te worden en te blijven aan de BIG	Alle

[9] In dit verband moeten in elk geval de verplichte verantwoordingen worden genoemd: de ENSIA-audits, inclusief de zelfevaluaties over de basisregistraties BAG, BGT, BRP, BRO en PUN, de DigiD-beveiligingsassessments, de Suwinet-audits en de IT-audits in het kader van de jaarrekeningcontrole door de accountant.

1.5 Leeswijzer

Het beleid is zodanig opgezet dat het een naslagwerk vormt voor alle bestuurders en medewerkers die in het kader van hun reguliere werkzaamheden, in een project of ad hoc moeten weten aan welke kwaliteitsaspecten ten aanzien van informatieveilig werken aandacht moet worden besteed.

De hoofdstukken 1 tot en met 4 geven de inleiding, de context en primaire uitgangspunten van het onderwerp weer. Vervolgens geven de inhoudelijke hoofdstukken 5 tot en met 15 een nadere duiding per relevant onderdeel van informatiebeveiliging. Dit is in lijn met de structuur en de processen van de BIG. Hiermee wordt de vindbaarheid van normen en de mogelijkheid tot benchmarking vergroot. Tevens kan daardoor op een gestructureerde wijze onderdeel voor onderdeel invulling worden gegeven aan het onderwerp.

In de tabel in paragraaf 1.4 is per doelgroep aangegeven welke hoofdstukken vanwege de rol/functie het meest relevant zijn.

Voor de leesbaarheid van het beleid is ervoor gekozen om alle begrippen in de tekst zelf (en niet apart in een bijlage) te verklaren en de afkortingen alleen bij het eerste gebruik voluit te schrijven.

1.6 Samenvatting

Gemeente Groningen is, evenals iedere verbonden organisatie, zelf bestuurlijk (wettelijk) eindverantwoordelijk voor informatiebeveiliging binnen haar eigen organisatie. Dit informatiebeveiligingsbeleid is de basis voor de werkprocessen om de beveiliging van alle informatie binnen de gemeente Groningen (en de keten) als één geheel te kunnen waarborgen. Het is van toepassing op alle interne en externe medewerkers binnen de gemeente Groningen en is in lijn met de relevante Nederlandse en Europese wet- en regelgeving.

Het basisuitgangspunt is dat *minimaal* door de gemeente Groningen wordt voldaan aan het gemeentelijke normenkader: de *Baseline Informatiebeveiliging Nederlandse Gemeenten* (BIG), waarbij het 'pas toe of leg expliciet uit'-principe altijd geldt indien daaraan (nog) niet wordt of kan worden voldaan.

Het informatiebeveiligingsbeleid geeft alle uitgangspunten weer voor de organisatorische en technische maatregelen in het informatiebeveiligingsplan. Alle bestaande en nieuwe processen, procedures, medewerkers en technische instellingen moeten (gaan) voldoen aan dit beleid. Tevens geeft het beleid weer op welke wijze zal worden toegezien op de naleving van het beleid binnen de gemeente Groningen.

De belangrijkste uitgangspunten van het beleid zijn:

1. Het **informatiebeveiligings*beleid*** vormt samen met het **informatiebeveiligings*plan*** één van de fundamenten onder een betrouwbare informatievoorziening. Hierin wordt de betrouwbaarheid van de informatievoorziening én de gemeente Groningen breed benaderd. Zij worden periodiek (het beleid minimaal eens per drie jaar) bijgesteld op basis van de nieuwe interne en externe ontwikkelingen, de incidentenregistraties en de (bestaande) procesrisicoanalyses.
2. Het **bestuurlijk niveau** is **eindverantwoordelijk** voor informatiebeveiliging en draagt deze verantwoordelijkheid en het beleid actief uit.
3. Alle **taken, bevoegdheden en verantwoordelijkheden** voor de bescherming van informatie en voor het uitvoeren van beveiligingsprocedures zijn binnen iedere organisatie **expliciet vastgelegd**.
4. Door een **gemeente Groningen brede planning, coördinatie én periodieke controle** op informatiebeveiliging wordt de kwaliteit van de informatievoorziening verankerd binnen de gemeente Groningen.
5. Informatie en informatiesystemen zijn van kritiek en vitaal belang voor de gemeente Groningen en zijn **geclassificeerd** om maatregelen gericht in te kunnen zetten.
6. Informatiebeveiliging is een **continu verbeterproces**, dat is ingericht conform het 'Plan, do, check en act'-principe.
7. Informatiebeveiliging is **integraal** opgenomen in de reguliere **planning- & controlcyclus**[10] (als **informatiebeveiligingsmanagementsysteem**) van heel de gemeente Groningen en vormt een integraal aspect van gegevensmanagement in de gemeente Groningen.
8. De **informatiebeveiligingsfunctionaris**, de Chief Information Security Officer (CISO) ondersteunt vanuit zijn **onafhankelijke positie** de informatiebeveiligingsfunctionarissen binnen de gemeente Groningen en binnen de verbonden organisaties. Zij bewaken en verhogen de betrouwbaarheid van de eigen informatievoorziening. De CISO coördineert de initiatieven binnen de gemeente Groningen en rapporteert over de voortgang.
9. De gemeente Groningen stelt de benodigde **mensen en middelen beschikbaar** conform de bestaande afspraken om haar informatie en de informatievoorziening te kunnen beveiligen volgens de wijze gesteld in dit beleid.
10. **Procedures en regels** die voortvloeien uit het informatiebeveiligingsbeleid dienen te worden **vastgelegd, vastgesteld** (op het juiste niveau), **uitgevoerd** en periodiek

[10] Onder de planning- & controlcyclus vallen ook de interne kwaliteitssystemen.

geëvalueerd. Alle medewerkers van de gemeente Groningen worden verplicht getraind in het gebruik van de noodzakelijke beveiligingsprocedures.

11. Iedere medewerker, zowel vast als tijdelijk, intern of extern is **verplicht informatie en informatiesystemen te beschermen** tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

2 Informatiebeveiliging

2.1 Begrippenkader

De gemeente Groningen hanteert de BIG definitie van informatiebeveiliging:

*"Het proces van vaststellen van de vereiste **betrouwbaarheid** van informatieverwerking in termen van **beschikbaarheid**, **integriteit** en **vertrouwelijkheid (BIV)** alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen."*

Het begrip 'informatiebeveiliging' heeft betrekking op de volgende vier kwaliteitsaspecten:

- **Beschikbaarheid (continuïteit)**: het zorgdragen voor het zonder belemmeringen beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers, overeenkomstig de daarover gemaakte afspraken en wettelijke voorschriften. Beschikbaarheid wordt gedefinieerd als de ongestoorde voortgang van een informatieverwerking zonder verlies van informatie.
- **Integriteit (betrouwbaarheid)**: het waarborgen van de correctheid, authenticiteit, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking. Informatie die wordt weergegeven moet in overeenstemming zijn met de werkelijkheid en niets mag ten onrechte worden achtergehouden of zijn verdwenen. Hiervoor dient informatie beschermd te worden tegen mutaties door onbevoegden en tegen onbevoegde mutaties.
- **Vertrouwelijkheid (exclusiviteit)**: het beschermen van informatie tegen kennisname door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn. Uitsluitend bevoegde personen hebben (vooraf) goedgekeurde toegang tot informatie en kunnen gebruik maken van informatie.

- **Controleerbaarheid**: de mogelijkheid om en de wijze waarop (achteraf) vast te stellen is hoe de informatievoorziening en haar componenten zijn gestructureerd. Controleerbaarheid is een randvoorwaardelijk kwaliteitsaspect om *aantoonbaar* te kunnen sturen op de eerste drie primaire kwaliteitsaspecten. Een regelmatige controle op uitvoering van de beheersmaatregelen is noodzakelijk om vast te stellen of deze goed werken of hebben gewerkt. Daarom is een audittrail van groot belang.

2.2 Belang van informatieveiligheid

Informatie is één van de voornaamste bedrijfsmiddelen van de gemeente Groningen. Het verlies van informatie, uitval van ICT, of het door onbevoegden kennisnemen of (bewust) manipuleren van informatie kan ernstige gevolgen hebben voor de bedrijfsvoering. Het kan direct of indirect ook leiden tot politieke consequenties doordat maatschappelijke en/of financiële schade kan ontstaan en de gemeente Groningen daarmee imagoschade oploopt. Incidenten hebben namelijk mogelijk ernstig negatieve gevolgen voor burgers, bedrijven, partners en/of de eigen organisatie met waarschijnlijk ook politieke consequenties. Informatieveiligheid is daarom van groot belang en informatiebeveiliging is het proces dat daaraan invulling geeft. Het proces van informatiebeveiliging is primair gericht op bescherming van informatie binnen de gemeente Groningen.

2.3 Reikwijdte

De reikwijdte van informatiebeveiliging omvat de opslag en uitwisseling van informatie in alle verschijningsvormen binnen alle interne processen met onderliggende informatiesystemen. Dit beleid omvat derhalve niet alleen de beveiliging van ***digitale*** informatie binnen de ICT-infrastructuur van de gemeente Groningen (de technische infrastructuur van hardware en applicaties / informatiesystemen), maar omvat ook alle informatie daarbuiten zoals digitale informatie (in cloudapplicaties en op digitale gegevensdragers), ***analoge*** informatie (op fysieke gegevensdragers zoals papier) en zelfs ***impliciete*** / 'mondelinge' informatie (kennis en ervaring van mensen die kan worden geuit).

Het omvat het gebruik van deze informatie door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht de locatie, het tijdstip en het gebruikte proces, software of apparatuur. Het gaat bij informatiebeveiliging dus niet alleen over ICT: verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid.

Informatiebeveiliging is uitdrukkelijk niet gelijk aan de bescherming van privacy. Privacy heeft als primaire doelstelling vertrouwelijkheid van persoonsgegevens[11] te waarborgen. Informatiebeveiliging is de belangrijkste randvoorwaarde / een zeer belangrijk middel om privacy aantoonbaar te kunnen garanderen.

Informatiebeveiliging gaat dus breder dan privacy, omdat het ook randvoorwaardelijk is voor de bescherming van de vitale maatschappelijke functies, die worden ondersteund / gereguleerd met informatie (verkeer/vervoer, openbare orde en veiligheid, waterstanden, et cetera).

Dit beleid omvat de algemene basis voor de gehele informatiebeveiliging binnen de gemeente Groningen. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke beveiligingseisen, zoals bijvoorbeeld in het sociale domein voor Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI) en de gemeentelijke basisregistraties (BAG, BGT, BRO, BRP, WOZ). Deze wettelijke eisen worden als eerste in de uitwerking van het initiële informatiebeveiligingsplan en de eerste procesrisicoanalyses (zie hoofdstuk 4) meegenomen.

[11] Een gegeven dat *herleidbaar* is tot een geïdentificeerde of identificeerbaar natuurlijk persoon.

2.4 Visie

De ambitie van de gemeente Groningen is om de komende jaren de informatieveiligheid te verhogen en de totale informatiebeveiligingsfunctie binnen alle heel de organisatie verder te professionaliseren. Daarmee bereikt de gemeente Groningen onder andere dat:

De basis voor een betrouwbare informatievoorziening wordt gegarandeerd die noodzakelijk is voor het goed functioneren van de gemeente Groningen en de verbonden organisaties en die de basis vormt voor de bescherming van rechten en plichten van burgers en bedrijven (binnen en buiten de gemeente Groningen) waarvoor taken worden uitgevoerd door de gemeente Groningen.

Informatiebeveiliging wordt binnen de gemeente Groningen en verbonden organisaties gezamenlijk en integraal, op basis van risicomanagement, gericht opgepakt zodat een eenduidig geheel (raamwerk) aan beheersingsmaatregelen ontstaat dat de gehele keten versterkt.

Het onderwerp wordt breed gedragen binnen alle bestuurlijke en ambtelijke lagen van de gemeente Groningen en verbonden organisaties als onderdeel van zowel goed werkgeverschap, opdrachtnemerschap en opdrachtgeverschap.

Informatiebeveiliging is de basis voor de dienstverlening en nieuwe innovatieve manieren van werken, die op verantwoorde wijze blijvend mogelijk worden gemaakt.

2.5 Kosten en opbrengsten

2.5.1 Kosten

- De risico's en de huidige en benodigde informatiebeveiligingsmaatregelen binnen de gemeente Groningen zijn nog niet gestructureerd en volledig in kaart gebracht. Daardoor is de vraag hoeveel informatiebeveiliging in totaal kost of mag kosten nog niet zinvol te beantwoorden[12].

- Met de huidige kennis zijn de kosten voor het Informatiebeveiligingsteam, onderzoeks- en verantwoordingsaudits en bewustzijnscampagnes echter voldoende gedekt binnen de reeds beschikbare, bestaande financiële middelen en budgetten.

- De kosten van de invoering en de implementatie van alle relevante maatregelen die voortvloeien uit het informatiebeveiligingsbeleid zijn echter afhankelijk van de huidige kwaliteit en de status van reeds ingevoerde beheersingsmaatregelen in de reguliere bedrijfsvoering, de gekozen strategie, de architectuur en de inrichting van de IT-beheersingsprocessen en systemen. Daarnaast zijn de kosten afhankelijk van de toekomstige (verplichte) extra eisen en audits. De eventuele aansluiting van nieuwe verbonden organisaties en de uitbreiding van het netwerk aan ketenpartners zullen de kosten tevens beïnvloeden.

- Het doel is uiteraard om de beschikbare middelen van de gemeente Groningen zo efficiënt en effectief mogelijk in te zetten om de (wettelijke) doelstellingen van de gemeente Groningen te verwezenlijken.

- Zoals bij alle kosten is een integraal beeld zeer handig, maar niet noodzakelijk. Ook zonder een totaal beeld kan bij de invoering van een losse maatregel of set van maatregelen toch tot een afweging worden gekomen tussen de voordelen (de beveiligingswinst en effectiviteit van processen) en de nadelen (de invoerings- en

[12] Onderzoekspartijen zoals Gartner gaan uit van tussen de 6-10% van het jaarlijks IT-budget wordt gespendeerd aan (voornamelijk technische) informatiebeveiligingsmaatregelen.

onderhoudskosten). Door het integrale karakter van informatiebeveiliging mogen ook de kosten niet losstaand worden bezien van andere operationele onderwerpen.

2.5.2 Opbrengsten

- Informatieveiligheid is voor de overheid een 'license to operate'; het is de randvoorwaarde waarvan geldt dat als deze is ingevuld het betekent dat serieuze directe en indirecte schade kan worden voorkomen voor (delen van) de gemeente Groningen. Het vormt een basis voor het bestaansrecht van de gemeente Groningen.
- Het inrichten van werkende informatiebeveiligingsmaatregelen zal een serieuze bijdrage leveren aan een effectievere en efficiëntere bedrijfsvoering, omdat processen en het gebruik van systemen verder moet worden gestandaardiseerd.
- Het geeft nadere invulling aan het eigenaarschap van processen en systemen doordat taken, bevoegdheden en verantwoordelijkheden voor informatiebeveiliging concreet en expliciet dienen te worden vastgelegd.
- De kwaliteit van het totaal aan audits en interne controles wordt vergroot, doordat kan/mag worden gesteund op (rapportages uit) applicaties.
- Alleen met een gestructureerde aanpak van informatiebeveiliging kan de beschikbaarheid, integriteit en vertrouwelijkheid van informatie binnen de gemeente Groningen aantoonbaar worden gewaarborgd. Dit leidt tevens tot een minder ad hoc en meer gestructureerde aanpak van (informatiebeveiligings-)incidenten.
- Het voorkomen van aansprakelijkheidsstelling voor schade aan burgers en bedrijven, van bestuurlijke boetes en van imago/reputatieschade voor de overheidsorganisaties, hun medewerkers en bestuurders in het bijzonder.

3 Implementeren van informatiebeveiliging

3.1 Gelaagdheid

De BIG bevat als normenkader drie niveaus. De bovenste laag is opgedeeld in elf inhoudelijke hoofdstukken, conform de standaard Code voor Informatiebeveiliging. De volgorde van de hoofdstukken is van belang. Door dezelfde systematiek te volgen wordt de compliance efficiënter geborgd. Daarnaast wordt de vergelijkbaarheid met normenkaders van andere (gemeentelijke) organisaties, ten behoeve van benchmarking, vergroot.

Vanwege het huidige volwassenheidsniveau[13] en het toenemende belang van dit onderwerp voor de gemeente Groningen is er voor gekozen om de gedetailleerde invulling van maatregelen geen onderdeel te laten uitmaken van dit strategische beleid. De tactische invulling van BIG-maatregelen wordt in een apart (meer dynamisch) document, het informatiebeveiligingsplan, opgenomen met daarin verwijzingen naar de van toepassing zijnde rolbeschrijvingen en operationele werkprocesbeschrijvingen.

De implementatieaanpak voor informatiebeveiliging is ook opgebouwd in een gelaagde structuur zoals eerder is weergegeven in figuur 1:

1. Het informatiebeveiligings*beleid* behandelt de context en globale risicogebieden, afgezet tegen de kwaliteitsaspecten beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid. Het vormt het raamwerk met de doelen en de context van de maatregelen. Het geeft invulling aan het (bestaande) besturingsmodel en de rapportagelijnen: het *informatiebeveiligingsmanagementsysteem*[14] en de borging in de reguliere planning- & controlcyclus (en daarmee in de afdelingsplannen).
2. Het informatiebeveiligings*plan* beschrijft doelgericht de gerubriceerde organisatorische en technische maatregelen op onderdelen: gericht op processen,

[13] Uit intern onderzoek in 2016 naar de volwassenheid van informatiebeveiliging blijkt dat de gemeente Groningen niveau 2 heeft op de schaal van 1 tot 5 conform het CMMI-model (Capability Maturity Model Integration).
[14] Vaak aangeduid als *Information Security Management System* of ISMS.

mensen en middelen conform het BIG-normenkader en op basis van de procesrisicoanalyses (Business Impact Analyses, kortweg: BIA's).
3. De uitgewerkte procedures, regelingen en policies, waarin de maatregelen worden vertaald naar de operationele werkinstructies met taken, bevoegdheden en verantwoordelijkheden van de uitvoerende afdelingen en individuele medewerkers. Daarbij geldt dat binnen de gemeente Groningen zoveel mogelijk gebruik wordt gemaakt van in de markt beschikbare en breed geaccepteerde standaarden.

3.2 Volwassenheid – verbeterproces

Uit de verschillende (jaarlijkse) audits is gebleken dat binnen de gemeente Groningen in de komende jaren nog een duidelijk groeipad dient te worden doorlopen voordat de invoering van het totale beleid is gerealiseerd. Het beleid geeft nadrukkelijk de "soll"-situatie weer die de gemeente Groningen in de toekomst (in de komende jaren) conform de afspraken van de VNG-resolutie willen bereiken.

De gemeente Groningen streeft er naar om 'in control' te zijn en daarover op professionele wijze verantwoording af te leggen. In control zijn betekent in dit verband enerzijds dat elke afdeling van de gemeente Groningen weet welke maatregelen genomen zijn en of die werken (effectief zijn). En anderzijds dat er een SMART[15] planning is van de maatregelen die nog genomen of verbeterd (door bijvoorbeeld de uitkomsten van de BIG-gapanalyse en audits) moeten worden, maar die nog niet (volledig) zijn ingevoerd.

Binnen het beleid (Plan) worden de beveiligingsmaatregelen (Do) bottom-up ingevoerd door de uitvoerende laag van de beveiligingsorganisatie. De maatregelen worden vervolgens gecontroleerd en getoetst (Check) door de hogere kaderstellende lagen, waarna eventuele corrigerende maatregelen weer worden uitgevoerd door de uitvoerende laag (Act). Waarna de PDCA-cyclus weer opnieuw begint.

Door de ketenafhankelijkheid[16] is voor de sturing op informatiebeveiliging een totaal overzicht nodig van het informatiebeveiligingsniveau binnen de gemeente Groningen. Daarvoor dient de informatiebeveiliging verankerd te worden in de reguliere planning- & controlcyclus van iedere afdeling, waarna alle informatie door de CISO wordt samengevoegd voor één geheel beeld van de gemeente Groningen. Door centrale coördinatie kunnen de risico's voor de gemeente Groningen als geheel eerder en beter worden onderkend en kunnen verbeteringen van de beheersingsmaatregelen vervolgens effectiever en efficiënter worden ingevoerd.

3.3 Invoering maatregelen

Voor de maatregelen die impact hebben op de huidige bedrijfsvoering binnen één of meerdere afdelingen van de gemeente Groningen, zal per maatregel of set van maatregelen één implementatieplan worden opgesteld. In de implementatieplannen staat beschreven hoe de maatregelen uit de BIG stapsgewijs worden ingevoerd. Jaarlijks wordt in het informatiebeveiligingsplan vastgesteld welke maatregelen uit de BIG op deze wijze gemeente Groningen breed (met voorrang) worden opgepakt. De maatregelen uit het informatiebeveiligingsplan moeten worden verankerd in de (afdelings-)jaarplannen binnen de gemeente Groningen als onderdeel van de reguliere planning- & controlcyclus.

[15] SMART is een middel om eenduidige en controleerbare doelstellingen te maken en staat voor Specifiek, Meetbaar, Acceptabel, Realistisch en Tijdsgebonden. De kritieke prestatie-indicatoren (KPI's) in de planning- & controlcyclus dienen aan dit principe te voldoen.
[16] De zwakste schakel in de informatieketen vormt een (direct) risico voor de gehele informatieketen. Voor de meeste processen binnen de gemeente Groningen verloopt het merendeel van de informatiestromen via de ICT-infrastructuur. Daarom zijn alle gebruikers van de ICT-infrastructuur afhankelijk van elkaars informatiebeveiligingsmaatregelen.

Om de focus te houden wordt gestart met de meest kritische informatie en informatiesystemen[17]. Voor nieuwe projecten of in het geval van wijzigingen in bestaande informatiesystemen geldt steeds dat dit beleid en de BIG-maatregelen direct integraal van toepassing zijn.

Om de controleerbaarheid en efficiëntie van de beheerprocessen te vergroten worden alle beheersingsmaatregelen (in het implementatieplan) beschreven in de **5W's + H-vorm** (*Wie, Wat, Wanneer, Waar, Waarom en Hoe*). Tevens wordt in alle onderliggende documentatie een expliciete link gelegd naar de maatregelen (nummers) in de BIG. Dit bevordert de vindbaarheid van en sturing op de maatregelen en voorkomt dat bij een wijziging in de documentatie de link naar de verplichte maatregel wordt verbroken.

3.4 Status maatregelen

Iedere maatregel wordt periodiek in *opzet, bestaan* en *werking*[18] geëvalueerd en de status wordt dan bijgewerkt in een statustabel voor een actueel beeld van de stand van zaken.

4 Procesrisicoanalyse (BIA)

Uit wetenschappelijk onderzoek is gebleken dat risico's initieel vaak niet juist worden ingeschat. Pas wanneer risicomanagement een structureel onderdeel van de bedrijfsvoering vormt, wordt de ervaring (letterlijk) opgebouwd en de kwaliteit van risico-inschattingen realistischer. Risicomanagement dient derhalve een vast onderdeel te zijn binnen de reguliere planning- & controlcyclus ter continue verbetering en borging van de informatieveiligheid in de bedrijfsvoering.

De aanpak van informatiebeveiliging in de gemeente Groningen is gebaseerd op aantoonbaar bewuste (dus expliciete) risicoanalyses op de processen. Zo wordt tevens de prioriteit bepaald van de inzet van middelen en de volgorde waarin de maatregelen moeten worden geïmplementeerd.

Een procesrisicoanalyse kan alleen gedegen worden uitgevoerd met voldoende kennis van dat proces. Kennis van de applicaties en van de informatie die nodig zijn om het proces uit te (blijven) voeren zijn echter ook onmisbaar. De procesrisicoanalyses worden derhalve door de proceseigenaar uitgevoerd in samenwerking met de applicatie- en gegevenseigenaren.

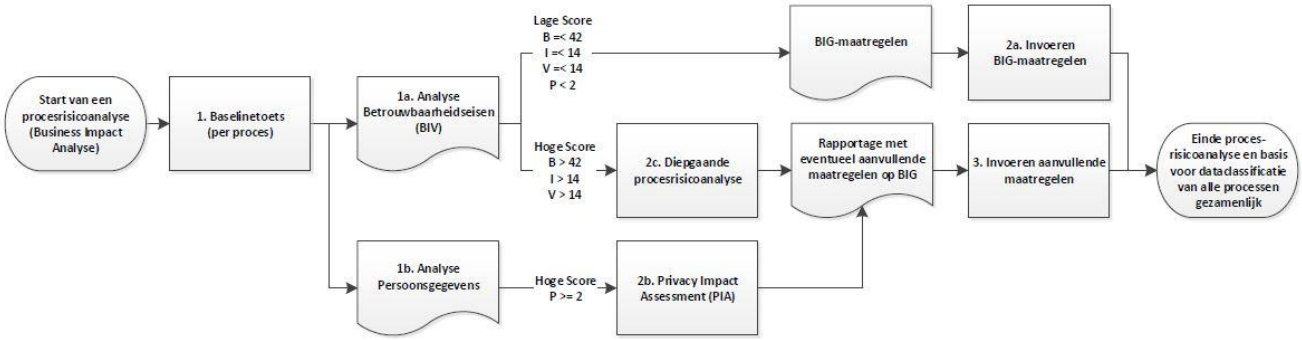
In relatie tot het eigenaarschap van processen, systemen en gegevens zijn de volgende rollen op managementniveau te onderscheiden:
De *proceseigenaar* is verantwoordelijk voor het goed functioneren van een proces dat een wisselwerking kan hebben met een of meerdere informatiesystemen.
De *applicatie-/systeemeigenaar*[19] (meestal het Shared Service Centrum van de gemeente Groningen of kortweg SSC) is verantwoordelijk voor het juist functioneren van een informatiesysteem.
De *data/gegevenseigenaar* (werkt meestal voor de proceseigenaar, maar is geregeld de proceseigenaar zelf) is verantwoordelijk voor de juistheid van de gegevens in een informatiesysteem.

[17] De dataclassificatie *kritisch* is een uitkomst van de (totaal)resultaten van de baselinetoetsen / BIA's. In eerste instantie worden hier de systemen bedoeld uit de primaire processen zoals gedefinieerd in GEMMA versie 2.0.
[18] Maatregelen dienen te zijn beschreven (*opzet*), te zijn ingevoerd (*bestaan*) en te werken over de gehele periode van onderzoek (*werking*).
[19] Met applicatie-/systeemeigenaarschap wordt niet het juridische eigendom bedoeld, maar de beheerrol van de applicatie. Zodra de applicatie op de ICT-infrastructuur van de gemeente Groningen draait, is het SSC verantwoordelijk voor het applicatiebeheer en veelal ook voor het functioneel beheer. SSC is dan technisch eigenaar van de applicatie. Voor een cloudapplicatie is de desbetreffende leverancier technisch eigenaar.

Iedere proceseigenaar inventariseert de kwetsbaarheden (operationeel, technisch en financieel) in zijn werkproces en de dreigingen die kunnen leiden tot een beveiligingsincident. De proceseigenaar stelt vast hoe groot de *kans* is dat de verstoring zich voor doet en wat de *impact* is van de verstoring van zijn proces / informatiesysteem. Daarbij wordt een inschatting gemaakt van het belang van het proces voor zijn eigen afdeling en de gemeente Groningen als geheel.

Het *risico* van beveiligingsincidenten is de *kans* op beveiligingsincidenten maal de *impact* daarvan op het werkproces: ***risico = kans x impact***.

Rekening houdend met de interne en externe beschermingseisen voor informatie bepaalt de proceseigenaar welke van deze risico's nog onacceptabel hoog zijn en treft daarna waar nodig aanvullende maatregelen. Daartoe is de procesrisicoanalyse in de vorm van een Business Impact Analyse (BIA) de geijkte methode (zie figuur 2). Als eerste dienen alle processen geschaald/geclassificeerd te worden op de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid (BIV) en privacy-gevoeligheid in de *baselinetoets*[20]. Vervolgens worden in de *diepgaande procesrisicoanalyses*[21] op alle *kritische* en *privacy gevoelige* processen de benodigde aanvullende maatregelen bepaald. De aanvullende maatregelen komen bovenop de verplichte maatregelen uit de BIG.



Figuur 2 – Stappen voor uitvoering van procesrisicoanalyse (BIA)

De te nemen (aanvullende) maatregelen moeten worden afgestemd op de risico's, waarbij rekening dient te worden gehouden met technische mogelijkheden en de kosten van maatregelen. Naarmate de informatie een gevoeliger karakter heeft, of gezien de context waarin het gebruikt wordt een groter risico inhoudt, dienen zwaardere eisen aan de beveiliging van die informatie te worden gesteld. In het algemeen kan worden gesteld, dat indien met naar verhouding geringe extra kosten meer informatiebeveiliging kan worden bewerkstelligd dit als 'passend' kan worden beschouwd. Extra informatiebeveiliging is echter niet meer passend, indien de kosten voor het mitigeren van de risico's disproportioneel hoog zijn. Kort gezegd: de risico's en tegenmaatregelen dienen in balans te zijn. Dit is meestal afhankelijk van de specifieke situatie.

Er dient te worden opgemerkt dat voor *bijzondere persoonsgegevens*[22] extra strenge privacyregels gelden met mogelijk (zeer) grote financiële consequenties voor de gemeente Groningen. Een puur financiële afweging van de maatregelen is daardoor onvoldoende.

[20] Baselinetoets BIG, VNG-IBD, versie 1.3.1, 12 maart 2018. Voorbeeld Baselinetoets, VNG-IBD, versie 1.0, juni 2014. En Handreiking Dataclassificatie, VNG-IBD, versie 1.7.1, 12 april 2018.
[21] Diepgaande risicoanalysemethode gemeenten, VNG-IBD, versie 1.0.1, juli 2016. En Risicoanalyse gemeenten – Voorbeeldrapportage, VNG-IBD, versie 1.0, 2014.
[22] Zoals bedoeld in bijvoorbeeld artikel 10, eerste lid onder d Wob jo. en hoofdstuk 2, paragraaf 2 van de Wbp/AVG.

Vanuit de theorie kan men op vier verschillende manieren een risico benaderen:

1. ***Reduceren***: expliciet benoemen en analyseren van het risico en vervolgens de benodigde maatregelen treffen om de kans en de impact te beperken.
2. ***Vermijden***: kiezen voor een andere situatie die geen risico heeft.
3. ***Overdragen***: beleggen van het geheel of een gedeelte van het risico bij een andere partij door het (proces) uit te besteden aan bijvoorbeeld een leverancier of door het te verzekeren.
4. ***Accepteren***: expliciet accepteren (door het hoogste bevoegde gezag) van de eventuele schade van het opgetreden risico.

Bij de vastlegging van de typen beheersingsmaatregelen per risico wordt het *CARP*-model gehanteerd om te visualiseren dat voor ieder risico (voldoende: niet te weinig en niet te veel) verschillende (type) maatregelen zijn getroffen. Hier wordt voor ieder type maatregel een voorbeeld gegeven:

- ***C****onfiguratie* (preventief; zoals wachtwoordinstellingen).
- ***A****utorisatie* (preventief; zoals vast gebruikersprofiel/rol voor de netwerktoegang en de autorisatiestructuur in een applicatie).
- ***R****apport* (reactief/detectief; zoals automatisch gegenereerde controlerapporten).
- ***P****rocedure* (preventief en reactief/detectief; zoals procesafspraken voor periodieke controle van gebruikersrechten of werkinstructies voor de behandeling van wijzigingsaanvragen).

Het CARP-model ondersteunt het gestructureerd inrichten en beheersen van maatregelen, waarbij expliciet aandacht is voor het onderscheid naar maatregelen die preventief zijn (vooraf) en maatregelen die reactief/detectief werken (achteraf). Preventieve maatregelen zijn meestal efficiënter in het afdekken van de risico's, maar zijn technisch gezien niet altijd mogelijk of organisatorisch gewenst.

5 Informatiebeveiligingsbeleid

De gemeente Groningen heeft behoefte aan een eenduidig beleid op het gebied van informatiebeveiliging om gericht invulling en sturing te kunnen geven aan de "soll"-situatie voor dit onderwerp. Het vaststellen met de verbonden organisaties is noodzakelijk, omdat iedereen reeds gebruik maakt van één en dezelfde technische ICT-infrastructuur. Ondanks de fysiek aparte locaties van de gemeente Groningen en verbonden organisaties is door de ICT-infrastructuur een onderlinge ketenafhankelijkheid ontstaan. Het eigenaarschap van de ICT-infrastructuur berust bij de gemeente Groningen. Eén gemeenschappelijk informatiebeveiligingsbeleid biedt daarnaast synergievoordelen en maakt de aansluiting met andere initiatieven en externe partijen eenvoudiger door de uniformiteit in communicatie en normering.

5.1 Informatiebeveiligingsbeleid

Doelstelling: Borgen van betrouwbare dienstverlening en een aantoonbaar niveau van informatiebeveiliging binnen de gemeente Groningen, waarbij de gemeente Groningen voldoet aan de relevante wetgeving. Het informatiebeveiligingsbeleid wordt algemeen geaccepteerd door al hun (keten-)partners en zorgt er mede voor dat de kritische bedrijfsprocessen bij een calamiteit of incident voortgezet kunnen worden.

5.1.1 Uitgangspunten

- De gemeente Groningen beschikt over een informatiebeveiligingsbeleid dat is opgesteld en gezamenlijk met de verbonden organisaties formeel is bekrachtigd op de hoogste organisatieniveaus (college van B&W, directies, etc.).
- Informatiebeveiligingsbeleid wordt gepubliceerd voor alle werknemers en relevante externe partijen. Het beleid is een verzameling van strategische uitgangspunten voor informatiebeveiliging. Daarin maken de bestuurlijke en ambtelijke top aan de tactische en operationele niveaus eendrachtig duidelijk welke gedragslijnen binnen de

gemeente Groningen dienen te worden gevolgd, om te komen tot een adequaat niveau van informatiebeveiliging.
- Het informatiebeveiligingsbeleid van de gemeente Groningen is in lijn met het overige interne algemene beleid.
- De gemeente Groningen dient naast de interne eisen te voldoen aan nationale en internationale / Europese wet- en regelgeving die betrekking heeft op de beveiliging van informatie en informatiesystemen. Daarbij wordt zoveel mogelijk aangesloten bij de landelijke initiatieven en beschikbare standaarden. Daarom is de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)[23] als strategisch en tactisch uitgangspunt genomen voor het informatiebeveiligingsbeleid van de gemeente Groningen. Hiermee kan ook de horizontale en verticale verantwoording[24] over informatieveiligheid worden beperkt[25].
- Het informatiebeveiligingsbeleid wordt met geplande tussenpozen, of zodra zich belangrijke wijzigingen voordoen, beoordeeld om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft. Hiertoe herijken het college van B&W en de directies gezamenlijk periodiek (minimaal eens per drie jaar of bij relevante wijzigingen) het informatiebeveiligingsbeleid.
- Het informatiebeveiligingsbeleid en het daarvan afgeleide informatiebeveiligingsplan worden continue verder ontwikkeld en worden periodiek formeel getoetst volgens vastgelegde procedures. Voor het naleven van het beleid en de plannen geldt het '*comply or explain*'-principe (pas toe of leg uit) op basis van een formele procesrisicoanalyse en risicoacceptatie, indien (nog) niet wordt / kan worden voldaan aan het informatiebeveiligingsbeleid.
- Informatiebeveiliging wordt als integraal onderdeel van de bedrijfsvoering en het risicobeheer opgepakt.
- Het beleid biedt het kader en vormt de basis voor de te hanteren normen en te treffen informatiebeveiligingsmaatregelen.
- Door middel van controles op de uitvoering dient op het hoogste managementniveau te worden vastgesteld of de maatregelen werken. Evaluatie van het beleid vindt vervolgens plaats om na te gaan of het beleid nog steeds aansluit op de gemeente Groningen en of de juiste maatregelen zijn getroffen.
- Informatiebeveiliging is onderdeel van de informatiearchitectuur van de gemeente Groningen. Deze architectuur beschrijft onder meer principes, richtlijnen en maatregelen op basis van verschillende beschermingsniveaus (dataclassificaties).
- De informatiebeveiligingsprocessen vormen een onderdeel van de landelijke referentiearchitectuur voor gemeenten: GEMeentelijke Model Architectuur of GEMMA (versie 2.0), waarmee de basis voor informatieveiligheid is verankerd als integraal onderdeel van de interne gemeentelijke bedrijfsvoering.

6 Organisatie van informatiebeveiliging

6.1 Interne organisatie

Doelstelling: Beheren van de informatiebeveiliging binnen de organisatie.

6.1.1 Uitgangspunten

- De hoogste managementlagen (alle bestuurders en leidinggevenden) ondersteunen actief informatiebeveiliging binnen de gemeente Groningen door duidelijk richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor

[23] De BIG is opgesteld door de Informatiebeveiligingsdienst (VNG-IBD) en is gebaseerd op de algemeen erkende Code voor Informatiebeveiliging (NEN/ISO 27001/27002:2007).
[24] Verantwoording vanuit de gemeente aan het rijk, vanuit de systeemverantwoordelijkheid van de minister.
[25] Het terugdringen van verantwoordingslast verloopt sinds 2017 via de Eenduidige Normatiek Singel Information Audit (ENSIA). De verantwoording over de informatieveiligheidseisen richting de gemeenteraad en de ministeries dient verplicht te worden geaudit vanuit de diverse regel- en wetgevingen zoals BAG, BRP, DigiD, SUWI en de algemene IT-audit in het kader van de jaarrekeningcontrole. Een groot deel van de eisen uit die audits overlappen met de onderdelen van de BIG.

informatiebeveiliging toe te kennen en te erkennen. Zie verder de beslissende en sturende rol in paragraaf 6.1.2.

- Deze managementlagen waarborgen dat de informatiebeveiligingsdoelstellingen worden vastgesteld en voldoen aan de kaders zoals gesteld in dit beleid en zijn geïntegreerd in de relevante processen. Dit gebeurt door één keer per jaar de opzet, het bestaan en de werking van de informatiebeveiligingsmaatregelen te bespreken en hiervan verslag te doen.
- Activiteiten voor informatiebeveiliging worden uitgevoerd en gecoördineerd door vertegenwoordigers uit de verschillende delen van de gemeente Groningen met relevante rollen en functies.
- De rollen van de Chief Information Security Officer (CISO [26]) en van het lijnmanagement zijn beschreven.
  a. De CISO rapporteert rechtstreeks aan de hoogste managementlagen.
  b. De CISO bevordert en adviseert gevraagd en ongevraagd over de informatiebeveiliging van de gemeentelijke organisatie, verzorgt rapportages over de status, controleert of met betrekking tot de informatiebeveiliging van de gemeente Groningen de maatregelen worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de informatiebeveiliging.
- Alle verantwoordelijkheden voor informatiebeveiliging binnen de gemeente Groningen zijn duidelijk gedefinieerd in een organisatieschema met alle informatiebeveiligingsfuncties. Daarbij zijn voor alle relevante afdelingen vaste aanspreekpunten voor informatiebeveiliging formeel toegewezen.
- Het SSC[27] beheert de technische ICT-infrastructuur voor de gemeente Groningen en verbonden organisaties, daarvoor is een formele goedkeuringsprocedure vastgesteld en geïmplementeerd die zij hanteert voor het autoriseren van de invoering van nieuwe of de wijziging van bestaande ICT-voorzieningen.
- De eisen voor de vertrouwelijkheid van informatie en voor de verplichte (juridische) inhoud van geheimhoudingsovereenkomsten zijn vastgesteld en worden regelmatig beoordeeld.
- Er worden geschikte contacten met relevante overheidsinstanties onderhouden. Daarvoor stelt het lijnmanagement vast in welke gevallen en door wie er contacten met autoriteiten (brandweer, toezichthouders, enz.) wordt onderhouden (in lijn met de mandaatbesluiten).
- Namens de gemeente Groningen participeert het Informatiebeveiligingsteam in (landelijke) overlegorganen over informatiebeveiliging, zoals de Informatiebeveiligingsdienst voor gemeenten. Het Informatiebeveiligingsteam neemt daarbij deel aan relevante activiteiten die de informatiebeveiliging binnen de gemeente Groningen bevorderen, die worden georganiseerd door speciale belangengroepen of platforms en professionele organisaties.
- De benadering van de gemeente Groningen voor het beheer van informatiebeveiliging en de implementatie daarvan (dat wil zeggen beleid, beheerdoelstellingen, beheersmaatregelen, processen en procedures voor informatiebeveiliging) wordt onafhankelijk en met geplande tussenpozen beoordeeld, of zodra zich wijzigingen voordoen in de implementatie van de beveiliging.
- De kwaliteit van de informatiebeveiliging wordt periodiek (minimaal eens in de 3 jaar) door een onafhankelijke derde (door een onafhankelijke deskundige) beoordeeld en desgewenst bijgesteld.
- Periodieke beveiligingsaudits worden uitgevoerd in opdracht van het lijnmanagement.

[26] De BIG heeft gekozen voor *Chief Information Security Officer* als benaming voor deze rol, om enerzijds aan te sluiten bij de gangbare benaming van deze rol binnen andere grote gemeenten, het Rijk en het bedrijfsleven. Anderzijds om een duidelijk onderscheid te maken met de verschillende bestaande wettelijke rollen (die reeds een *deel*verantwoordelijkheid hebben op dit domein, zoals de BRP beveiligingsbeheerder, de Security Officer voor Suwinet en de Privacy Officer voor de gemeente Groningen binnen de afdeling Juridische Zaken) en met de *ISO*-normeringen in dit domein. Daarnaast benadrukt het de plaatsing/locatie van deze rol binnen het Informatiebeveiligingsteam met Information Security Officers binnen de Regieorganisatie.
[27] Vanaf september 2018 wordt het technisch beheer door het SSC uitbesteed aan Fujitsu.

- Over het functioneren van de informatiebeveiliging wordt, conform de planning- & controlcyclus, jaarlijks gerapporteerd aan het lijnmanagement.

6.2 Externe partijen

Doelstelling: Het beveiligen van de informatie en ICT-voorzieningen van de gemeente Groningen waar externe partijen toegang toe hebben (voor beheer of verwerking) en informatie die naar externe partijen wordt gecommuniceerd.

6.2.1 Uitgangspunten

- De informatiebeveiligingsrisico's voor de bedrijfsprocessen waarbij externe partijen (leveranciers en ketenpartners waarmee de gemeente Groningen samenwerken en informatie mee uitwisselen) betrokken zijn, worden geïdentificeerd en er worden geschikte beheersmaatregelen geïmplementeerd voordat toegang wordt verleend.
- Alle geïdentificeerde beveiligingseisen worden beoordeeld voordat klanten (burgers en bedrijven) toegang wordt verleend tot de informatie of bedrijfsmiddelen van de gemeente Groningen.
- In (bewerkers)overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of ICT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan ICT-voorzieningen (bewerkersovereenkomsten) worden geregeld, zijn alle relevante beveiligingseisen opgenomen.

7 Beheer van bedrijfsmiddelen

7.1 Verantwoordelijkheid voor bedrijfsmiddelen

Doelstelling: Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de gemeente Groningen door het definiëren van de verschillende beveiligingsniveaus aan de hand van een formeel classificatiesysteem.

7.1.1 Uitgangspunten

- Alle bedrijfsmiddelen met informatie zijn duidelijk geïdentificeerd en staan in een actuele inventaris van alle bedrijfsmiddelen.
- Van alle informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen is expliciet het eigenaarschap (op de niveaus proces, applicatie-/systeem, gegevens) belegd binnen de gemeente Groningen bij een formeel verantwoordelijke[28].
- Er zijn regels vastgesteld, gedocumenteerd en geïmplementeerd voor het aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen.

7.2 Classificatie van informatie en bedrijfsmiddelen

Doelstelling: Bewerkstelligen dat informatie en bedrijfsmiddelen een geschikt niveau van bescherming krijgen.

7.2.1 Uitgangspunten

- Informatie (en daarvan afgeleid de bedrijfsmiddelen) is juist en tijdig op basis van formeel vastgestelde richtlijnen geclassificeerd[29] met betrekking tot de waarde,

[28] Eigenaarschap wordt vastgelegd in de Configuration Management Database (CMDB). Momenteel wordt hiervoor gebruik gemaakt van de applicatie *CMDBuild*. Deze applicatie zal in 2019 door Fujitsu worden vervangen door *Service Now*.

[29] Voor de classificatie van informatiesystemen gebruikt de gemeente Groningen in lijn met de BIG de *Baselinetoets* in combinatie met de *Handreiking Dataclassificatie* (beide van VNG-IBD) voor het expliciet kwantificeren van de kwaliteitsaspecten BIV en privacy. Vervolgens wordt het MAPGOOD-model (mensen, apparatuur, programmatuur, gegevens, omgeving, organisatie en diensten) gebruikt in de risicoanalyse voor het in expliciet in kaart brengen van dreigingen en beveiligingsmaatregelen voor alleen de *kritische* processen en systemen.

wettelijke eisen[30] en interne eisen van gevoeligheid en onmisbaarheid (beschikbaarheid, integriteit en vertrouwelijkheid) voor de gemeente Groningen.
- Er zijn geschikte, samenhangende procedures ontwikkeld en geïmplementeerd voor het labelen en verwerken van informatie overeenkomstig het classificatiesysteem dat de gemeente Groningen heeft geïmplementeerd.

8 Personele beveiliging

8.1 Voorafgaand aan het dienstverband

Doelstelling: Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers binnen de gemeente Groningen hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen.

8.1.1 Uitgangspunten

- De rollen en verantwoordelijkheden van werknemers, ingehuurd personeel en externe gebruikers ten aanzien van informatiebeveiliging worden vastgesteld en gedocumenteerd overeenkomstig het beleid voor informatiebeveiliging van de gemeente Groningen.
- Screening (verificatie van de achtergrond) van alle kandidaten voor een dienstverband, ingehuurd personeel en externe gebruikers worden uitgevoerd overeenkomstig relevante wetten, voorschriften en ethische overwegingen, en zijn evenredig aan de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend, en de waargenomen risico's.
- Als onderdeel van hun contractuele verplichting aanvaarden werknemers, ingehuurd personeel en externe gebruikers de algemene voorwaarden (inclusief dit beleid) en ondertekenen voor de start van hun werkzaamheden een contract, waarin hun verantwoordelijkheden en die van de gemeente Groningen ten aanzien van informatiebeveiliging formeel zijn vastgelegd.

8.2 Tijdens het dienstverband

Doelstelling: Bewerkstelligen dat alle werknemers, ingehuurd personeel en externe gebruikers binnen de gemeente Groningen zich bewust zijn van bedreigingen en gevaren voor informatiebeveiliging, van hun verantwoordelijkheid en aansprakelijkheid, en dat ze zijn toegerust om het informatiebeveiligingsbeleid van de gemeente Groningen in hun dagelijkse werkzaamheden te ondersteunen en het risico van menselijke fouten te verminderen.

8.2.1 Uitgangspunten

- Het lijnmanagement eist van interne werknemers, ingehuurd personeel en externe gebruikers dat ze informatiebeveiliging toepassen overeenkomstig vastgesteld beleid en vastgestelde procedures van de gemeente Groningen.
- Alle interne en externe werknemers van de gemeente Groningen krijgen, voor zover relevant voor hun functie, geschikte training en regelmatige bijscholing met betrekking tot beleid en procedures van de gemeente Groningen.
- Er is een formeel disciplinair proces vastgesteld voor werknemers die inbreuk op de informatiebeveiliging hebben gepleegd.

8.3 Beëindiging of wijziging van het dienstverband

Doelstelling: Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers ordelijk de gemeente Groningen verlaten of hun dienstverband wijzigen.

[30] Specifiek voor de AVG: Voor alle gevoelige informatie, maar zeker voor de *bijzondere categorieën*, zoals 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.

8.3.1 Uitgangspunten

- De verantwoordelijkheden voor beëindiging of wijziging van het dienstverband zijn duidelijk vastgesteld en toegewezen.
- Alle werknemers, ingehuurd personeel en externe gebruikers retourneren alle bedrijfsmiddelen van de gemeente Groningen die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst, of het bedrijfsmiddel wordt na wijziging van het dienstverband aangepast.
- De toegangsrechten van alle werknemers, ingehuurd personeel en externe gebruikers tot informatie en ICT-voorzieningen worden geblokkeerd bij beëindiging van het dienstverband, het contract of de overeenkomst, of worden na wijziging aangepast.

9 Fysieke beveiliging en beveiliging van de omgeving

9.1 Beveiligde ruimten

Doelstelling: Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de gemeente Groningen.

9.1.1 Uitgangspunten

- Er zijn toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) aangebracht om ruimten te beschermen waar zich (niet openbare) informatie en ICT-voorzieningen bevinden.
- Beveiligde zones zijn beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten.
- Er is fysieke beveiliging van kantoren, ruimten en faciliteiten ontworpen en toegepast.
- Ruimten met kritische faciliteiten zijn fysiek beschermd tegen schade door hitte, brand, vocht, overstroming, aardschokken, explosies, oproer en andere vormen van natuurlijke of menselijke calamiteiten ontworpen en toegepast (airco, rooksensoren, blusmateriaal, etc.).
- Er zijn een fysieke bescherming en richtlijnen voor werken in beveiligde ruimten ontworpen en toegepast.
- Toegangspunten zoals gebieden voor laden en lossen en andere punten waar onbevoegden het terrein kunnen betreden, zijn beheerst en indien mogelijk afgeschermd van ICT-voorzieningen, om onbevoegde toegang te voorkomen.

9.2 Beveiliging van apparatuur

Doelstelling: Het voorkomen van verlies, schade, diefstal of compromitteren van bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten.

9.2.1 Uitgangspunten

- Apparatuur is zo geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang worden verminderd.
- Apparatuur is beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen.
- Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, zijn tegen interceptie of beschadiging beschermd conform de norm NEN 1010[31].
- Apparatuur wordt op correcte wijze onderhouden, om te waarborgen dat deze voortdurend beschikbaar is en in goede staat verkeert.
- Apparatuur buiten de terreinen is beveiligd waarbij rekening is gehouden met de diverse risico's van werken buiten de terreinen van de gemeente Groningen.

[31] Zie ook het handboek ICT-huisvesting en bekabeling van de Rijksgebouwendienst: http://www.rijksvastgoedbedrijf.nl/documenten/richtlijn/2008/07/01/handboek-ict-huisvesting-en-bekabeling-hib-versie-1.0.

- Alle apparatuur die opslagmedia bevat[32], wordt gecontroleerd om te bewerkstelligen dat alle gevoelige informatie en in licentie gebruikte programmatuur zijn verwijderd of veilig zijn overschreven voordat de apparatuur wordt verwijderd.
- Apparatuur, informatie en programmatuur van de gemeente Groningen mogen niet zonder expliciete toestemming van de eigenaar vooraf van de locatie worden meegenomen.

10 Beheer van communicatie- en bedieningsprocessen

10.1 Bedieningsprocedures en -verantwoordelijkheden

Doelstelling: Waarborgen van een correcte en veilige bediening van ICT-voorzieningen.

10.1.1 Uitgangspunten

- Bedieningsprocedures zijn gedocumenteerd, actueel en digitaal beschikbaar gesteld aan alle gebruikers die deze nodig hebben.
- Alle wijzigingen in ICT-voorzieningen en informatiesystemen worden formeel en beheerst doorgevoerd.
- Taken en verantwoordelijkheidsgebieden zijn gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de gemeente Groningen te verminderen.
- Faciliteiten voor ontwikkeling, testen en/of acceptatie en productie zijn gescheiden om het risico van onbevoegde toegang tot of wijzigingen in het productiesysteem te verminderen.

10.2 Exploitatie door een derde partij

Doelstelling: Een geschikt niveau van informatiebeveiliging en dienstverlening implementeren en bijhouden in overeenstemming met de overeenkomsten voor dienstverlening door een derde partij.

10.2.1 Uitgangspunten

- Iedere afdeling / organisatie is zelf eindverantwoordelijk voor de beveiliging van haar dienstverlening. Er wordt aantoonbaar bewerkstelligd dat de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening, zoals vastgelegd in de overeenkomst voor dienstverlening door een derde partij, worden geïmplementeerd en uitgevoerd en worden bijgehouden door die derde partij.
- De diensten, rapporten en registraties die door de derde partij worden geleverd, worden regelmatig gecontroleerd en beoordeeld en er worden regelmatig audits uitgevoerd.
- Wijzigingen in de dienstverlening door derden, waaronder het bijhouden en verbeteren van bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging, worden binnen contractmanagement beheerd, waarbij rekening wordt gehouden met de onmisbaarheid van de betrokken bedrijfssystemen en -processen en met heroverweging van risico's.

10.3 Systeemplanning en -acceptatie

Doelstelling: Het risico van systeemstoringen tot een minimum beperken.

10.3.1 Uitgangspunten

- Het gebruik van middelen wordt gecontroleerd en afgestemd door de applicatie-eigenaar (veelal SSC). Er worden verwachtingen opgesteld voor toekomstige capaciteitseisen, om de vereiste systeemprestaties te bewerkstelligen.

[32] In het geval van Bring Your Own Device geldt 'zero footprint' waardoor géén bedrijfsinformatie op het apparaat staat. Anders is een policy nodig die regelt dat data wordt verwijderd als de apparatuur niet meer gebruikt wordt door de medewerker.

- Er worden aanvaardingscriteria door de applicatie-eigenaar vastgesteld voor nieuwe informatiesystemen, upgrades en nieuwe versies en er wordt tijdens ontwikkeling en voorafgaand aan formele de acceptatie door de proceseigenaren aantoonbaar een geschikte acceptatietest van het systeem en de koppelingen uitgevoerd.

10.4 Bescherming tegen virussen en 'mobile code[33]'

Doelstelling: Beschermen van de integriteit van programmatuur en informatie.

10.4.1 Uitgangspunten

- Er zijn maatregelen getroffen voor de detectie, de preventie en het herstel ter bescherming tegen *malware*[34] (zoals virussen) en er zijn geschikte procedures ingevoerd om het bewustzijn van de gebruikers te vergroten.
- Als gebruik van 'mobile code' is toegelaten, dient de configuratie te bewerkstelligen dat de geautoriseerde 'mobile code' functioneert volgens een duidelijk vastgesteld beveiligingsbeleid, en wordt voorkomen dat onbevoegde 'mobile code' wordt uitgevoerd.

10.5 Back-up

Doelstelling: Handhaven van de beschikbaarheid en integriteit van informatie en ICT-voorzieningen.

10.5.1 Uitgangspunten

- Er worden reservekopieën (back-ups) van informatie en programmatuur gemaakt en regelmatig getest conform het overeenkomstig en vastgestelde back-upbeleid.

10.6 Beheer van netwerkbeveiliging

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

10.6.1 Uitgangspunten

- Netwerken worden adequaat beheerd en beheerst om ze te beschermen tegen bedreigingen en om beveiliging te handhaven voor de systemen en toepassingen die gebruikmaken van het netwerk, waaronder de informatie die wordt getransporteerd.
- Beveiligingskenmerken, niveaus van dienstverlening en beheereisen voor alle netwerkdiensten worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten.

10.7 Behandeling van media

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

10.7.1 Uitgangspunten

- De gemeente Groningen heeft procedures vastgesteld voor het beheer van verwijderbare media (zoals een harde schijf en een USB-stick).
- Media worden op een veilige en beveiligde manier verwijderd (en zo nodig vernietigd) als ze niet langer nodig zijn, overeenkomstig formele procedures.
- Er worden procedures vastgesteld voor de behandeling en opslag van informatie om deze te beschermen tegen onbevoegde openbaarmaking of misbruik.

[33] Mobile code is software die tussen systemen wordt overgedragen en welke vervolgens wordt uitgevoerd op het lokale system, denk hier bijvoorbeeld aan JavaScript, Adobe Flash animaties of Microsoft Silverlight. Meestal gebeurt dit in een browser, maar het kan ook een e-mailbijlage, zoals een officedocument, een afbeelding of een PDF zijn.

[34] Afkomstig van *malicious software* (kwaadwillende software).

- Systeemdocumentatie wordt beschermd tegen onbevoegde toegang.

10.8 Uitwisseling van informatie

Doelstelling: Handhaven van beveiliging van informatie en programmatuur die wordt uitgewisseld binnen de gemeente Groningen en met externe partijen.

10.8.1 Uitgangspunten

- De gemeente Groningen heeft formeel beleid, formele procedures en formele beheersmaatregelen vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen.
- Er worden overeenkomsten vastgesteld voor de uitwisseling van informatie en programmatuur tussen de gemeente Groningen en externe partijen.
- Media die informatie bevatten worden binnen de gemeente Groningen beschermd tegen onbevoegde toegang, misbruik of corrumperen tijdens transport buiten de fysieke begrenzing van de locatie van de organisatie.
- Informatie die een rol speelt bij elektronische berichtuitwisseling wordt op geschikte wijze beschermd.
- Beleid en procedures zijn ontwikkeld en geïmplementeerd om informatie te beschermen die een rol speelt bij de onderlinge koppeling van systemen voor bedrijfsinformatie.

10.9 Diensten voor elektronische bedrijfsvoering[35]

Doelstelling: Bewerkstelligen van de beveiliging van diensten voor elektronische bedrijfsvoering, en veilig gebruik ervan.

10.9.1 Uitgangspunten

- Informatie die een rol speelt bij elektronische bedrijfsvoering en die via openbare netwerken wordt uitgewisseld, wordt beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en modificatie.
- Informatie die een rol speelt bij online-transacties wordt beschermd om onvolledige overdracht, onjuiste routing, onbevoegde wijziging van berichten, onbevoegde openbaarmaking, onbevoegde duplicatie of weergave van berichten te voorkomen.
- De betrouwbaarheid van de informatie die beschikbaar wordt gesteld op een openbaar toegankelijk systeem wordt beschermd om onbevoegde modificatie te voorkomen.

10.10 Controle

Doelstelling: Ontdekken van onbevoegde informatieverwerkingsactiviteiten.

10.10.1 Uitgangspunten

- Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen worden vastgelegd in audit-logbestanden. Deze audit-logbestanden voldoen aan de daarvoor geldende wet- en regelgeving. Deze logbestanden worden gedurende de (wettelijk) verplichte periode bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.
- Er zijn procedures vastgesteld om het gebruik van ICT-voorzieningen te controleren. Het resultaat van de controleactiviteiten wordt regelmatig beoordeeld.
- Logfaciliteiten en informatie in logbestanden voldoen aan de (wettelijke) voorschriften daaromtrent en worden beschermd tegen inbreuk en onbevoegde toegang.
- Activiteiten van systeemadministrators en systeemoperators worden in logbestanden te vastgelegd.

[35] In de BIG aangeduid met de internationale term e-commerce. Het is de verzamelnaam van alle manieren waarop via computernetwerken (voornamelijk het internet) elektronische diensten worden aangeboden. Dit kan tevens worden aangeduid met de term *elektronische overheid*.

- Storingen worden in logbestanden vastgelegd en worden volgens een vast stramien geanalyseerd en opgevolgd met geschikte maatregelen.
- De klokken van alle relevante informatiesystemen binnen een organisatie of beveiligingsdomein zijn gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron.

11 Toegangsbeveiliging

11.1 Toegangsbeleid

Doelstelling: Beheersen van de toegang tot informatie.

11.1.1 Uitgangspunten

- Er is toegangsbeleid vastgesteld, gedocumenteerd en beoordeeld op basis van organisatie-eisen en beveiligingseisen voor toegang.

11.2 Beheer van toegangsrechten van gebruikers

Doelstelling: Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot informatiesystemen voorkomen.

11.2.1 Uitgangspunten

- Er zijn formele procedures voor het registreren en afmelden van gebruikers vastgesteld, voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten.
- De toewijzing en het gebruik van speciale bevoegdheden worden beperkt en beheerst.
- De toewijzing van wachtwoorden wordt met een formeel beheerproces beheerst.
- Proceseigenaren beoordelen de toegangsrechten van de gebruikers van applicaties in hun proces regelmatig in een formeel proces.

11.3 Verantwoordelijkheden van gebruikers

Doelstelling: Voorkomen van onbevoegde toegang door gebruikers, en van beschadiging of diefstal van informatie en ICT-voorzieningen.

11.3.1 Uitgangspunten

- Alle gebruikers voldoen aan het wachtwoordbeleid van de gemeente Groningen en nemen in geval de volgende goede beveiligingsgewoontes in acht bij het kiezen en gebruiken van wachtwoorden:
    - Wachtwoorden worden niet opgeschreven.
    - Gebruikers delen hun wachtwoord nooit met anderen.
    - Wachtwoorden mogen niet opeenvolgend zijn.
    - Een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde.
    - Wachtwoorden worden niet gebruikt in automatische inlogprocedures (bijvoorbeeld opgeslagen onder een functietoets of in een macro).
- Gebruikers bewerkstelligen dat onbeheerde apparatuur passend is beschermd.
- Er geldt een formeel *"clean desk"*-beleid[36] voor papier en verwijderbare opslagmedia en een *"clear screen"*-beleid voor ICT-voorzieningen.

11.4 Toegangsbeheersing voor netwerken

Doelstelling: Het voorkomen van onbevoegde toegang tot netwerkdiensten.

[36] Naast informatiebeveiliging overlapt dit uitgangspunt met het flexibiliseringsconcept in *Het Nieuwe Werken* (zoals dat reeds geldt voor de flexwerkplekken bij de gemeente en in het werkplekconcept van het SSC). In dit principe laat iedere medewerker zijn eigen bureau of flexwerkplek aan het einde van de dag schoon en leeg (zonder documenten) achter.

11.4.1 Uitgangspunten

- Gebruikers wordt alleen toegang verleend tot netwerkdiensten (waaronder Wi-Fi) waarvoor ze expliciet en specifiek bevoegd zijn.
- Er worden geschikte authenticatiemethoden gebruikt om toegang van gebruikers op afstand te beheersen.
- Automatische identificatie van (netwerk)apparatuur wordt gebruikt als de methode om verbindingen vanaf specifieke locaties en apparatuur te authentiseren op *vertrouwde* zone(s). Alle overige apparatuur (zoals *Bring Your Own Device*) wordt alleen aangesloten op *onvertrouwde* zone(s).
- De fysieke en logische toegang tot poorten voor diagnose en configuratie wordt beheerst.
- Groepen informatiediensten, gebruikers en informatiesystemen worden op netwerken gescheiden.
- Voor gemeenschappelijke netwerken, vooral waar deze de grenzen van de gemeente Groningen (en binnen de verschillende verbonden organisaties) overschrijden (zoals een extranet), zijn de toegangsmogelijkheden voor gebruikers beperkt, overeenkomstig het toegangsbeleid en de eisen van bedrijfstoepassingen.
- Netwerken zijn voorzien van beheersmaatregelen voor netwerkroutering, om te bewerkstelligen dat computerverbindingen en informatiestromen niet in strijd zijn met het toegangsbeleid voor de bedrijfstoepassingen.

11.5 Toegangsbeveiliging voor besturingssystemen

Doelstelling: Voorkomen van onbevoegde toegang tot besturingssystemen.

11.5.1 Uitgangspunten

- Toegang tot besturingssystemen wordt beheerst met een beveiligde inlogprocedure.
- Elke gebruiker beschikt over een unieke identificatiecode (gebruikers-ID/account) voor uitsluitend persoonlijk gebruik, en er is een geschikte authenticatietechniek gekozen om de geclaimde identiteit van de gebruiker te kunnen bewijzen. Daarmee is ieder gebruikersaccount te herleiden tot één persoon of systeem (in het geval van systeemaccounts). Alleen onder strikte voorwaarden wordt hiervan afgeweken.
- Systemen voor wachtwoordbeheer zijn interactief en bewerkstelligen dat alleen wachtwoorden van geschikte kwaliteit kunnen worden gekozen.
- Alle systemen voldoen aan het wachtwoordbeleid van de gemeente Groningen.
- Het gebruik van hulpprogrammatuur waarmee systeem- en applicatiebeheersmaatregelen zouden kunnen worden gepasseerd zijn beperkt en worden strikt beheerst.
- Inactieve sessies worden na een vastgestelde periode van inactiviteit uitgeschakeld.
- De verbindingstijd wordt beperkt als aanvullende beveiliging voor toepassingen met een verhoogd risico (onderhoud op afstand door leveranciers).

11.6 Toegangsbeheersing voor toepassingen en informatie

Doelstelling: Voorkomen van onbevoegde toegang tot informatie in toepassingssystemen.

11.6.1 Uitgangspunten

- Toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel wordt beperkt overeenkomstig het vastgestelde toegangsbeleid.
- Gevoelige systemen hebben een eigen, vast toegewezen (geïsoleerde) computeromgeving.

11.7 Draagbare computers en telewerken

Doelstelling: Waarborgen van informatiebeveiliging bij het gebruik van draagbare computers en faciliteiten voor telewerken (binnen de gemeente Groningen via *Het Nieuwe Werken*[37]).

11.7.1 Uitgangspunten

- Er is formeel beleid vastgesteld en er zijn geschikte beveiligingsmaatregelen getroffen ter bescherming tegen risico's van het gebruik van draagbare computers en communicatiefaciliteiten.
- Er zijn beleid, operationele plannen en procedures voor telewerken ontwikkeld en geïmplementeerd.

12 Verwerving, ontwikkeling en onderhoud van informatiesystemen

12.1 Beveiligingseisen voor informatiesystemen

Doelstelling: Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.

12.1.1 Uitgangspunten

- In bedrijfseisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen worden altijd de eisen voor beveiligingsmaatregelen meegenomen. Daarbij is leidende adagium 'security by design'[38].

12.2 Correcte verwerking in toepassingen

Doelstelling: Voorkomen van fouten, verlies, onbevoegde modificatie of misbruik van informatie in toepassingen.

12.2.1 Uitgangspunten

- Gegevens die worden ingevoerd in de primaire bedrijfstoepassingen (zoals de kern- en basisregistraties) worden gevalideerd om te bewerkstelligen dat deze gegevens juist en geschikt zijn.
- Er worden validatiecontroles opgenomen in toepassingen om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen te ontdekken.
- Er worden eisen vastgesteld, en geschikte beheersmaatregelen vastgesteld en geïmplementeerd, voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.
- Gegevensuitvoer uit een toepassing wordt gevalideerd, om te bewerkstelligen dat de verwerking van opgeslagen gegevens op de juiste manier plaatsvindt en geschikt is gezien de omstandigheden.

12.3 Cryptografische beheersmaatregelen

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

[37] Het beleid voor tijd en plaats onafhankelijk werken: *Het Nieuwe* Werken binnen de gemeente Groningen (via telewerken thuis).

[38] Het meenemen van beveiligingseisen in het ontwerp (van processen, applicaties en systemen) voorkomt beveiligingsrisico's in de productieomgeving. Het treffen van nieuwe, corrigerende maatregelen in een bestaande productieomgeving is veel duurder en werkt verstorend voor het reguliere bedrijfsproces. Bepaalde beveiligingseisen zijn zelfs "knock-out"-(acceptatie)criteria voor een veilige infrastructuur. Door deze criteria vanaf het begin in het ontwerp mee te nemen worden wijzigingen (en mogelijk zelfs vroegtijdige vervanging van applicaties / systemen) op een later tijdstip voorkomen.

12.3.1 Uitgangspunten

- Er wordt beleid ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie.
- Er wordt sleutelbeheer vastgesteld ter ondersteuning van het gebruik van cryptografische technieken binnen de organisatie.

12.4 Beveiliging van systeembestanden

Doelstelling: Beveiliging van systeembestanden bewerkstelligen.

12.4.1 Uitgangspunten

- Er zijn procedures vastgesteld om de installatie van programmatuur op productiesystemen te beheersen.
- Testgegevens worden zorgvuldig gekozen, beschermd en beheerst.
- De toegang tot broncode van programmatuur wordt beperkt.

12.5 Beveiliging bij ontwikkelings- en ondersteuningsprocessen

Doelstelling: Beveiliging van toepassingsprogrammatuur en -informatie handhaven.

12.5.1 Uitgangspunten

- De implementatie van wijzigingen wordt beheerst door middel van formele procedures voor wijzigingsbeheer.
- Bij wijzigingen in besturingssystemen worden bedrijfskritische toepassingen beoordeeld en formeel getest om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de activiteiten of beveiliging van de informatievoorziening van de gemeente Groningen. Voor websites geldt dat een (externe) penetratietest[39] wordt uitgevoerd voor dat deze in de lucht wordt gebracht.
- Wijzigingen in programmatuur/standaardpakketten worden ontmoedigd, beperkt tot noodzakelijke wijzigingen, en alle wijzigingen worden strikt beheerst.
- Er wordt voorkomen dat zich gelegenheden voordoen waarin informatie wordt uitgelekt en er is formeel een proces waarin het lekken van (persoons)informatie gemeld wordt.
- Uitbestede ontwikkeling van programmatuur staat onder supervisie van en wordt expliciet gecontroleerd door de gemeente Groningen.

12.6 Beheer van technische kwetsbaarheden

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

12.6.1 Uitgangspunten

- Er wordt tijdig informatie verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie bloot staat aan dergelijke kwetsbaarheden wordt geëvalueerd en er worden geschikte maatregelen genomen voor behandeling van daarmee samenhangende risico's.

[39] Hierbij gelden de NCSC- of OWASP-richtlijnen.

13 Beheer van informatiebeveiligingsincidenten

13.1 Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken

Doelstelling: Bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.

13.1.1 Uitgangspunten

- Informatiebeveiligingsgebeurtenissen worden zo snel mogelijk via de juiste leidinggevende niveaus gerapporteerd.
- Van alle werknemers, ingehuurd personeel en externe gebruikers van informatiesystemen en -diensten wordt geëist dat zij alle waargenomen of verdachte zwakke plekken in systemen of diensten registreren en rapporteren.

13.2 Beheer van informatiebeveiligingsincidenten en verbeteringen

Doelstelling: Bewerkstelligen dat een consistente en doeltreffende benadering wordt toegepast voor het beheer van informatiebeveiligingsincidenten.

13.2.1 Uitgangspunten

- Er zijn verantwoordelijkheden en procedures vastgesteld om een snelle, doeltreffende en ordelijke reactie op informatiebeveiligingsincidenten te bewerkstelligen.
- Er zijn mechanismen ingesteld waarmee de aard, omvang en kosten van informatiebeveiligingsincidenten kunnen worden gekwantificeerd en gecontroleerd.
- Waar een vervolgprocedure tegen een persoon of organisatie na een informatiebeveiligingsincident juridische maatregelen omvat (civiel of strafrechtelijk), wordt bewijsmateriaal verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

14 Bedrijfscontinuïteitsbeheer

14.1 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

Doelstelling: Tegengaan van onderbreking van bedrijfsactiviteiten en bescherming van kritische bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.

14.1.1 Uitgangspunten

- Er wordt een beheerd proces voor bedrijfscontinuïteit in de gehele organisatie ontwikkeld en bijgehouden, voor de naleving van eisen voor informatiebeveiliging die nodig zijn voor de continuïteit van de bedrijfsvoering.
- Gebeurtenissen die tot onderbreking van bedrijfsprocessen kunnen leiden, worden geïdentificeerd, tezamen met de waarschijnlijkheid en de gevolgen van dergelijke onderbrekingen en hun gevolgen voor informatiebeveiliging (Business Impact Analyse).
- Er zijn plannen ontwikkeld en geïmplementeerd om de bedrijfsactiviteiten te handhaven of te herstellen of uit te wijken en om de beschikbaarheid van informatie op het vooraf afgesproken niveau en binnen in de vereiste tijdspanne te bewerkstelligen na onderbreking of uitval van kritische bedrijfsprocessen.
- Er wordt een enkelvoudig kader voor bedrijfscontinuïteitsplannen gehandhaafd om te bewerkstelligen dat alle plannen consistent zijn, om eisen voor informatiebeveiliging op consistente wijze te behandelen en om prioriteiten vast te stellen voor testen en onderhoud.
- Bedrijfscontinuïteitsplannen worden minimaal jaarlijks geoefend / getest en geactualiseerd, om te bewerkstelligen dat ze actueel en doeltreffend blijven.

15 Naleving

15.1 Naleving van wettelijke voorschriften

Doelstelling: Voorkomen van schending van enige strafrechtelijke of civielrechtelijke wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van beveiligingseisen.

15.1.1 Uitgangspunten

- Alle relevante wettelijke en regelgevende eisen en contractuele verplichtingen en de benadering van de organisatie in de naleving van deze eisen, zijn expliciet vastgesteld, gedocumenteerd en worden actueel gehouden voor elk informatiesysteem van de gemeente Groningen.
- Er zijn geschikte procedures geïmplementeerd om te bewerkstelligen dat wordt voldaan aan de wettelijke en regelgevende eisen en contractuele verplichtingen voor het gebruik van materiaal waarop intellectuele eigendomsrechten kunnen berusten en het gebruik van programmatuur waarop intellectuele eigendomsrechten berusten.
- Belangrijke registraties worden beschermd tegen verlies, vernietiging en vervalsing, overeenkomstig wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.
- De bescherming van informatie en privacy wordt bewerkstelligd overeenkomstig relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen.
- Gebruikers worden ervan weerhouden ICT-voorzieningen te gebruiken voor onbevoegde doeleinden.
- Cryptografische beheersmaatregelen worden overeenkomstig alle relevante overeenkomsten, wetten en voorschriften gebruikt.

15.2 Naleving van beveiligingsbeleid en -normen en technische naleving

Doelstelling: Bewerkstelligen dat systemen voldoen aan het informatiebeveiligingsbeleid en de informatiebeveiligingsnormen van de gemeente Groningen.

15.2.1 Uitgangspunten

- Managers bewerkstelligen dat alle beveiligingsprocedures die binnen hun verantwoordelijkheid vallen correct worden uitgevoerd om naleving te bereiken van informatiebeveiligingsbeleid en -normen.
- Informatiesystemen worden regelmatig gecontroleerd op naleving van implementatie van informatiebeveiligingsnormen.

15.3 Overwegingen bij audits van informatiesystemen

Doelstelling: Doeltreffendheid van audits van het informatiesysteem maximaliseren en verstoring als gevolg van systeemaudits minimaliseren.

15.3.1 Uitgangspunten

- Audits en andere activiteiten waarbij controles worden uitgevoerd op productiesystemen, worden zorgvuldig gepland en (de eisen voor) deze activiteiten worden vooraf goedgekeurd. Hiermee kan de kwaliteit van deze audits worden gewaarborgd en het risico van verstoring van bedrijfsprocessen tot een minimum worden beperkt.
- Toegang tot hulpmiddelen voor audits van informatiesystemen wordt beschermd om mogelijk misbruik of compromitteren te voorkomen.

Bijlage 1: Overzicht van gemeente Groningen met verbonden organisaties[40]

Dit overzicht geeft alle verbonden organisaties[41] van de gemeente Groningen weer die zich direct via het college van B&W van de gemeente Groningen hebben geconformeerd of indirect als gebruiker van de ICT-infrastructuur van de gemeente Groningen (beheerd door het SSC) dienen te conformeren aan de *keten*informatiebeveiligingsmaatregelen zoals verwoord in dit informatiebeveiligingsbeleid.

Gemeente
- Gemeente Groningen[42]

Gemeenschappelijke Regelingen (GR)
- Noordelijk Belastingkantoor (NBK)
- Regionale Inkooporganisatie Groninger Gemeenten (RIGG)
- Afval Regio Centraal Groningen (ARCG)

Andere rechtsvormen
- Stichting WIJ Groningen
- Sociale werkvoorziening / Werkvoorzieningsschap / Arbeidsontwikkelbedrijf Iederz

Bijlage 2: Bronnen

- VNG-resolutie, Vereniging van Nederlandse Gemeenten (VNG), v1.0, 31 oktober 2013.
- Strategische variant van de BIG, Informatiebeveiligingsdienst (VNG-IBD), v1.02, juli 2016.
- Tactische variant van de BIG, Informatiebeveiligingsdienst (VNG-IBD), v1.02, juni 2016.
- Diepgaande risicoanalysemethode gemeenten, VNG-IBD, versie 1.0, augustus 2014.
- Risicoanalyse gemeenten – Voorbeeldrapportage, VNG-IBD, versie 1.0, 2014.

Bijlage 3: Detailuitwerking voor het informatiebeveiligingsplan

Deze bijlage geeft in lijn met het vastgestelde beleid de nadere aanvulling en uitwerking van de *organisatie van informatiebeveiliging* (hoofdstuk 6) als eerste concretiseringslag voor het informatiebeveiligings*plan.*

B3.1 Interne organisatie

B3.1.1 Uitgangspunten

- De dagelijkse interactie tussen de diverse informatiebeveiligingsfuncties is geborgd in de reguliere bedrijfsvoering. In het geval van bijvoorbeeld een calamiteit is snellere reactietijd gewenst. Daarvoor wordt een communicatieplan (communicatielijnen met escalatieladder) opgesteld.
- De verantwoordelijkheden voor informatiebeveiliging zijn formeel belegd en zijn integraal ingebed in de reguliere planning- & controlcyclus binnen de (kwaliteitshandhaving van de) productie- en bedrijfsvoeringsprocessen.
- Ter borging van het onderwerp geeft iedere organisatie jaarlijks, binnen de reguliere planning- & controlcyclus, een interne "*in control"-verklaring* af over de werking van de organisatorische maatregelen aan de andere organisaties binnen de gemeente

[40] Het overzicht is gebaseerd op de lijst uit de jaarrekeningcontrole 2017 van de gemeente Groningen 2017 en de partijen die een *direct* contract hebben met het SSC van de gemeente Groningen. Een dergelijk contract zal ook gelden voor de GGD Groningen na de verzelfstandiging van de gemeente Groningen (beoogde startdatum 1 januari 2020).
[41] Gebaseerd op outsourcingsdocument Generieke ICT *GG_OGICT_223 Overzicht klanten v2.pdf* (Bron: SSC).
[42] Vanaf 1 januari 2019 vallen hier de huidige gemeenten Ten Boer en Haren ook onder.

Groningen. Het SSC doet dat voor de werking van de technische maatregelen die zij beheert.
- De gemeente Groningen borgt zowel intern met functiescheiding de onafhankelijke rol van uitvoerende informatiebeveiligingsfuncties binnen de organisatie en de decentrale controle en handhaving. Het centrale handhavingsorgaan is belegd bij een onafhankelijke controlefunctie belegd (team Auditing).
- De gemeente Groningen beschikt over een auditkalender voor de controlefuncties.
- Proceseigenaren zijn verantwoordelijk voor het inventariseren van de risico's (samen met de applicatie-/systeemeigenaren) die verbonden zijn aan het verlenen van toegang tot hun voorziening aan derden; zij zijn ook verantwoordelijk voor het treffen van de benodigde (aanvullende) informatiebeveiligingsmaatregelen.

B3.1.2 Verantwoordelijkheden

De volgende vier rollen zijn van belang bij de indeling van verantwoordelijkheden voor informatiebeveiliging die binnen de organisatie van de gemeente Groningen zijn belegd.

Beslissende rol
De dagelijkse besturen (college van B&W, directies, etc.) zijn als gegevenseigenaren op *bestuurlijk niveau* integraal verantwoordelijk voor de beveiliging van informatie binnen de informatieverwerkende processen binnen de eigen organisaties. Deze besturen:
- Besluiten om de beschikbare normenkaders voor informatiebeveiliging op basis van Nederlandse en Europese wet- en regelgeving te hanteren.
- Stellen individueel het informatiebeveiligingsbeleid formeel vast.
- Nemen jaarlijks kennis van de evaluatie van de stand van zaken met betrekking tot de informatiebeveiliging.
- Deze rol is effectief vormgegeven door de Informatiebeveiligingsraad, gevormd door tenminste de volgende functionarissen:
    - GMT-lid (voorzitter en vertegenwoordiger van de organisatie);
    - Directeur SSC-I&S;
    - Directeuren, één per domein als vertegenwoordiging van de lijnorganisatie;
    - CISO (secretaris);
    - Concerncontroller.
- Primaire taken van de Informatiebeveiligingsraad:
    - Bevorderen van het bewustzijn voor informatieveiligheid bij het management van de gemeente Groningen;
    - Bewaken van de informatiebeveiligingsrisico's;
    - Beheren informatiebeveiligings(jaar)*plan.* Het plan wordt periodiek geactualiseerd. Het opstellen en actualiseren van eventueel hiervan afgeleide, detailplannen blijft de verantwoordelijkheid van de individuele organisaties;
    - Adviseren van het GMT en overige managementlagen over informatiebeveiliging;
    - Rapporteren aan het GMT, onder andere over naleving van het informatiebeveiligingsbeleid, de voortgang van de implementatie van informatiebeveiligingsmaatregelen en over de uitkomsten van interne en externe audits.

Sturende rol
De directies zijn als proceseigenaren op *ambtelijk niveau* integraal verantwoordelijk voor informatiebeveiliging binnen iedere individuele organisatie en bepalen binnen de gegeven bestuurlijke kaders de koers van het ambtelijk apparaat.

De directies zijn in hun sturende rol verantwoordelijk voor het:
- Laten implementeren van het gegeven informatiebeveiligingsbeleid.
- Jaarlijks evalueren van het beleid en laten bijstellen van de onderliggende documentatie.
- Bevorderen van het beveiligingsbewustzijn bij medewerkers door het actief en aantoonbaar uitdragen van het informatiebeveiligingsbeleid.

- Beleggen formeel organisatorische afspraken in rollen met expliciete taken, bevoegdheden en verantwoordelijkheden (per organisatie is minimaal één decentrale informatiebeveiligingsfunctionaris benoemd en die kan worden afgevaardigd naar de Informatiebeveiligingsraad of dient als vertegenwoordiger en primair contactpersoon van de organisatie).
- Stellen op basis van een expliciete risicoanalyse de betrouwbaarheidseisen voor de informatiesystemen in hun processen vast (classificatie).
- Sturen op (keten)risico's.
- Controleren of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden.
- Goedkeuren van initiatieven om de informatiebeveiliging te verbeteren.

De Regieorganisatie geeft op dagelijkse basis namens de directies van de verbonden organisaties invulling aan de sturende rol door enerzijds de strategische besluitvorming voor de directies voor te bereiden (beleids- en planvorming) en toe te zien op de invoering en controle daarop ervan (toetsend). Het SSC heeft een voorbeeldfunctie op dit onderwerp.

Het Informatiebeveiligingsteam heeft de volgende verantwoordelijkheden:
  - Jaarlijkse evalueren van het informatiebeveiligings*beleid* en zorgen voor de driejaarlijkse vaststelling door het college van B&W en gemeenteraad.
  - Opstellen van het onderhavige informatiebeveiligings*plan* en er voor zorgdragen dat dit periodiek (minimaal jaarlijks of indien nodig eerder) wordt bijgesteld.
  - Inhoudelijke afstemming vanuit de gemeente Groningen en richting de directies van de verbonden organisaties (via de directies en/of via een door hen aangestelde decentrale informatiebeveiligingsfunctionaris). Eventuele escalaties verlopen via de Regieorganisatie naar de directies.
  - Coördineren van de inzet van (indien nodig extern) specialistisch advies op het gebied van informatiebeveiliging binnen geheel de gemeente Groningen.
- Conform de BIG heeft de gemeente Groningen een Chief Information Security Officer (CISO[43]) aangesteld. De CISO-rol binnen de Regieorganisatie omvat de volgende verantwoordelijkheden:
  - Bevorderen van informatiebeveiliging door direct (gevraagd en ongevraagd) te adviseren over de informatiebeveiliging van de verbonden organisaties van de gemeente Groningen.
  - Adviseren aan alle informatiebeveiligingsfuncties in de gemeente Groningen en verbonden organisaties. Het opstellen van een communicatieplan.
  - Als generalist op hoofdlijnen verbanden leggen tussen de individuele belangen van de verbonden organisaties en de beveiligingsbelangen van de gemeente Groningen als geheel. Het met elkaar verenigen van de eventueel tegengestelde belangen, mede op basis van adviezen van interne en externe deskundigen.
  - Direct en rechtstreeks rapporteren van relevante bevindingen op het gebied van informatiebeveiliging aan de hoogste ambtelijke niveaus.
  - Beheren van de auditkalender voor de controlefuncties in relatie tot informatiebeveiliging.
  - Controleren of de maatregelen met betrekking tot de informatiebeveiliging van de organisaties worden nageleefd.
  - Evalueren van de audituitkomsten en het doen van voorstellen tot implementatie c.q. aanpassing van de plannen op het gebied van de informatiebeveiliging van de verbonden organisaties.

[43] De BIG heeft gekozen voor *Chief Information Security Officer* als benaming voor deze rol, om enerzijds aan te sluiten bij de gangbare benaming van deze rol binnen andere grote gemeenten, het Rijk en het bedrijfsleven. Anderzijds om een duidelijk onderscheid te maken met de verschillende bestaande wettelijke rollen (die reeds een *deel*verantwoordelijkheid hebben op dit domein, zoals de BRP beveiligingsbeheerder, de Security Officer voor Suwinet en de Privacy Officer voor de gemeente Groningen binnen SSC) en met de *ISO*-normeringen in dit domein. Daarnaast benadrukt het de plaatsing/locatie van deze rol binnen de Regieorganisatie.

  - Periodiek rapporteren over de stand van zaken op het gebied van de informatiebeveiligingsmaatregelen aan de portefeuillehouders bedrijfsvoering (zowel ambtelijk als bestuurlijk).
  - Beheren van de template voor de "*in control*"-verklaringen en coördineren van de afstemmingen tussen de organisaties binnen de gemeente Groningen.
- Het uitgangspunt is hierbij dat het uitvoeren van de beheersingsmaatregelen zelf de verantwoordelijkheid blijft voor individuele organisaties.

Vertalende rol
De afdelingen binnen de organisaties zijn volledig verantwoordelijk voor de informatiebeveiliging van hun eigen organisatieonderdeel. De lijnmanagers:
- Zijn verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen.
- Sturen op beveiligingsbewustzijn, bedrijfscontinuïteit en de naleving van regels en richtlijnen (gedrag en risicobewustzijn).
- Sturen op de toegekende verantwoordelijkheden.
- Rapporteren over compliance binnen de eigen organisatie aan wet- en regelgeving en algemeen beleid van de organisatie in de managementrapportages.
- Leveren input aan de decentrale informatiebeveiligingsfunctionaris of rechtstreeks aan het informatiebeveiligingteam voor het actualiseren van het informatiebeveiligingsbeleid en -plan en vertalen van het beleid naar operationele informatiebeveiligingsmaatregelen en procedures binnen de eigen afdeling.
- Stemmen procedures onderling af tussen de verschillende proces- en applicatie-/systeemeigenaren. Dit verloopt via de decentrale informatiebeveiligingsfunctionarissen en eventuele escalaties verlopen via het informatiebeveiligingsteam en de directies naar het college B&W.

Uitvoerende rol
De verantwoordelijkheid voor het veilig werken met informatie ligt feitelijk bij alle individuele medewerkers binnen de gemeente Groningen, maar er zijn specifiek twee groepen die expliciet verantwoordelijk zijn voor de onderstaande zaken.

Allereerst is het Shared Service Centrum (SSC-I&S) als beheerorganisatie, in haar rol van applicatie-/systeemeigenaar, voor alles dat op de ICT-infrastructuur draait, specifiek verantwoordelijk voor:
- De dagelijkse centrale uitvoering van de gestelde (technische) informatiebeveiligingsmaatregelen.
- De technische beveiliging van de informatievoorziening en implementatie van de beveiligingsmaatregelen, die voortvloeien uit de betrouwbaarheidseisen (classificaties van de proces-, applicatie-/systeem- en gegevenseigenaren).
- Alle formeel uitbestede beheeraspecten van informatiebeveiliging, zoals technische ICT-beveiligingsmaatregelen, wijzigingsbeheer, incident- en probleembeheer, facilitaire en personele zaken.
- Logging[44], monitoring en aanlevering van audittrails en rapportages aan de diverse informatiebeveiligingsfunctionarissen binnen de gemeente Groningen.
- Het leveren van (technisch) beveiligingsadvies aan haar klanten.
- Het dagelijks coördineren van het beheer van technische informatiebeveiligingsaspecten (centraal bij ICT-beveiligingsfunctionaris belegd binnen het SSC).

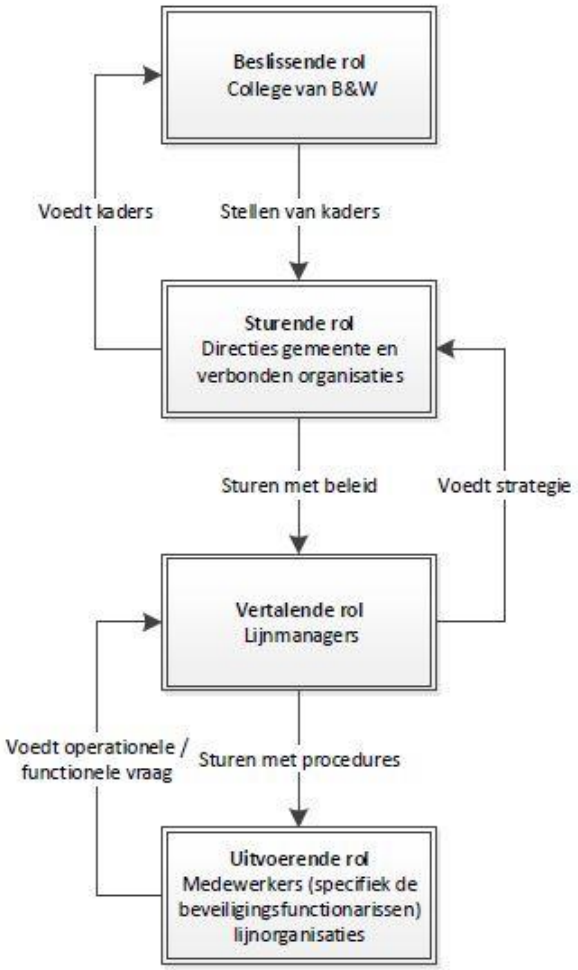
Als tweede is iedere directie (en diens decentrale informatiebeveiligingsfunctionaris) verantwoordelijk voor:
- Alle bovenstaande punten indien het niet centraal door het SSC beheerde applicaties betreft.

[44] Vastlegging van systeemhandelingen.

- Het dagelijkse toezicht op de decentrale invoering en de naleving van de alle organisatorische (en soms dus ook technische) beveiligingsmaatregelen en -procedures, zoals uitgewerkt in het informatiebeveiligingsbeleid en -plan.
- Het acteren als het lokale aanspreekpunt voor vragen en het melden van incidenten.
- Het periodiek rapporteren (minimaal eens per jaar) aan het hoogste ambtelijke en bestuurlijke organisatieniveau (directies en college van B&W).
- Het geven van voorlichting of instructies aan (nieuwe) medewerkers.
- Het vervullen van een lokale coördinerende rol.
- Het geven van gevraagd en ongevraagd advies ter verbetering van de informatieveiligheid aan de lokale organisatie.
- Het periodiek rapporteren aan de CISO over beveiligingsincidenten en de realisatie en effectiviteit van de beveiligingsmaatregelen en zaken of ontwikkelingen die bedreigend kunnen zijn voor de informatieveiligheid.

Alle medewerkers:
- Zijn verantwoordelijk voor de veiligheid van de activiteiten die behoren in de processen waarvan zij deel uit maken door hun eigen functie en taken.
- Betrachten zorgvuldigheid en discipline bij het omgaan met de informatie en (informatie)systemen die zij gebruiken.
- Zijn zich bewust van de eisen ten aanzien de beschikbaarheid, de integriteit en de vertrouwelijkheid van de informatieprocessen waarbij zij zijn betrokken.

Deze vier hoofdrollen worden samengevat weergegeven in figuur 3:



Figuur 3 – Verantwoordelijkheidsrelaties tussen informatiebeveiligingsrollen

B3.2 Externe partijen

B3.2.1 Uitgangspunten

- De opdrachtgever is als proceseigenaar altijd eindverantwoordelijk voor de kwaliteit en veiligheid van de uitbestede diensten. De opdrachtgever eist van de externe partijen dat zij voldoen aan alle aspecten van dit beleid, die voor de dienst of het betreffende systeem van belang zijn en betrekking hebben op de geleverde dienst.
- In (bewerkers)overeenkomsten dient gebruik te worden gemaakt van een '*third party*'-mededeling (TPM) of een ISAE3402-verklaring indien de opslag of verwerking van (privacygevoelige) gegevens niet op de infrastructuur van de gemeente Groningen plaatsvindt. De gemeente Groningen behoudt zich het recht voor om de informatiebeveiligingsaspecten van de processen buiten de gemeente Groningen infrastructuur periodiek te laten auditen.
- Externe partij(en) houden actief toezicht op de naleving van externe eisen (zoals de AVG) en interne eisen van de gemeente Groningen, zodat de gemeente Groningen compliant blijven. Bijvoorbeeld op de regels omtrent grensoverschrijdend dataverkeer en de melding bij de Autoriteit Persoonsgegevens (AP) in het geval van doorgifte van persoonsgegevens naar landen buiten de Europese Unie.
- Voor de externe partijen zelf geldt daarbij ook het '*comply or explain'*-beginsel (pas toe of leg uit) indien (nog) niet wordt / niet kan worden voldaan aan het informatiebeveiligingsbeleid van de gemeente Groningen.