

Instructiedocument voor het uitwerken en vaststellen van het strategisch kader voor integraal beveiligingsbeleid voor gemeenten (visie, beveiligingsdoelen, uitgangspunten en kwaliteitsborging)

Versiebeheer

Versie	Datum	Gewijzigd door	Omschrijving
0.2	28-01-2021	COT	Eerste conceptversie - vertrouwelijk

Inhoudsopgave

1	Inleiding.....	2
1.1	Waarom integraal beveiligingsbeleid gemeenten?	2
1.2	Positie van dit document in het project Integrale Beveiliging Gemeenten.....	2
1.3	Definities en toelichting	3
1.4	Leeswijzer	4
2	Hoe stel je als gemeente een strategisch kader op voor integrale beveiliging?	6
2.1	Stap 1: Opstellen van een visie op integrale beveiliging	6
2.2	Stap 2: Bepaal de scope voor integrale beveiliging	7
2.3	Stap 3: Stel beveiligingsdoelen op	8
2.4	Stap 4: Stel uitgangspunten op voor integrale beveiliging.....	9
2.5	Stap 5: Stel een kwaliteitssysteem op voor Plan-Do-Check-Act	11
	Bijlage I: Wettelijk kader en normen	12

1 Inleiding

Het project Integrale Beveiliging van het ministerie van BZK heeft verschillende doelgroepen. Niet elke gemeente is hetzelfde ofwel heeft dezelfde startsituatie voor integrale beveiliging. Zo kunnen bezoekers van het platform Integrale Beveiliging precies weten wat ze zoeken of nog zoekende zijn. Of het volledige programma integrale beveiliging willen vormgeven of juist een onderdeel te versterken. Om hieraan tegemoet te komen zijn de stukken zo vormgegeven dat – afhankelijk van de vraag of behoefte – er gebruik is te maken van de diverse onderdelen. Het platform integrale beveiliging is op dezelfde wijze ingericht.

1.1 Waarom integraal beveiligingsbeleid gemeenten?

Gemeenten zijn vanwege hun bestaansgrond een gedeeltelijk open instelling. Een open instelling betekent een voor publiek deels toegankelijke gebouwen met een dienstverlenende functie. En veelal publieke toegankelijke informatie, publieksoptreden van en herleidbare informatie naar personen. Mede door deze openheid staat een gemeente ook dagelijks bloot aan verschillende soorten 'bedreigingen'. In onze maatschappij zijn tal van bedreigingen. Ondermijning van lokaal bestuur schaadt het vertrouwen in de overheid en veilig werken is een basisvoorwaarde voor het goed functioneren van het openbaar bestuur. Politieke ambtsdragers en gemeenteambtenaren moeten hun publieke taak kunnen uitvoeren in een veilige werkomgeving, vrij van ongewenste beïnvloeding of bedreiging. Hierdoor is er een noodzaak voor beveiligen van gemeentelijke gebouwen, terreinen, personen, data, ICT-systemen en eigendommen.

Gemeenten zetten maatregelen in om risico's tot een aanvaardbaar niveau te reduceren. Om de maatregelen in samenhang te kunnen treffen is overkoepelend beleid noodzakelijk. Integraal beveiligingsbeleid vormt derhalve de kapstok (te hanteren uitgangspunten, beveiligingsdoelen) voor de opzet en organisatie van de beveiliging binnen een gemeente.¹

1.2 Positie van dit document in het project Integrale Beveiliging Gemeenten

Het doel van het project Integrale Beveiliging Gemeenten van het ministerie van BZK is om gemeenten te ondersteunen in hun ambitie om weerbaar te zijn tegen moedwillige risico's die schade kunnen veroorzaken aan de gemeentelijke organisatie. Op de website (XXX) zijn alle bouwstenen opgenomen voor de inhoudelijke uitwerking en organisatorische inbedding van integrale beveiliging. Dit document is de uitwerking van 1 van de bouwstenen.



Figuur 1: thema's integrale beveiliging

¹ Deze aanpak vindt haar oorsprong in een weerbare overheid en bestuur. Hiervoor is een netwerk opgericht, Het Netwerk Weerbaar Bestuur, wat zich inspant voor een weerbaar bestuur waarin (politieke) ambtsdragers hun ambt veilig en integer uit kunnen oefenen. <https://www.weerbaarbestuur.nl/producten-en-diensten/aanpak-integrale-beveiliging>

Let wel: integrale beveiliging is bedoeld als kapstok voor de beveiligingsplannen. De deelplannen worden niet (opnieuw) ontwikkeld, maar worden via integrale beveiliging aan elkaar gekoppeld. Hierbij is er een duidelijke link met continuïteitsmanagement omdat continuïteitsplanvorming de herstelmaatregelen bevatten voor het continueren van de gemeentelijke dienstverlening.

1.3 Definities en toelichting

De volgende definities zijn te hanteren in de gemeente. Let wel: er worden diverse voorbeelden genoemd.

Definitie	Toelichting
Integrale beveiliging	Het Beveiligingsvoorschrift Rijksdienst definieert integrale beveiliging als volgt: het selecteren, implementeren en periodiek evalueren van een samenhangend stelsel van beveiligingsmaatregelen van de organisatie, medewerkers, materieel, informatiesystemen, gebouwen en overige objecten op basis van risicomanagement. Het betreft maatregelen tegen elke inbreuk die de doelstellingen van de organisatie kan bedreigen. (Beveiligingsvoorschrift Rijksdienst, artikel 1). Een voorbeeld definitie is ook: De wijze waarop binnen de gemeentelijke organisatie op proces en inhoud wordt samengewerkt met als doel de weerbaarheid van de organisatie te verhogen en weerbaar te zijn tegen moedwillige verstoringen of overtredingen die een mogelijke impact/negatieve invloed hebben op de personen, middelen en gebouwen waardoor de maatschappelijke functie die de gemeentelijke organisatie heeft bedreigd wordt. <i>Let wel:</i> in de benaderingen is onderscheid te maken tussen de 'organisatorische integraliteit' en de 'inhoudelijke integraliteit'. De organisatorische integraliteit krijgt vorm in proces, werkwijze en afstemming. De inhoudelijke integraliteit is de samenhang in inhoudelijke besluiten en thema's.
Beveiligingsthema's	Onder integrale beveiliging vallen de volgende inhoudelijke thema's: informatiebeveiliging, fysieke/technische beveiliging en personele beveiliging. Integrale beveiliging gaat daarmee niet over de inhoud van deze thema's, maar brengt de proces/inhoud samen in een gezamenlijke aanpak. De integraliteit zorgt voor gezamenlijke belangen en besluiten vanuit een gedeelde verantwoordelijkheid. • <i>Informatiebeveiliging</i> - Het proces van vaststellen van de vereiste kwaliteit van informatie(systemen) in termen van vertrouwelijkheid, beschikbaarheid, integriteit, onweerlegbaarheid en controleerbaarheid alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende (fysieke, organisatorische en logische) beveiligingsmaatregelen. Bron; IBD-VNG • <i>Fysieke/technische beveiliging</i> - de organisatorische, bouwkundige en elektronische maatregelen/barrières die nodig zijn om informatie en personen te beveiligen tegen ongewenste of ongeoorloofde handelingen. • <i>Personele beveiliging</i> - de maatregelen die nodig zijn om personen veilig en zonder afbreuk van kwaliteit hun werkzaamheden te kunnen uitvoeren, zonder/zo min mogelijk afbreuk te doen aan de integriteit van de personen. Belangrijk hierbij is dat alle beveiligingsthema's bij elkaar opgeteld het stelsel van beveiligingsmaatregelen bevat. Dit houdt in dat de verschillende aandachtsgebieden niet volledig los maar soms in onderlinge relatie met elkaar staan. Het stelsel van maatregelen heeft hierbij tot doel een blijvend niveau van beveiliging te realiseren op de verschillende niveaus in de gemeente.

Beveiligingsrisico's	Beveiligingsrisico's zijn risico's die het gevolg zijn van doelbewust kwaadwillig menselijk handelen met schade voor de gemeentelijke organisatie. Het voorkomen van beveiligingsrisico's wordt 'beveiliging' genoemd. Het draait daarmee om het voorkomen dat onbevoegden gebruik maken middelen/informatie. Hoe voorkom je dit. Een risicomanagement benadering. Op het moment dat het zich alsnog voordoet zijn er maatregelen (repressief) om de impact te reduceren of de oorzaak weg te nemen. De respons op een incident/crisis. Denk aan continuïteits- of crisismanagement.
Niet moedwillige risico's	Waar het bij beveiligingsrisico's gaat om moedwillig/doelbewust, gaat het bij niet moedwillige risico's om natuurrampen, technische storingen, stroomuitval, brand, griepvirus, et cetera.
Beveiligingsproces	Een continu proces voor het beheersbaar maken en houden van integrale beveiliging. De volgende aspecten zijn van belang om de integraliteit te kunnen waarborgen (vanuit de procesbenadering): • visie en beleid integrale beveiliging (voorliggend document), • governance(structuur) • kwaliteitsborging (inclusief PDCA-cyclus) • preparatie middels bijv. trainen, testen en oefenen • awareness/draagvlak
Beveiligingsmaatregelen	Set van maatregelen tegen elke inbreuk die de doelstellingen van de gemeentelijke organisatie kan bedreigen. De beveiligingsmaatregelen van de gemeente stellen de gemeente in staat om door barrières kwaadwillende het fysiek onmogelijk te maken hun daden te verrichten, hen duidelijk te maken dat de beveiliging goed op orde is én om tijdig en adequaat te reageren.
Bedrijfsmiddelen	Integrale beveiliging is bedoeld als basis voor de bescherming van alle bedrijfsmiddelen die zijn geïdentificeerd (middels een risicoanalyse) als noodzakelijk om te beveiligen. Daarbij gaat het om (voorbeelden van) bedrijfsmiddelen, zoals de mensen, gebouwen, terreinen, locaties, maar ook om computers, instrumenten, installaties en informatie in fysieke vorm.

1.4 Leeswijzer

Dit document is bedoeld om u een indruk te geven van hoe u als gemeente integraal beveiligingsbeleid kunt opstellen. De invulling van dit format vereist dat u en anderen binnen uw organisatie een aantal noodzakelijke denkstappen zetten. Het algemene format moet op basis van specifieke keuzes, kenmerken en behoeften worden ingevuld en aangepast (organisatie specifiek). Doordat gemeenten verschillen op onder meer grote, situatie, context, en organisatiestructuur is er niet 1 beveiligingsbeleid voor alle gemeenten. Het document wat voorligt dient dan ook op maat te worden gemaakt, passend bij de eigen gemeente en situatie. Per onderdeel wordt in een korte instructie aangegeven op welke wijze keuzes zijn te maken.

Bij het schrijven zijn enkele uitgangspunten gehanteerd, namelijk:

1. Het gaat om integrale beveiliging, niet over integrale veiligheid. In de kern gaat integrale veiligheid over de zorg voor openbare orde en veiligheid. De verantwoordelijkheid voor het veiligheidsbeleid op lokaal niveau ligt bij de gemeente. Gemeenten hebben regie op het veiligheidsbeleid. Dat houdt in dat gemeenten sturen op de prioritering van veiligheidsthema's en op de samenwerking met en tussen partijen. Integrale veiligheid richt zich dus op de maatschappij en in mindere mate op de eigen organisatie. Integrale beveiliging richt zich op de gemeentelijke organisatie, om zo haar rol in de maatschappij – en daarmee integrale veiligheid – te kunnen blijven uitvoeren. Het versterkt daarmee de aanpak van integrale veiligheid indirect.
2. De scope van integrale beveiliging en van dit document richt zich op de weerbaarheid van de gemeentelijke organisatie. Het overstijgt en verbindt hiermee de onderliggende – inhoudelijke – thema's.

3. Op het platform van Integrale beveiliging staan diverse voorbeelden uit het werkveld, gemeenten etc. Ook worden per thema's tips gedeeld. Het is aan de gemeenten zelf om te bepalen wat het beste aansluit op de eigen organisatie.
4. We leggen met dit stuk geen norm neer voor integrale beveiliging. Het zijn bouwstenen voor de eigen organisatie.
5. De bouwstenen vergen een verdere uitwerking in de gemeente. Elke gemeente heeft een eigen context.
6. Dit document is opgesteld voor een brede doelgroep binnen de gemeentelijke organisatie. De focus ligt bij beleid/bestuursadviseur en projectleider/coördinator. Om zo de integraliteit te bevorderen en te zorgen voor aansluiting van de diverse disciplines. De expert op een (deel)thema zal de verdieping in een deelthema kunnen vinden.
7. We gaan uit van vakvolwassen adviseurs/betrokken. We beschrijven het proces, maar gaan uit van betrokken en ervaren ambtenaren. Het wordt hiermee niet een uitgeschreven training 'beveiligingsbeleid maken'. Het wordt wel een handleiding hoe de integraliteit te versterken in de organisatie met een basis in een integraal beveiligingsbeleid.
8. We nemen in dit document diverse voorbeelden op. Hierin verwijzen we zoveel mogelijk naar de digitale bron om zo – bij mogelijke updates – te kunnen blijven vernieuwen.
9. Het voorgestelde beleid voldoet aan de relevante wet- en regelgeving en van toepassing zijnde kaders.

2 Hoe stel je als gemeente een strategisch kader op voor integrale beveiliging?

Om een goed beveiligde gemeentelijke organisatie te zijn is een kader nodig met duidelijke beveiligingsdoelstellingen en uitgangspunten. Het doel van integrale beveiligingsbeleid is om vanuit 1 kader beveiligingsmaatregelen in samenhang te treffen. De beveiligingsmaatregelen stellen de gemeente in staat om door barrières kwaadwillende het fysiek/digitaal onmogelijk te maken hun daden te verrichten, hen duidelijk te maken dat de beveiliging goed op orde is én om tijdig en adequaat te reageren. En daarmee vertrouwen uit te stralen naar gemeentefunctionarissen en inwoners. De ambitie voor integrale beveiliging vraagt om een organisatiestructuur en kwaliteitssysteem dat daarbij past.

Het kader voor integrale beveiliging bestaat uit de volgende stappen:



Figuur 2: stappen vormgeven strategisch kader

Deze bovengenoemde stappen worden in dit document verder toegelicht en voorzien van voorbeelden. Hierbij staan we per stap stil bij de hoofdactiviteiten, de 'wat' en 'hoe'. De 'wie' en 'waarom' en op 'welke wijze' krijgen vorm door de gemeente zelf. Waar mogelijk worden suggesties gedaan, voorbeelden gegeven of naar verwezen.

2.1 Stap 1: Opstellen van een visie op integrale beveiliging

Toelichting	Gemeenten hebben een lokale maatschappelijke verantwoordelijkheid voor hun inwoners. Gemeenten hebben hun eigen bestuurlijke en ambtelijke organisatie, systemen, gebouwen etc. om daar uitvoer aan te geven. Om te voorkomen dat de uitvoer opzettelijk wordt bedreigd/ondermijnd/verstoord is beveiliging nodig. Om de beveiliging goed vorm te geven is integrale voorbereiding, planvorming en uitvoering nodig. Integrale beveiliging is een middel om hiertoe te komen en een veerkrachtige en weerbare organisatie te worden. Daarbij dient er een balans te zijn in het omgaan met deze risico's, de maatregelen en een proportionele calamiteitenorganisatie.
Waarom een visie op integrale beveiliging?	Een integrale visie op beveiliging geeft de gemeente richting, het brengt focus aan en bindt medewerkers en de doelgroepen van de gemeente. Een visie is het beeld of de verwachting die een gemeente heeft van integrale beveiliging. Het is een gezamenlijk beeld, gedeeld door alle betrokkenen, dat een verwachting geeft van de voor de gemeente integrale beveiliging. Een visie wordt kort en krachtig beschreven.
Voorbeelden van een visie op integrale beveiliging	Voorbeeld 1 <i>De gemeente versterkt de weerbaarheid van haar organisatie zodat zij weerbaar is tegen moedwillige verstoringen of overtredingen die een mogelijke impact/negatieve invloed hebben op de personen, middelen en gebouwen waardoor de maatschappelijke functie die de gemeentelijke organisatie heeft bedreigd wordt. Hierdoor kunnen medewerkers en bezoekers veilig werken en gebruik maken van de gemeentelijke dienstverlening. Dit gaat niet ten koste van de gemeenschapswaarde van de gemeente.</i> Voorbeeld 2 <i>De gemeente wil haar maatschappelijke functie zo goed mogelijk uitoefenen. Hierom investeert ze in de weerbaarheid van haar personeel, gebouwen en middelen en versterkt dit door in gezamenlijkheid zorg te dragen voor de kwaliteitsborging op de (deel)thema's van beveiliging.</i> Voorbeeld 3

	<i>Door integrale beveiliging vorm te geven zorgen wij voor kruisbestuiving en een gezamenlijke aanpak op de diverse beveiligingsthema's met als doel een veilige werkomgeving te realiseren.</i> Voorbeeld 4 <i>Zorgdragen voor uniformiteit en duidelijkheid in de doelen en gezamenlijke aanpak. Om zo ook verschil in aanpak en maatregelen te voorkomen.</i> Voorbeeld 5 <i>Met het integraal beveiligingsbeleid en aanpak worden preventieve, repressieve en herstellende maatregelen samengebracht.</i>
Welke hoofdactiviteiten zijn nodig om een visie op te stellen?	• Stel vast wie de visie kan vaststellen en hoe dit proces verloopt. • Bepaal wie de opstellers zijn van de visie. • Betrek de benodigde betrokkenen inclusief deelonderwerpen. Let op ambtelijke, bestuurlijke en politieke betrokkenheid. • Betrek eventueel de meerjaren plannen/visie/beleid van de gemeente. • Betrek eventueel de bestaande plannen/visies van de deelonderwerpen. • Kom in een werksessie tot een gezamenlijk beeld van de context van de gemeentelijke organisatie en wat jullie gezamenlijk willen bereiken. Bepaal hierbij een minimale en maximale variant. • Formuleer een visie die recht doet aan bovenstaande stappen en beargumenteer waarom. • Laat het de visie bestuurlijk vaststellen.

2.2 Stap 2: Bepaal de scope voor integrale beveiliging

Toelichting scope	Het beveiligingsbeleid richt zich op de gehele gemeentelijke organisatie. Het is hiermee van toepassing op organisatie, medewerkers, materieel, informatiesystemen, gebouwen en overige objecten. <i>Zie ook de definities.</i> De scope dient ook te worden bepaald door relevante wet- en regelgeving. De scope zorgt voor een duidelijke afbakening van integrale beveiliging voor de gemeente.
Onderdelen van scope integrale beveiliging	Bedrijfsmiddelen (materieel) Het beleid is bedoeld als basis voor de bescherming van alle bedrijfsmiddelen die zijn geïdentificeerd (middels een risicoanalyse) als noodzakelijk om te beveiligen. Daarbij gaat het om bedrijfsmiddelen, zoals de terreinen, de gebouwen en locaties, maar ook om computers, instrumenten, installaties en informatie in digitale en fysieke vorm. Medewerkers en derden Medewerkers, gasten en vrijwilligers van de gemeente, dienen zich te houden aan de in dit beleid vastgelegde richtlijnen. Zij worden er ook door beschermd. Leveranciers, ingehuurd personeel, communicatiepartners, schoonmaakdiensten en vergelijkbare partijen worden op de hoogte gesteld van de in dit beleid verwoorde uitgangspunten en afgeleide maatregelen en voorschriften. Wet- en regelgeving Gemeenten voldoen ten minste aan alle van toepassing zijnde wet- en regelgeving waarin eisen ten aanzien van beveiliging zijn opgenomen. De lijst van wetten en normen is opgenomen in bijlage I.
Voorbeelden van scope onderliggende deelplannen	Informatiebeveiliging Het beleid voor informatiebeveiliging is van toepassing op de hele organisatie: • Alle informatieverwerking die plaatsvindt binnen en namens de gemeente • Alle diensten die worden geleverd en de diensten die worden ingekocht • De eigen medewerkers, tijdelijk personeel en op personeel dat door derden wordt ingezet om diensten te verlenen aan of namens onze organisatie. • De middelen die hierbij worden ingezet. Fysieke beveiliging Fysieke beveiliging is van toepassing op: • Beveiliging barrières van de omgeving (toegang tot gebouw of delen van gebouwen)

	- Fysieke toegangsbeveiliging in gemeentelijke gebouwen (identificatie, registratie van bezoekers, afhalen bij receptie, lijst deelnemers bijeenkomsten et cetera) - Beveiliging van kantoren, ruimten en faciliteiten (barrières in ruimtes die niet toegankelijk zijn voor niet-geautoriseerde functionarissen en/of publiek) Personele veiligheid/beveiliging Het beleid voor personele beveiliging is van toepassing op de hele organisatie: - Een veilige werkomgeving voor de medewerkers; ambtelijk, bestuurlijk, politiek. - Een veilige werkcultuur - Een goede opvolging bij melding/incidenten. Continuïteit Gemeentelijke continuïteit is van toepassing op: - Alle herstelactiviteiten/maatregelen wanneer kritische processen uitvallen en daarmee ongewenste impact op de continuïteit van de gemeentelijke organisatie/dienstverlening.
Hoe stel je de scope vast?	- De definitie van integrale beveiliging is hierin leidend. En specifiek; 'Het betreft maatregelen tegen elke inbreuk die de doelstellingen van de organisatie kan bedreigen.' Bepaal of achterhaal de gemeentelijke doelstelling, <i>ofwel de gemeentelijke missie</i>. Dus: wat streeft de gemeentelijke organisatie minimaal na (bestaansrecht en wettelijke verplichtingen)? - Een manier om dit inzichtelijk te maken is gebruik te maken van de scope uit de diverse deelplannen (informatiebeveiliging, fysieke beveiliging, technische beveiliging, personele veiligheid). - Bepaal aan de hand van de scope van de onderliggende deelplannen de gemeentelijke scope, inclusief relevante wettelijke vereisten. - Stel je scope vast en leg het vast in het strategisch kader integrale beveiliging. Let wel: indien de gemeente geen deelplannen heeft, gaat dit andersom; je bepaalt de integrale beveiligingsscope met daarbij de duiding van de deelonderwerpen. Indien er niets op papier staat is het mogelijk om daarna de maatregelen te inventariseren en samen te brengen voor inzicht in de bestaande beveiligingsmaatregelen.

2.3 Stap 3: Stel beveiligingsdoelen op

Toelichting	Beveiligingsdoelen zijn expliciete doelen die een gewenst effect beschrijven als gevolg van de beveiligingsmaatregelen. Voorwaarde voor het vaststellen van de integrale beveiligingsmaatregelen is dat zij dienen bij te dragen aan integrale beveiligingsdoelen van de gemeente en de andere organisatiebelangen niet in de weg staan. Om zo een veerkrachtige en weerbare organisatie te worden en om de rol als lokale overheid, binnen de regio/context van de maatschappelijke doelen vorm te geven.
Voorbeelden van beveiligingsdoelen	- Het beschermen van de werknemers en bezoekers, zodat zij op een zo veilige mogelijke wijze hun werk kunnen doen, dan wel gebruik kunnen maken van de dienstverlening van de gemeente. - Ontmoedigen van kwaadwillende. - De kwaadwillende moet het gevoel hebben dat de beveiliging bij de gemeente goed op orde is. Hierbij kan de kwaadwillige zowel een intern als extern persoon zijn. - Voorkomen onbevoegde toegang tot gevoelige informatie - Voorkomen dat persoons- en bedrijfsgevoelige informatie in het publieke domein terecht komt (bijvoorbeeld op het internet). - Tegenhouden - De kwaadwillende wordt het fysiek onmogelijk gemaakt zijn daad te verrichten. - Afschermen - Afschermen van attractieve en kwetsbare onderdelen om kennisname en verkenningssacties door kwaadwillende te bemoeilijken. - Detectie.

	a. Indien al het voorgaande de kwaadwillende niet heeft afgeschrikt of tegengehouden, is het zaak zijn inbreuk zo vroeg mogelijk te detecteren. • Vertragen a. Het opwerpen van barrières tussen de kwaadwillende en zijn doel. Dit kan zowel het binnendringen als het kunnen vluchten betreffen. • Interventie a. De kwaadwillende wordt tijdig door de beveiliging tegengehouden of afgeschrikt. Overdracht aan de politie behoort tot de mogelijkheden. • Continuïteit. a. Door de integrale beveiliging juist vorm te geven wordt de continuïteit van de gemeentelijke dienstverlening zo goed mogelijk geborgd. Indien er toch sprake is van dreigend en of een beveiligingsrisico zich voordoet dan dient dit aansluiting te hebben op de continuïteitsaanpak binnen de gemeente en de incident/crisisorganisatie.
Hoe stel je beveiligingsdoelen vast?	1. Bepaal aan de hand van de bovengenoemde beveiligingsdoelen welke relevant zijn voor de gemeente 2. Leg de beveiligingsdoelen vast in het strategisch kader integrale beveiliging

2.4 Stap 4: Stel uitgangspunten op voor integrale beveiliging

Toelichting	Om de beveiligingsdoelen te behalen dienen ook uitgangspunten te worden vastgesteld. Uitgangspunten zijn randvoorwaarden of keuzes die leidend zijn voor gewenste effecten (beveiligingsdoelen). Net als doelstellingen kunnen uitgangspunten ook gebruikt worden om de beveiligingsmaatregelen te toetsen. Een uitgangspunt is gekoppeld aan een specifieke doelstelling en kan ook gelden als uitgangspunt voor meerdere/alle doelstellingen.
Voorbeelden van uitgangspunten	Beleid • De gemeente heeft een beveiligingsbeleid en dat beleid wordt regelmatig geactualiseerd. Dit beleid is in lijn met het algemene beleid van de gemeente. • De gemeente zorgt dat beveiliging zoveel als mogelijk past in het openbare, toegankelijke en gastvrije karakter van de gemeente (visie/beleid gemeente). • De portefeuillehouder, het college en de gemeenteraad zijn nauw betrokken bij de beleidsontwikkelingen en deze zijn vastgelegd in beleid, en het collegeprogramma. Het beveiligingsbeleid is opgesteld en vastgesteld onder verantwoordelijkheid van het college van burgemeesters en wethouders. • Besluitvorming in de thema's kan daarmee niet los worden gezien van de gezamenlijke kaders/besluitvorming voor integrale beveiliging. • Het beveiligingsbeleid wordt integraal vormgegeven. Hiertoe worden de dwarsverbanden bewaakt tussen de thema's en vinden er combinaties plaats van preventieve, repressieve en herstellende maatregelen. Om zo de samenhang te stimuleren. • Er is voldoende financieel draagvlak en speling voor het in standhouden van integrale beveiliging binnen de gemeente, inclusief benodigde capaciteit, aanpak, preparatie en incidentenrespons. Dit betekent een jaarlijks budget/begroting inclusief voorzieningen, eenmalig en terugkerend. • Scope: De gemeente heeft een gedegen en actueel inzicht in de specifieke en toekomstige beveiligingsrisico's van de organisatie, locaties en eventueel personen. • Uitgangspunt bij dit alles is dat het gaat om een risicogerichte aanpak, niet een regelgerichte aanpak. • Scope: De risicoanalyse en bijbehorende maatregelen zijn proportioneel naar het profiel van de gemeente. Waar nodig worden risico's geaccepteerd, verwijderd of geaccepteerd. Ook is het mogelijk om zich op onderdelen te verzekeren. Uitgangspunten voor kwaliteitsborging • De gemeente zorgt dat het voor beveiliging voldoet aan relevante wet- en regelgeving zowel Europees als Nederlands als branche gerelateerd.

- De gemeente werkt via de Plan-Do-Check-Act cyclus en draagt zorg voor borging in de control cyclus. Dit geldt zowel voor de implementatie van integrale beveiliging (project/programma, meerjarenplan) als het uitvoeren van het beleid (on going concern).
- Risico's die zich nog niet hebben voorgedaan, maar waarvan wordt ingeschat dat deze zich kunnen voordoen worden verwerkt in bondige scenario's voor inzicht en mogelijk sturing in maatregelen mocht het risico zich alsnog voordoen.

Uitgangspunten voor governance(structuur)

- De gemeente streeft naar een goede samenwerking met de ketenpartners inclusief duidelijke afspraken over de taakverdeling en grenzen aan de inzet van de beveiligingsdienst.
- Gemeenten werken samen met benodigde partners en dragen zorg voor de benodigde afstemming.
- Ook geldt dat verantwoordelijkheid en aansturing zoveel mogelijk plaats vindt vanuit de lijnorganisatie en lijnverantwoordelijkheden.
- De gemeente verwacht van de beveiligingsdienst scherpheid en alertheid en daadkracht om te handelen bij ongewenste situaties of ambigue signalen.
- Indien risico's zich voordoen dan staat hier een responsorganisatie tegenover die aansluiting heeft op BHV, crisisorganisatie, etc. er wordt kundig geacteerd door deze responsorganisatie waarbij de negatieve impact zo goed mogelijk wordt teruggebracht naar de bestaande organisatie.

Uitgangspunten preparatie

- De gemeente werkt met een meer jaren trainen-, oefen- en testenbeleid.
- Planvorming is gevat in planvorming, waarin ook inhoudelijke thema's in planvorming en praktijk gelinkt worden aan integrale beveiliging.
- Werknemers hebben jaarlijks een betrokkenheid bij het thema integrale beveiliging middels een sessie, incidentenevaluatie, training, e-learning, etc.
- Jaarlijks update de gemeente de plannen en zorgen voor balans in integrale beveiliging.
- Maatregelen mogen elkaar niet overlappen, elkaar vooral niet tegenwerken en onderlinge prioriteiten moeten worden afgestemd. Beveiligingsmaatregelen als gevolg van de integrale benadering moeten op de werkvloer als logisch en vanzelfsprekend worden ervaren.
- De gemeente houdt bij de beveiligingsmaatregelen zoveel mogelijk rekening met de impact van de maatregelen en eventuele ongewenste bijeffecten voor bezoekers en medewerkers.
- De gemeente zal zich ten aanzien van het treffen van de vereiste beveiligingsmaatregelen en voorzieningen bij voortdurend laten leiden door datgene dat op dit terrein qua ontwikkeling gebruikelijk en noodzakelijk is.

Uitgangspunten voor draagvlak en awareness (en cultuur)

- Het betrekken van de directies en besturen in de integrale 'allesomvattende' aanpak is van essentieel belang aangezien zij in alle gevallen een voorbeeldfunctie hebben en de integrale aanpak als eindverantwoordelijke voor moeten staan.
- De gemeente toont management commitment richting beveiliging en het breed kenbaar maken ervan. Hiermee wordt een duidelijk signaal afgegeven aan iedereen dat beveiliging belangrijk is en dat eenieder (die het aangaat) een eigen verantwoordelijkheid heeft in deze.
- De gemeente heeft een systeem en een attitude op alle niveaus van de organisatie om proactief en reactief risico's en dreigingen op het gebied van beveiliging te herkennen en er opvolging aan te geven. Dit beperkt zich niet tot het kiezen en gebruiken van een methode of kader maar veel meer tot een cultureel aspect van "risico denken en –handelen".
- De gemeente verwacht van alle medewerkers dat zij positief bijdragen (naleven beveiligingsmaatregelen en gedrag) aan een veilige werk- en zorgomgeving. Er is een positieve en proactieve beveiligingscultuur onder alle medewerkers.
- De gemeente zorgt voor goede communicatie van de uitgangspunten en voorschriften naar het personeel.
- Door heldere communicatie, transparantie over beleid, incidenten en respons geven wij inzicht in de werkwijze van integrale beveiliging en zorgen wij voor een gezamenlijk doelstelling binnen de organisatie.

	• Door communicatie over de aanpak, beleid en bijbehorende trainingen/sessies/... zorgen wij voor draagvlak en herkenbaarheid. Dit start bij nieuwe medewerkers en werkt door bij alle collega's. • Door communicatie uitingen, cultuur, sfeer worden ook aan bezoekers en buitenstaanders duidelijk wat het beleid/uitgangspunt is voor de gemeente. Uitgangspunten voor borging en lerend vermogen • De gemeente zorgt voor een duidelijke toewijzing en delegatie van taken, verantwoordelijkheden en bevoegdheden ten aanzien van de beveiligingsmaatregelen en voorzieningen. • Incidenten worden geregistreerd en op gerefleeteerd. Waar mogelijk worden de inzichten op jaarbasis verrat tot rode draden en is dit input voor de lerende organisatie (planvorming, response en organisatie). • De gemeente verwacht dat tijdig geleerd wordt van beveiligingsincidenten en oefeningen en dat daar waar nodig beveiligingsmaatregelen worden aangepast c.q. aangevuld. • Door als organisatie te leren en te blijven ontwikkelen zorgen wij voor een lerende organisatie. Interventies als trainingen, oefeningen, testen, scenario's uitwerken etc. dragen hieraan bij.
Hoe kom je tot een selectie van uitgangspunten?	1. Stel met de vorige drie stappen de uitgangspunten vast. 2. Leg de uitgangspunten vast in het strategisch kader integrale beveiliging

2.5 Stap 5: Stel een kwaliteitssysteem op voor Plan-Do-Check-Act

Toelichting	Een kwaliteitssysteem geeft het principe weer van continue verbetering en wordt gevormd door de facetten Plan-Do-Check-Act. Elke stap heeft een eigen karakter en logica. En ze komen logischerwijze ook voor in deze vaste volgorde. • PLAN: plannen van activiteiten en stellen van doelen; • DO: voer het plan uit, neem kleine stappen in gecontroleerde omstandigheden; • CHECK: controleer en analyseer de resultaten; • ACT: neem actie om te standaardiseren of het proces te verbeteren.
Hoe stel je een kwaliteitssysteem op voor integrale beveiliging?	De organisatorische inrichting en daarmee het kwaliteitssysteem van integrale beveiliging in gemeenten kan verschillende vormen en gedaanten aannemen. In het 'Instructiedocument voor organisatorische inrichting van integrale beveiliging gemeenten' schetsen we twee basisvarianten als kader. Het is aan de gemeenten om – passend bij de eigen context en situatie – een passende governancestructuur en kwaliteitssysteem op te zetten.
Verwijzing	Link naar ander deel van platform waarin dit is uitgewerkt

Bijlage I: Wettelijk kader en normen

Integraal beveiligingsbeleid en deelthema's zijn gebaseerd op diverse wet- en regelgeving. Hieronder is een eerste overzicht genereerd wat richting geeft. Dit vergt een periodieke update.

Beveiligingsplan

- Arbeidsomstandighedenwet

Brandveiligheid

- Bouwbesluit 2012
- Besluit Omgevingsrecht
- Handleiding Brandveilig Gebruik
- Arbeidsomstandighedenwet
- Woningwet
- Richtlijn (EU) 92/58/EEG
- NEN-normen

Informatiebeveiliging

- Baseline Informatieveiligheid Overheid
- Wet basisregistratie personen
- Besluit basisregistratie personen
- Algemene Verordening Gegevensbescherming
- Richtlijn (EU) 2016/1148
- Regeling SUWI
- Leidraad Coordinated Vulnerability Disclosure
- Archiefwet
- NEN-NL-ISO 27001/2

Cameratoezicht

- Gemeentewet
- Richtlijn (EU) 2016/680
- Algemene Verordening Persoonsgegevens
- Wet Politiegegevens
- Wet justitiële en strafvorderlijke gegevens
- Guidelines 3/2019 on processing of personal data through video devices (European Data Protection Board)

Personele veiligheid:

- Burgerlijk Wetboek
- Arbeidsomstandighedenwet
- Arbeidsomstandighedenbesluit
- Handleiking Voorkomen en beperken van agressie en geweld 2013
- Gemeentewet
- Richtlijn (EU) 89/391/EEG en Richtlijn (EU) 92/58/EEG
- Wet particuliere beveiligingsorganisaties en recherchebureaus
- RICHTLIJN 2014/24/EU
- Circulaire met betrekking tot de bewaking en beveiliging van personen, objecten en diensten 2019
- Regeling rechtspositie decentrale politieke ambtsdragers
- Algemene Verordening Persoonsgegevens
- Normenkader Beveiliging Rijkskantoren (NKBR)

Integriteit

- Gemeentewet
- Ambtenarenwet 2017
- Modelaanpak basisnormen integriteit
- Handleiking integriteit van politieke ambtsdragers bij gemeenten, provincies en waterschappen
- Registratie integriteitsschendingen (handleiking 2008)
- 12 principles of good democratic governance