Gemeentelijk Informatiebeveiligingsplan

Algemeen Informatiebeveiligingsbeleid

Gemeente Ooststellingwerf

Versie : 2.0

Status : definitief

Datum : 27-01-2015

Inhoudsopgave

1 Algemeen

1.1 Inleiding

We maken steeds meer en steeds vaker gebruik van geautomatiseerde systemen. Ook is er sprake van toenemende (digitale) informatie-uitwisseling tussen overheidsorganisaties onderling en met burgers en bedrijven door ontwikkelingen zoals internet, e-government en telewerken. We moeten hierbij rekening houden met de privacyregels. Burgers, bedrijven, instellingen moeten de overheid kunnen vertrouwen en hebben er recht op te weten wie welke gegevens verzamelt en waarvoor deze gebruikt worden. Het is daarom van groot belang dat gegevens alleen onder strikte voorwaarden gebruikt worden en goed beveiligd zijn tegen onbevoegd gebruik.

Iedereen kan voorbeelden bedenken van zaken die mis kunnen gaan bij informatie-uitwisseling: het netwerk doet het niet, een virus meegestuurd met een e-mail, de website of een database wordt gehackt en gegevens gewijzigd, onbevoegden in het gebouw die informatie zien die niet voor hen bestemd is etc. Dit zal soms ervaren worden als een vervelende bijkomstigheid, maar het kan soms ook grote consequenties hebben. Verstoring van vooral maatschappelijk- en bedrijfsvitale processen kan resulteren in schade voor de burgers en (imago)schade voor de gemeente. Bijvoorbeeld doordat de privacy van de persoonsgegevens niet meer gewaarborgd is, de betaling van de sociale uitkeringen vertragen, dat de berekening van de OZB-aanslagen onjuist zijn, het beheer van de openbare ruimten en gronden niet meer op een betrouwbare wijze kan plaatsvinden.

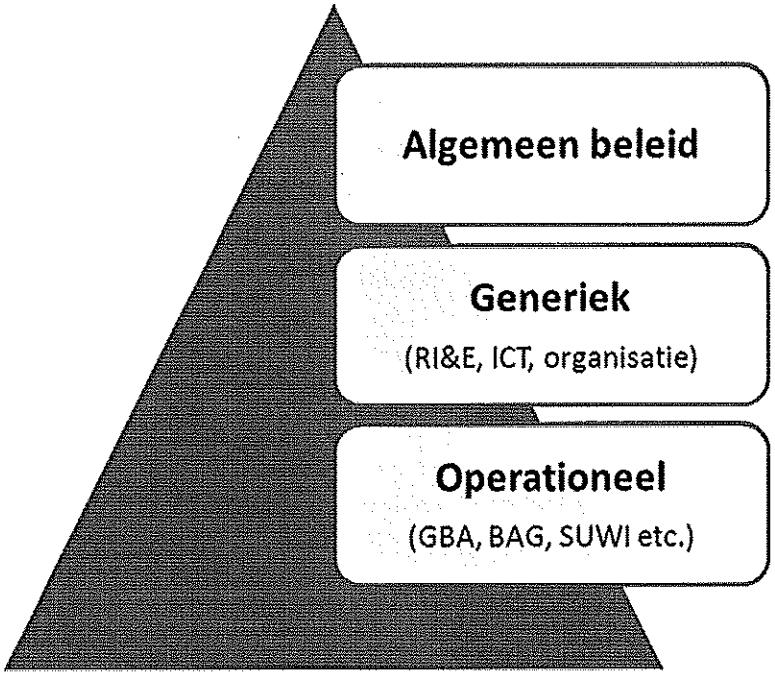
Het bestuur en management is verantwoordelijk voor de continuïteit en kwaliteit van de dienstverlening en de betrouwbaarheid en beschikbaarheid van alle daarvoor noodzakelijke informatie. Het is dus van belang dat de vitale informatie op een goede en adequate wijze wordt beveiligd ter beperking van risico's op dit vlak. Daarom wordt in dit document op algemeen niveau vormgegeven aan de informatiebeveiliging binnen de gemeente Ooststellingwerf. Hiermee wordt bedoeld: het borgen van informatiebeveiliging binnen de hele organisatie door middel van het vaststellen van een aantal uitgangspunten op het gebied van informatiebeveiliging en het inrichten van een 'beveiligingsorganisatie'.

In voorliggend algemeen Informatiebeveiligingsbeleid wordt ingegaan op de visie op informatiebeveiliging binnen de gemeente Ooststellingwerf. Er wordt mee bepaald wat het minimale organisatiebrede informatiebeveiligingsniveau dient te zijn. Ook worden de beleidsuitgangspunten geschetst die ervoor moeten zorgen dat binnen de gemeente Ooststellingwerf de (digitale) informatie voldoende beveiligd is en dat verantwoord wordt omgegaan met die informatie.

Het algemene beleid vormt het kader voor de verschillende tactische en operationele informatiebeveiligingsplannen. In deze (deel-)plannen wordt voor de specifieke vakgebieden verdere uitwerking aan het beleid gegeven.

1.2 De Informatiebeveiligingspiramide

In dit Informatiebeveiligingsbeleid is op algemeen en tactisch niveau aangeven welke uitgangspunten van toepassing zijn op de informatiebeveiliging binnen de gemeente Ooststellingwerf.
Teneinde de scope van dit document te verduidelijken is hieronder aangegeven welke niveaus van informatiebeveiliging vallen te onderkennen.



Figuur 1: Informatiebeveiligingspiramide Ooststellingwerf

Het informatiebeveiligingsbeleid van de gemeente Ooststellingwerf is in de piramide gesitueerd op algemeen niveau. Met een doorlooptijd van 4 a 5 jaar beslaat het algemeen beleid, een voor informatieprocessen, relatief lang tijdpad.
Het beleid is bedoeld als richtinggevend document en gaat derhalve niet in op specifieke technische of organisatorische maatregelen. Het stuk is wel zodanig opgezet dat praktijksituaties eenvoudig kunnen worden opgezet of getoetst.

Het tweede niveau is gericht op het implementatietraject. De implementatie begint met het uitvoeren van een risico inventarisatie en evaluatie (RI&E). Tijdens deze RI&E worden de 'harde aspecten' onderzocht. Dat wil zeggen de techniek, de regels en de procedures. Daarnaast worden ook de 'zachte aspecten' meegenomen. Deze richten zich op het menselijk handelen en cultuuraspecten en daarnaast de sociale en fysieke inrichting van de organisatie.
De risico inventarisatie en evaluatie geeft weer welke onderwerpen kritisch zijn en waar nog aanvullende maatregelen nodig zijn. De uitkomst van de analyse wordt vervolgens gebruikt als input voor de diverse generieke en operationele informatiebeveiligingsplannen.

In de generieke informatiebeveiligingsplannen worden de beveiligingsobjecten benoemd die gelden voor de gehele organisatie. Het Informatiebeveiligingsplan ICT benoemt de beveiligingsobjecten op het gebied van de ICT en de getroffen maatregelen ten behoeve van het gevraagde beveiligingsniveau. Het Informatiebeveiligingsplan Organisatie benoemt de beveiligingsobjecten op het gebied van fysieke toegangsbeveiliging (gebouwen) en personeel en de getroffen maatregelen ten behoeve van het gevraagde beveiligingsniveau.

De specifieke wettelijke eisen die gesteld worden aan de beveiliging van onder meer de GBA, Suwinet en BAG vallen onder de verantwoordelijkheid van de betreffende proceseigenaren: dit is het derde niveau. De hieruit voortvloeiende beveiligingsmaatregelen zijn beschreven in de operationele informatiebeveiligingsplannen van de betreffende teams. Daarin zal ook verwezen worden naar de generieke informatiebeveiligingsmaatregelen die zijn getroffen op het gebied van ICT en organisatie.

1.3 Goedkeuring

Goedkeuring van dit Algemeen Informatiebeveiligingsbeleid en de daarbij horende bijlagen vindt plaats nadat de betrokken personen van zowel de opdrachtnemer als opdrachtgever overeenstemming hebben bereikt over wat hierin staat beschreven.

Versie 2.0 van het Algemeen Informatiebeveiligingsbeleid dient te worden vastgesteld door het college van B&W van de gemeente Ooststellingwerf.

Versie	Datum	Status	Aard wijzigingen	Verstuurd aan
1.0	12-11-2013	Definitief	Gereed voor vaststelling	College van B&W
2.0	13-01-2015	Definitief	Gereed voor vaststelling	College van B&W

1.4 Verantwoording

De Baseline Informatiebeveiliging Nederlandse gemeenten (BIG) is het normenkader dat de beschikbaarheid, de integriteit, de vertrouwelijkheid en de controleerbaarheid van de gemeentelijke informatie(systemen) bevordert. De BIG is opgesteld door de Informatiebeveiligingsdienst voor gemeenten (IBD), een initiatief van de VNG en het Kwaliteitsinstituut Nederlandse Gemeenten (KING). De BIG is een richtlijn die een totaalpakket aan informatiebeveiligingsmaatregelen omvat die voor iedere gemeente geldt. De BIG is opgezet rondom de bestaande normen (NEN/ISO 27002:2007 en NEN/ISO 27001:2005). Deze standaard is voor de Nederlandse overheid gekozen en algemeen aanvaard als de norm voor informatiebeveiliging. Voor specifieke maatregelen is in de BIG ook gebruik gemaakt van onder andere de WBP, de wet SUWI, de wet BRP, de BAG en de PUN.

De gemeente stelt het normenkader vast, waarbij er ruimte is voor afweging en prioritering op basis van het principe 'pas toe of leg uit'.

1.5 Uitvoering en evaluatie

Informatiebeveiliging is pas effectief als deze op een gestructureerde manier wordt aangepakt. De basis hiervoor is de beleidsdoelstelling van het Algemeen Informatiebeveiligingsbeleid. Binnen de gemeente moeten medewerkers verantwoordelijkheden krijgen voor de implementatie van dit beleid.

De medewerkers worden betrokken (o.a. tijdens werkoverleg) bij de ontwikkeling en implementatie van zowel het beleid als de uitvoering.

Het Algemeen informatiebeveiligingsbeleid wordt jaarlijks geëvalueerd en eventueel bijgesteld door de beveiligingsadviescommissie. Bij wijziging wordt het geactualiseerde plan aangeboden ter vaststelling aan het college van B&W.

2 Informatiebeveiligingsbeleid

Zonder betrouwbare informatie is de gemeente Ooststellingwerf niet in staat kwalitatief hoogwaardige diensten te leveren aan de burgers, bedrijven en instellingen. Informatie dient juist te zijn, beschikbaar en ontoegankelijk voor onbevoegden.

De eindverantwoordelijkheid voor het informatiebeveiligingsbeleid ligt te allen tijde bij het bestuur en wordt in het kader van integraal management uitgedragen en bewaakt door het lijnmanagement, de proceseigenaren. Onder proceseigenaar wordt verstaan de verantwoordelijke voor de beheersing, aansturing en het resultaat van een proces. De proceseigenaar is daarmee tevens eigenaar van de in zijn proces ontstane informatie (informatie-eigenaar) en verantwoordelijk voor de beveiliging van die informatie binnen en buiten de gemeente. De zorg voor betrouwbare informatie is daarmee een wezenlijk onderdeel van integraal management.

2.1 Toepassingsgebied

Informatiebeveiliging raakt de hele organisatie en betreft alle voorkomende informatie hetzij elektronisch, hetzij schriftelijk. Om de informatie adequaat te beschermen, moet een samenhangend stelsel van organisatorische, fysieke en ICT maatregelen genomen worden. Zo kunnen problemen worden voorkomen, opgespoord, beperkt en hersteld.

Informatiebeveiliging gaat over de continuïteit, vertrouwelijkheid, betrouwbaarheid en controleerbaarheid van de informatievoorziening.

Dit wordt onderverdeeld in de begrippen:

1. **Beschikbaarheid**
   Kan ik op het juiste moment over de benodigde informatie beschikken (continuïteit).
2. **Vertrouwelijkheid**
   Hebben alleen de juiste (bevoegde) personen toegang tot de informatie (vertrouwelijkheid).
3. **Integriteit**
   Klopt de informatie met de werkelijkheid (betrouwbaarheid).
4. **Controleerbaarheid**
   Vindt een regelmatige controle plaats om vast te stellen of de uitvoering van beheersingsmaatregelen goed werkt.

Het informatiebeveiligingsbeleid van de gemeente is daarmee van toepassing op:

- de fysieke beveiliging van gebouwen;
- de inrichting van de organisatie;
- alle informatiesystemen, zowel handmatig als geautomatiseerd;
- het beheer van de informatie, de systemen en de infrastructuur;
- de opslag, de invoer, het gebruik en de vernietiging van informatie.

Beveiligingsmaatregelen kunnen dus liggen op het fysieke vlak (zoals muren, deuren, sloten en noodstroomvoorziening), op het logische vlak (zoals wachtwoord-systemen, encryptie, digitale gegevensuitwisseling en digitale handtekeningen) en op het organisatorisch vlak (zoals functiescheiding, controle en audit).

2.2 Beleidsdoelstelling

Onder informatiebeveiliging wordt verstaan: "enerzijds het vooraf treffen van maatregelen ter voorkoming, opsporing en beperking van verstoringen in de informatievoorziening en anderzijds het herstel indien die verstoringen zich voordoen".

Er kan hierbij onderscheid gemaakt worden tussen:

1. Informatie die de organisatie binnenkomt.
2. Informatie binnen de organisatie.
3. Informatie die de organisatie verlaat.

Ad. 1. Informatie die de organisatie binnenkomt
Informatiebeveiliging beoogt te borgen dat de kwaliteit van informatie die de organisatie binnenkomt (in termen van beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid) van het gewenste niveau is en blijft. De organisatie stelt kwaliteitseisen en legt deze vast. De organisatie richt controles in om naleving van de afspraken te bewaken.

Ad 2. Informatie binnen de organisatie
Informatiebeveiliging richt zich op de continuïteit en kwaliteit van de informatie in de gemeentelijke organisatie. De organisatie stelt eisen aan de kwaliteit van de informatiebeveiliging die op basis van een risicoafweging door de proceseigenaar worden vertaald naar een bepaald beveiligingsniveau. Daarbij hoort het (laten) nemen van maatregelen ten behoeve van de desbetreffende processen. Hierbij houdt de proceseigenaar rekening met wettelijk gestelde kaders en richtlijnen. De organisatie richt controles in om de voortgang van de maatregelen te bewaken.

Ad 3. Informatie die de organisatie verlaat
Informatiebeveiliging is erop gericht dat informatie die de organisatie in welke vorm dan ook verlaat, door de juiste persoon wordt ontvangen, onderweg niet onderschept of gelezen kan worden en qua doorlooptijden binnen de normen blijft. De proceseigenaar zorgt ervoor dat hij invloed behoudt door 'gebruiksvoorwaarden' te koppelen aan de verstrekking van informatie aan externe partijen.

De beleidsdoelstelling luidt:

Het college van B&W van de gemeente Ooststellingwerf stelt zich ten aanzien van de informatiebeveiliging, met inachtneming van wettelijke verplichtingen, als doelstelling beveiligingsmaatregelen te treffen die de beschikbaarheid, de integriteit, de vertrouwelijkheid en de controleerbaarheid van de gemeentelijke bedrijfsgegevens zoveel mogelijk garanderen.

Deze doelstelling geldt ten aanzien van alle gegevensverwerkende processen waarvoor het college van B&W van de gemeente Ooststellingwerf de uiteindelijke verantwoordelijkheid draagt.

2.3 Wettelijke verplichtingen

Zoals reeds uit de beleidsdoelstelling blijkt, zijn het niet slechts interne redenen waarom de gemeente haar informatievoorziening moet beveiligen. Ook de wetgever stelt een aantal eisen. De gemeente Ooststellingwerf zal zich houden aan de bepalingen van de in het kader van informatiebeveiliging relevante wet- en regelgeving zoals het Wetboek van Strafrecht, het Wetboek van Strafvordering (Wet computercriminaliteit), evenals de relevante regelgeving. In de Wet Bescherming Persoonsgegevens (WBP) worden wettelijk verplichte eisen gesteld die zich richten tegen "verlies of enige vorm van onrechtmatige verwerking van gegevens". Onder onrechtmatige vormen van verwerking vallen de aantasting van de gegevens, onbevoegde kennisneming, wijziging of verstrekking daarvan. De beveiligingsverplichting strekt zich uit tot alle onderdelen van het proces van gegevensverwerking.

Artikel 13 van de Wet bescherming persoonsgegevens (WBP) geldt als grondslag voor het informatiebeveiligingsbeleid. De tekst van dit artikel luidt:

De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand der techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen persoonsgegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Naarmate bijvoorbeeld de gegevens een gevoeliger karakter hebben, of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekenen, worden strengere eisen gesteld aan de beveiliging van die gegevens.

2.4 Beleidselementen

Informatiebeveiligingsbeleid is niets anders dan een verzameling van algemene uitgangspunten van de bestuurlijke en ambtelijke top voor de medewerkers op het tactisch en operationeel niveau. Deze uitgangspunten dienen gevolgd te worden om te komen tot een adequate informatiebeveiliging.

Binnen het informatiebeveiligingsbeleid draait het om integrale verantwoordelijkheid. De verantwoordelijke manager is verantwoordelijk voor zijn (deel)processen en als proceseigenaar ook verantwoordelijk voor de beveiliging van de daarbij behorende informatie. De proceseigenaar doet dit door normen en kaders te stellen waarbij rekening gehouden wordt met wettelijke kaders. Deze normen en kaders moeten minimaal voldoen aan het via dit document vastgestelde basisbeveiligingsniveau.

Het beleid vormt daarmee de basis voor de tactische en operationele beveiligingsplannen die door de verschillende proceseigenaren dienen te worden opgesteld.

2.4.1 Beveiligingsniveaus

Er worden binnen de gemeente Ooststellingwerf drie beveiligingsniveaus onderscheiden:
- Hoog
- Midden
- Laag

Deze niveaus vormen het toetsingskader voor de bepaling van het beveiligingsniveau.

Op ieder niveau worden eisen gesteld ten aanzien van de beschikbaarheid (kunnen we beschikken over de informatie op het gewenste moment), vertrouwelijkheid (kunnen alleen de geautoriseerde medewerkers bij de informatie), integriteit (kunnen we er vanuit gaan dat de gevonden informatie 'betrouwbaar' is) en controleerbaarheid (kunnen we (achteraf) vaststellen hoe de informatievoorziening en haar componenten zijn gestructureerd).
Onderstaand wordt dit verder uitgewerkt.

Eisen die gesteld worden aan een **HOOG** beveiligingsniveau:

	Beschikbaarheid	**Vertrouwelijkheid**	**Integriteit**	**Controleerbaarheid**
Voorkomen	Max. 8 storingen per jaar bij de belangrijkste bedrijfsapplicaties	Braakbestendig voor 4 uur[1] (Digitale) toegang alleen voor bekende interne medewerkers	Bekende bron Bekende informatie Ervaren gebruikers	Mutaties herleidbaar naar individuele medewerker
Beperken	Gemiddelde storingsduur 1 uur en max. duur 4 uur per storing	Binnen een ½ uur poging verijdeld	1 op 1000 fouten Reconstrueerbaar	1 op 100 fouten Reconstrueerbaar
Opsporen	Binnen ½ uur probleem gesignaleerd	Direct	Wekelijks en na een incident	Dagelijks
Herstellen	Binnen 3 ½ uur na signalering hersteld	Binnen 1 uur (digitale) sloten hersteld	Binnen 1 uur na signalering	Dagelijks
	' Ongestoord werkproces'	**'geheim'**	**'100% zekerheid'**	**'Gestructureerde informatievoorziening'**

[1] Het betreft zowel fysieke inbraak als 'elektronische' inbraak (computerinbraak)

Eisen die gesteld worden aan een **MIDDEN** beveiligingsniveau:

	Beschikbaarheid	**Vertrouwelijkheid**	**Integriteit**	**Controleerbaarheid**
Voorkomen	Max. 14 storingen per jaar bij de belangrijkste bedrijfsapplicaties	Braakbestendig voor 2 uur. (Digitale) toegang voor bekende medewerkers	Bekende bron Opgeleide gebruikers	Mutaties herleidbaar naar individuele medewerker
Beperken	Gemiddelde storingsduur 4 uur en max. duur 8 uur per storing	Binnen een 1 uur poging verijdeld	1 op 500 fouten Reconstrueerbaar	5 op 100 fouten Reconstrueerbaar
Opsporen	Binnen 1 uur probleem gesignaleerd	Direct	Wekelijks en na een incident	Wekelijks
Herstellen	Binnen 7 uur na signalering	Binnen 4 uur (digitale) sloten hersteld	Binnen 4 uur na signalering	Wekelijks
	'Bijna ongestoord werkproces'	**'vertrouwelijk'**	**'90% zekerheid'**	**'Gestructureerde informatievoorziening'**

Eisen die gesteld worden aan een **LAAG** beveiligingsniveau:

	Beschikbaarheid	**Vertrouwelijkheid**	**Integriteit**	**Controleerbaarheid**
Voorkomen	Max. 20 storingen per jaar bij de belangrijkste bedrijfsapplicaties	Braakbestendig voor 1 uur. (Digitale) toegang voor bekende medewerkers	Bekende bron Opgeleide gebruikers	Mutaties herleidbaar naar individuele medewerker
Beperken	Gemiddelde storingsduur 8 uur en max. duur 16 uur per storing	Binnen een 1 uur poging verijdeld	1 op 100 fouten Reconstrueerbaar	10 op 100 fouten
Opsporen	Binnen 2 uur probleem gesignaleerd	Direct	Wekelijks en na een incident	steekproefsgewijs
Herstellen	Binnen14 uur na signalering	Zelfde dag (digitale) sloten hersteld	Binnen 8 uur na signalering	Na signalering
	'Meestal ongestoord werkproces'	**'semi- openbaar'**	**'80% zekerheid'**	**'Meestal gestructureerde informatievoorziening'**

2.4.2 Gemeentebreed beveiligingsniveau

Het gemeentebrede beveiligingsniveau vormt de minimale norm voor alle informatie binnen de gemeente, ongeacht of dit elektronische of papieren informatie is. Deze norm biedt voor ieder proces een bepaalde zekerheid over de beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van de informatie binnen het proces.

Beschikbaarheid

Als algemene beveiligingsdoelstelling is door het college vastgesteld dat de informatiesystemen een beschikbaarheid tijdens werktijd moeten kennen van minimaal 98%. Geconstateerd is dat in de afgelopen twee jaar de beschikbaarheid van de informatiesystemen hoger dan 98% is geweest. Dit betreft echter de beschikbaarheid van de informatiesystemen voor medewerkers en bestuur gedurende de openingstijden van het gebouw.

Buiten de openingstijden worden er op dit moment (formeel) nog geen eisen gesteld aan de beschikbaarheid van de informatiesystemen. Uitzondering hierop zijn voorzieningen in het kader van rampenbestrijding. In het kader van de (digitale) dienstverlening wordt van de gemeente wel steeds meer flexibiliteit verwacht door burgers, bedrijven en instellingen. Ook de flexibilisering van werktijden en de mogelijkheid om thuis te werken, vragen om een ruimere beschikbaarheid van de informatiesystemen dan binnen de genoemde openingstijden. De praktijk wijst namelijk uit dat medewerkers ook steeds vaker 's avonds of in het weekend thuis werken.

Vertrouwelijkheid
Binnen de gemeente wordt enerzijds veel gebruik gemaakt van openbare informatie, maar anderzijds wordt door diverse teams met vertrouwelijke en/of privacygevoelige informatie gewerkt. Voor deze laatstgenoemde informatie geldt dat voorkomen moet worden dat deze informatie ongeoorloofd openbaar gemaakt wordt. Dit kan door deze informatie zeer goed af te schermen voor onbevoegden en uitsluitend toegankelijk te maken voor daartoe geautoriseerde personen. Intern geldt dit voor medewerkers, maar vanzelfsprekend ook voor burgers en bedrijven die gebruik maken van het digitaal loket.
Voor vertrouwelijke informatie dienen geautoriseerde procedures vastgesteld en gevolgd te worden. Nadere uitwerking hiervan vindt in de separate informatiebeveiligingsplannen plaats.

Integriteit
Wanneer we het hebben over de betrouwbaarheid van informatie (integriteit) durven we te stellen dat het van groot belang is dat er met een grote mate van zekerheid van kan worden uitgegaan dat de gegevens in overeenstemming zijn met de werkelijkheid, zonder dat iets ten onrechte is toegevoegd, verdwenen of achtergehouden. Maatregelen moeten gericht zijn op het garanderen van de betrouwbaarheid van onze informatie. Dit is nodig om de kwaliteit van onze werkprocessen en dienstverlening te kunnen garanderen.

Controleerbaarheid
Een regelmatige controle op de uitvoering van de beheersmaatregelen is noodzakelijk om vast te stellen of deze goed werken. Daarom is controleerbaarheid (auditability, assurance, audit trail) van groot belang. Controleerbaarheid gaat over de mogelijkheid en de manier om (achteraf) vast te kunnen stellen hoe de informatievoorziening en de daarbij behorende componenten zijn gestructureerd.

Het organisatiebrede (basis)beveiligingsniveau luidt:

Het college van B&W van de gemeente Ooststellingwerf stelt vast dat het organisatiebrede (basis) beveiligingsniveau ten aanzien van beschikbaarheid, vertrouwelijkheid, integriteit en controleerbaarheid altijd **midden** dient te zijn.

2.4.3 Normen
Voorliggend Informatiebeveiligingsbeleid is gebaseerd op de normen zoals vastgesteld in de Baseline Informatiebeveiliging Nederlandse Gemeenten.

Uitwerking van het in paragraaf 2.4.2 genoemde beveiligingsniveau levert de volgende normen op:

Beschikbaarheid (midden)	Normen
Een bijna ongestoord werkproces	- (Een deel van) het gebouw en de werkplekken is voorzien van noodstroom, in ieder geval de serverruimtes. - Voor het garanderen van een bijna ongestoord werkproces en de daarvoor benodigde informatievoorziening zijn onderhoudscontracten afgesloten. - Er wordt dagelijks een back-up gemaakt. - Er is een uitwijklocatie beschikbaar. - Er is een (interne) uitwijkovereenkomst ten behoeve van het dataverkeer.
Goede telefoonvoorziening	- De telefooncentrale functioneert gedurende kantoortijden (bijna) ongestoord. - Er kan (deels) op mobiele telefonie overgeschakeld worden. - Voor de rampenbestrijding wordt teruggegrepen op noodnetvoorzieningen.
Vertrouwelijkheid (midden)	**Normen**
Een beveiligd gebouw, veilige werkplekken voor medewerkers en bestuur	- het gemeentehuis en het gebouw van de gemeentewerf zijn beveiligd tegen inbraak, bliksem, brand en wateroverlast. - Er is een elektronische toegangsbeveiliging voor het gemeentehuis en er is compartimentering. - het gemeentehuis is afgesloten voor publiek met uitzondering van de publieksruimte tijdens openingstijden van het gebouw. - Bezoekers worden begeleid buiten de publieksruimte. - Computer-, server- en kluisruimten zijn alleen toegankelijk voor geautoriseerde medewerkers.
Beveiligde systemen	- Er is een eigen firewall. - Er is een virusscanner. - Er wordt gewerkt met wachtwoorden / identificatie van gebruikers. - Er zijn procedures voor het vernietigen van verwijderbare media, back-up en recovery.
Integriteit (midden)	**Normen**
Opgeleide en deskundige gebruikers	- Gebruikers van de systemen zijn opgeleid, hebben verantwoordelijkheidsgevoel en weten wat van hen verwacht wordt. - Taken, verantwoordelijkheden en bevoegdheden zijn dusdanig geregeld dat medewerkers elkaars taken kunnen overnemen.
Procesbeveiliging	- Binnen de gemeente is bekend welke processen extra beveiligd moeten worden omdat het om vertrouwelijke/privacygevoelige informatie gaat, er wettelijke normen aan verbonden zijn en/of ze grote financiële belangen vertegenwoordigen.
Controleerbaarheid (midden)	**Normen**
Mutaties herleidbaar naar de individuele medewerker	- Regelmatige controle. - Minstens 95% van de mutaties zijn herleidbaar naar individuele medewerker.
Raadplegingen herleidbaar naar individuele medewerker	- Regelmatige controle. - Minstens 90% van de raadplegingen zijn herleidbaar naar de individuele medewerker.

2.4.4 Beveiligingsplannen en uitwerkingsafspraken

Bovenstaand overzicht levert een aantal 'beveiligingsobjecten' waarvoor maatregelen zijn te formuleren ten behoeve van het gewenste beveiligingsniveau van de basisnormen.

Nadere uitwerking van de benodigde beveiligingsmaatregelen wordt aan de hand van een gemeentebrede risicoanalyse op het gebied van ICT en Organisatie (gebouwen en personeel) generiek in het gemeentelijke informatiebeveiligingsplan opgenomen. De uitkomst van de analyse wordt vervolgens gebruikt als input voor de diverse generieke en operationele informatiebeveiligingsplannen. Deze (deel) plannen worden vastgesteld door de directie.

Het uitvoeren en handhaven van beveiligingsmaatregelen en -procedures is een integrale verantwoordelijkheid van het lijnmanagement. De lijnmanager is in die zin eigenaar en verantwoordelijk voor de beveiliging van de in zijn processen ontstane informatie. Hij dient te beoordelen of en welke (extra) maatregelen nodig zijn om te voldoen aan het (basis)beveiligingsniveau op operationeel niveau, uitgewerkt per proces, systeem en/of applicatie. Hierbij wordt rekening gehouden met de wettelijke kaders, zie ook paragraaf 2.3. Proceseigenaren maken, indien noodzakelijk, nadere uitwerkingsafspraken met de betreffende 'leveranciers'.

Indien er sprake is van wettelijke verplichtingen om een plan op te stellen en/of de beveiligingsrisico's als hoog ingeschat worden, moeten (operationele) beveiligingsplannen opgesteld worden. De beveiligingsadviescommissie zal hierover adviseren. Deze informatiebeveiligingsplannen worden vastgesteld door de directie.

Belangrijk is dat er gemeten en gerapporteerd wordt over beveiligingsrisico's en -incidenten op het gebied van beschikbaarheid, vertrouwelijkheid, integriteit en controleerbaarheid. Dit om (jaarlijks) te kunnen bepalen of het vastgestelde niveau daadwerkelijk behaald is en/of eventuele extra maatregelen genomen moeten worden. Communiceren over informatiebeveiliging is eveneens belangrijk in het kader van het beveiligingsbewustzijn.

2.5 Beleidsuitgangspunten

Informatiebeveiliging:

- is belangrijk en dient serieus vormgegeven te worden;
- is onderdeel van integraal management;
- is een organisatorisch vraagstuk met technische consequenties;
- gaat om de afweging tussen risico, kosten en werkbaarheid;
- omvat de (inrichting van de) organisatie, de medewerker, de informatiesystemen en de fysieke omgeving.

In onderstaand schema een uitwerking:

Uitgangspunt	Toelichting
Organisatie	
Inbedden in organisatie	- Informatiebeveiliging is ingebed in de organisatie als onderdeel van integraal management.
Procesbeveiliging	- Processen worden integraal beveiligd door de proceseigenaren. - Deze zijn gehouden aan het minimale niveau zoals in dit beleid geschetst. - Integraal betekent dit: het treffen van maatregelen ter voorkoming, beperking, herstel en opsporing van incidenten.
Derden	- Bij informatieverwerking of beheer door en bij derden worden schriftelijk eisen vastgelegd over de gewenste informatiebeveiliging.

Uitgangspunt	Toelichting
Efficiëntie, 100% veilig kan niet	- De proceseigenaar maakt altijd een afweging of het in te zetten middel niet erger is dan het te reduceren risico. - Er moet een evenwicht zijn tussen werkbaarheid, kosten en risico. - De gemeente beseft dat 100% beveiliging niet mogelijk is.
Prioritering van risicoreductie	- Bij prioritering van risicoreductie wordt rekening gehouden met: kans van optreden, impact bij optreden, verwijtbaarheid van het risico, omvang van de schade, betrokken partijen, wet- en regelgeving.
Toetsen	- De gemeente toetst haar informatiebeveiliging zowel door collegiale toetsing als door externe audits.
Integriteit van de organisatie	- De gemeente houdt zich aan alle bepalingen met betrekking tot privacy en informatiebeveiliging in overeenkomsten met derden.
Wet- en regelgeving	- De gemeente houdt zich aan alle geldende wet- en regelgeving waaruit voorwaarden voor informatiebeveiliging volgen.
Medewerkers	
Kennis over informatiebeveiliging	- De medewerkers worden geïnformeerd over en betrokken (bijvoorbeeld tijdens werkoverleg) bij de ontwikkeling en implementatie van zowel het beleid als de uitvoering.
Delen van informatie	- Uitgangspunt is dat medewerkers weten hoe zij om dienen te gaan met die vertrouwelijke informatie en daarin hun verantwoordelijkheid nemen en dragen. - Medewerkers leggen de ambtseed of de belofte af en tekenen een integriteitsverklaring.
Need to know	- Iedere medewerker krijgt of haalt de wettelijk toegestane informatie die hij nodig heeft voor het werk. Dit houdt in dat algemene gemeentelijke informatie voor iedereen beschikbaar is en dat werkspecifieke informatie binnen afdelingen/teams/functies blijft.
Eigen verantwoordelijkheid	- Iedere medewerker is verantwoordelijk voor de hem toevertrouwde informatie. - De medewerkers zijn beveiligingsbewust en -bekwaam. - Ten behoeve van het creëren van het beveiligingsbewustzijn is er de top tien informatiebeveiliging die ook uitgereikt wordt aan nieuwe medewerkers (zie bijlage).
Controle	- De gemeente vertrouwt haar medewerkers maar treft wel een aantal controle maatregelen (bijvoorbeeld screening, logging en monitoring).
ICT (informatie)	
Basisbeveiliging	- Er is een (basis)beveiligingsniveau voor alle systemen. - Er wordt gewerkt met een stelsel van identificatiecodes en wachtwoorden en voor geheime informatie kan met cryptografie gewerkt worden.
Uniformiteit	- Maatregelen voor beveiliging worden zoveel mogelijk geüniformeerd.
Facilitair	- De gemeente faciliteert de gewenste en benodigde procesbeveiliging, treft daartoe de noodzakelijke maatregelen en maakt de kosten inzichtelijk.
Fysiek	
Compartimentering	- De gebouwen vormen een fysieke beveiligingsschil voor toegang tot vertrouwelijke informatie en beschikbare apparatuur. - Bezoekers worden geregistreerd en begeleid achter de compartimentering.
Camerabeveiliging	- Publieksstromen worden op verschillende locaties zoals bij de hoofdingang deels gemonitord.

3 Beveiligingsorganisatie

3.1 Burgemeester en wethouders

De eindverantwoordelijkheid voor het informatiebeveiligingsbeleid ligt te allen tijde bij het bestuur en wordt in het kader van integraal management uitgedragen en bewaakt door het lijnmanagement.

3.2 Directie en lijnmanagement

Beveiliging is op ambtelijk niveau de verantwoordelijkheid van de directie van de gemeente Ooststellingwerf. De directie bepaalt binnen de gegeven bestuurlijke kaders de koers van het ambtelijk apparaat. De directie is in die zin ook verantwoordelijk voor de actualiteit en uitvoering van het informatiebeveiligingsbeleid.

Het uitvoeren en handhaven van beveiligingsmaatregelen en -procedures is een integrale verantwoordelijkheid van het lijnmanagement. De lijnmanager is verantwoordelijk voor de beheersing, aansturing en resultaten van alle (sub)processen binnen zijn team. Hij is daarmee tevens eigenaar en verantwoordelijk voor de beveiliging van de in zijn processen ontstane informatie. De lijnmanager kan de uitvoering van deze verantwoordelijk op procesniveau bij zijn medewerkers beleggen.

De lijnmanager is in die hoedanigheid degene die de directie adviseert over het vereiste beveiligingsniveau voor zijn processen, risicoafwegingen maakt, de uitvoering van de maatregelen controleert, medewerkers aanspreekt op gedrag. Voor eventuele sancties wordt verwezen naar het gemeentelijke HRM-beleid.

3.3 Beveiligingsfunctionaris

Voor een structurele borging van informatiebeveiliging in de gemeentelijke organisatie is de functie van beveiligingsfunctionaris in het leven geroepen. De beveiligingsfunctionaris is door het college van B&W benoemd.

De beveiligingsfunctionaris heeft een adviserende, signalerende, controlerende en coördinerende rol ten aanzien van het beveiligingsbeleid. De beveiligingsfunctionaris is mede verantwoordelijk voor het opstellen en vaststellen van het informatiebeveiligingsbeleid, het toezicht op de naleving van de beveiligingsmaatregelen en -procedures, het begeleiden van beveiligingsactiviteiten en een snelle adequate terugkoppeling in geval van beveiligingsincidenten.

De beveiligingsfunctionaris rapporteert jaarlijks aan het college van B&W over de voorbereiding, implementatie en uitvoering van het beveiligingsbeleid en de naleving van de beveiligingsmaatregelen en -procedures, zo nodig zonder tussenkomst van de lijnorganisatie. Hij verstrekt daarnaast gevraagd en ongevraagd advies om het gewenste beveiligingsniveau te kunnen realiseren.

3.4 Beveiligingsadviescommissie

Voor de totstandkoming van en periodieke afstemming over het informatiebeveiligingsbeleid heeft de gemeente Ooststellingwerf een beveiligingsadviescommissie ingesteld. De beveiligings-adviescommissie komt minimaal tweemaal per jaar bijeen en houdt zich bezig met de volgende aspecten:

- richting en invulling geven aan het informatiebeveiligingsbeleid;
- adviseren over het opstellen en aanscherpen van het informatiebeveiligingsbeleid;
- toezicht houden op het beveiligingsniveau op basis van rapportages over beveiligingsmaatregelen en procedures, controles en incidenten;
- bespreken van beveiligingsincidenten zoals gerapporteerd door de beveiligingsfunctionaris;
- bevorderen van het beveiligingsbewustzijn;
- bespreken van ontwikkelingen die de bedrijfsinformatie (kunnen) bedreigen;

- adviseren over te nemen beveiligingsmaatregelen ter beperking van risico's;
- erop toezien dat de (nog) te nemen maatregelen gerealiseerd worden.

De samenstelling van de beveiligingsadviescommissie is opgenomen in de Bijlage Functieverdeling in het onderdeel Organisatie van het Gemeentelijk Informatiebeveiligingsplan.

Voorzitter van deze commissie is de afdelingsmanager Publiekscentrum.
Secretaris van deze commissie is de beveiligingsfunctionaris.

3.5 Intergemeentelijk overleg OWO-gemeenten

Tussen de drie beveiligingsfunctionarissen van de gemeenten Ooststellingwerf, Weststellingwerf, Opsterland (OWO) vindt regelmatig een overleg plaats over algemene gemeenteoverstijgende onderdelen. Dit in verband met verdergaande samenwerking en samenvoeging van organisatieonderdelen. Het uitgangspunt daarbij is dat zoveel mogelijk wordt gepoogd het algemene informatiebeveiligingsbeleid en bijbehorende informatiebeveiligingsplannen gelijk vast te laten stellen. Uiteraard blijft het informatiebeveiligingsbeleid met bijbehorende informatiebeveiligingsplannen een eigen gemeentelijke verantwoordelijkheid.