duurzaam

Zwolle

Informatievoorziening

14 038
www.zwolle.nl/contact

Informatiebeveiligingsbeleid

2022 - 2026

Opdrachtgever	CISO
Opdrachtnemer	P.A.M. Kluitmans (ISO)
Versie	0.17
Datum	12-09-2022

Datum	12-09-2022
Titel	Informatiebeveiligingsbeleid

Inhoud

Datum 12-09-2022
Titel Informatiebeveiligingsbeleid

Samenvatting

1 Inleiding

1.1 Wat is informatiebeveiliging?

Onder informatiebeveiliging (IB) verstaan we het zorgen voor een bewust en veilig omgaan met informatie door het toepassen van een combinatie van organisatorische en technische maatregelen. Deze maatregelen zijn er op gericht de betrouwbaarheid (beschikbaarheid, integriteit en vertrouwelijkheid) van gemeentelijke processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens aantoonbaar te beschermen tegen onheil. De Baseline Informatiebeveiliging Overheid (BIO) is hiervoor de norm voor standaardisatie binnen de overheid.

De maatregelen borgen de juiste toegankelijkheid van informatie, het opbouwen en onderhouden van het bewustzijn over informatieveiligheid bij de medewerkers, en, in het geval van incidenten, de eventuele gevolgschade (impact) van deze incidenten te beperken. Deze maatregelen staan beschreven in het informatiebeveiligingsplan[1].

IB is breder dan alleen digitale veiligheid. Beschikbare en betrouwbare informatie is essentieel voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van bedrijven en burgers. De bescherming van vertrouwelijke informatie is waar het uiteindelijk om gaat. Dit vereist een integrale aanpak, waarin iedere manager verantwoordelijk is voor de veiligheid en beveiliging van zijn eigen organisatieonderdeel, processen en gegevens.

Leidend voor het organiseren van de informatiebeveiliging in de gemeente zijn de ambities op het gebied van dienstverlening en het optimaal organiseren (kwaliteit) en faciliteren van de bedrijfsvoering. Het informatiebeveiligingsbeleid is het kader voor passende technische en organisatorische maatregelen om informatie te beschermen en te waarborgen, waarmee de gemeente voldoet aan relevante wet- en regelgeving en zodat de dienstverleningsambities en bedrijfsvoering worden gefaciliteerd.

1.2 Doelstelling

De doelstelling van informatiebeveiligingsbeleid is het richting geven aan het inrichten van informatiebeveiliging binnen de gemeente; er worden doelen gesteld, verantwoordelijkheden beschreven, structuur geschetst en bewustwording gecreëerd, waarmee dit beleid moet worden vormgegeven.

Het informatiebeveiligingsbeleid is tevens de basis voor het inrichten van een procesgerichte benadering van informatiebeveiliging, ook wel het Information Security Management System (ISMS) genaamd. Dit proces hanteert een Plan Do Check Act Cyclus (PDCA) en sluit aan bij de Planning en Control (P&C) cyclus van de gemeente. Ook is vanuit het ISMS de mate van compliance af te lezen conform de BIO inclusief bijbehorende beheersmaatregel en bewijslast.

Het informatiebeveiligingsbeleid biedt de uitgangspunten, normen en kaders voor de veiligheid van alle onderliggende gemeentelijke informatieprocessen. Zie bijlage 1. Deze beleidsnota vervangt het in 2018 vastgestelde strategisch informatiebeveiligingsbeleid.

[1] Het informatiebeveiligingsplan is een nadere uitwerking van maatregelen t.b.v. implementatie BIO. Dit plan wordt jaarlijks opnieuw opgesteld.

Informatie is één van de belangrijkste bedrijfsmiddelen van de gemeente. Zonder actuele en betrouwbare informatie, op de juiste plaats en op de juiste tijd, kunnen wij onze taken niet naar behoren en afdoende veilig vervullen. We werken met informatie om diensten te leveren aan onze inwoners en bedrijven, en om richting te geven aan de ontwikkeling van onze gemeente. We zijn open en transparant in wat we doen en waarom we het doen. We helpen onze inwoners en bedrijven ‘in één keer goed’ en voorkomen dat we dezelfde vraag twee keer stellen door goed gebruik van de informatie die wij hebben. Om dit te kunnen doen zien wij informatie als ‘open tenzij’.

Maar met een nadrukkelijke ‘tenzij’, omdat informatie de privacy of belangen van personen of organisaties kan schaden. Het is onze verantwoordelijkheid om deze rechten te beschermen. Zodat iedereen erop kan vertrouwen dat zorgvuldig met zijn/haar gegevens wordt omgegaan en dat privacy gewaarborgd is. Wij zoeken daarbij naar een goede balans tussen de te nemen maatregelen en het behouden van een goede en efficiënte dienstverlening, een transparant proces en acceptabele kosten.

Informatiebeveiliging draag bij aan de doelstelling van de gemeente:

De gemeente Zwolle wil ***een betrouwbare partner*** zijn voor burgers, bedrijven en ketenpartners.

De gemeente zet de komende jaren in op het optimaliseren van de informatieveiligheid en het verder professionaliseren van de informatiebeveiligingsfunctie. Hiermee krijgt het onderwerp prioriteit om de bedrijfscontinuïteit van onze processen en informatie te waarborgen.

1.3 Ambitie en visie

Het is de ambitie om als gemeente Zwolle in de informatiemaatschappij een volwaardige en betrouwbare plek in te nemen, nu en in de toekomst. Om de ambitie te kunnen realiseren zorgen we er voor dat de ambtelijke organisatie op zijn taken is toegerust: de basis is en blijft op orde. Dit betekent dat medewerkers op hun taken zijn toegerust, bijbehorende risico’s onderkennen en de processen, gegevens en systemen op orde zijn.

Persoonlijke en gevoelige gegevens van inwoners worden toevertrouwd aan de lokale overheid. Inwoners en ondernemers moeten erop kunnen vertrouwen dat die informatie bij de lokale overheid in veilige handen is. Het is van essentieel belang dat lokale overheden interne bewustwording creëren over het belang van privacybescherming van privacygevoelige data van inwoners en de impact als deze data op straat komen te liggen.

Een ander thema waarop we willen inzetten is digitale veiligheid. Digitale veiligheid betekent dat medewerkers bewust zijn van de risico’s voor informatieveiligheid en de technische voorzieningen op orde zijn ter voorkoming van cybercriminaliteit, zodat schade door verstoring of uitval van ICT voorkomen wordt.

Een organisatie is digitaal weerbaar als het potentiële dreigingen en incidenten vroegtijdig kan signaleren en de gevolgen ervan kan voorkomen dan wel beperken. Niveau 3 van volwassenheid zou het minimale niveau moeten zijn om dit goed in te vullen (zie bijlage 2).

De dienstverlening verschuift al jaren naar digitaal. De dynamiek van de ’informatiemaatschappij’ plaatst ons ook voor nieuwe opgaven en uitdagingen. Inwoners en ondernemers raken gewend aan de snelheid, efficiëntie en gemak waarmee zij online zaken kunnen regelen in de digitale samenleving, ook bij Zwolle. Zij verwachten van ons dat wij hierin meegaan en onze dienstverlening en bedrijfsvoering hierop aanpassen. Waarbij zij tevens vragen om het borgen van goede randvoorwaarden voor de omgang met de groeiende hoeveelheid data en digitale oplossingen in de ‘slimme samenleving’.

Het is een permanente uitdaging om invulling te geven aan de grotere en snel veranderende vraag naar inzet van ICT. Hierbij zoeken we naar een balans tussen innovatie en continuïteit. Een aanpak die zich kenmerkt door een werkwijze van ‘verbouwen met de winkel open’.

Het is van belang dat bestuur en leiding vanwege hun invloed op de organisatiecultuur zelf in houding en gedrag het belang van privacy en informatiebeveiliging uitdragen. Het hanteren van een duidelijke strategie helpt bij het uitdragen van de boodschap, die met behulp van de in dit document besproken aanpak moet zorgen voor de verankering van het gewenste bewustzijn in de organisatie.

1.4 Leeswijzer

In hoofdstuk 2 zijn de ontwikkelingen voor het inrichten van de informatiebeveiliging weergegeven. In hoofdstuk 3 is de kern van het strategisch beleid uiteengezet. Hoofdstuk 4 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de gemeente belegd zijn, evenals de werking en geldigheidsduur van dit informatiebeveiligingsbeleid. Hoofdstuk 5 gaat in op de bevordering van het beveiligingsbewustzijn.

In de bijlage 1 is een overzicht weergegeven van de hiërarchische structuur tussen de verschillende soorten beleid. In bijlage 2 zijn de volwassenheidsniveaus voor informatiebeveiliging opgenomen. In bijlage 3 is het dreigingsbeeld informatiebeveiliging Nederlandse gemeente uitgewerkt. In bijlage 4 zijn de principes voor informatiebeveiliging (IBD, VNG realisatie) uitgewerkt. In bijlage 5 is de informatiebeveiligingsorganisatie weergegeven. In bijlage 6 is de bronvermelding opgenomen. In bijlage 7 zijn een aantal begrippen nader toegelicht. Tot slot zijn in bijlage 8 de gebruikte afkortingen opgenomen.

2 Ontwikkelingen

De ontwikkelingen in de samenleving en technologie maken dat informatiebeveiliging steeds belangrijker wordt. Onze inwoners en bedrijven willen snel en digitaal geholpen worden. We zien een verschuiving van in huis geïnstalleerde applicaties naar extern gehoste SaaS-oplossingen en webapplicaties. Dataverwerking is meer en meer “in de cloud”, dat wil zeggen bij andere organisaties op de servers die op onbekende plaatsen staan. Ons voorkeur cloud servicemodel gaat uit van een SaaS-oplossing, met als randvoorwaarde dat ze voldoen aan de gestelde informatiebeveiligingseisen van de BIO.

We willen plaats en tijd onafhankelijk werken. Dit heeft het gebruik van meer mobiele apparaten (smartphone, laptop, tablet) tot gevolg, maar ook gevolgen voor de connectiviteit en netwerken. Er worden veel meer gegevens gedeeld in ketens. Bijvoorbeeld in het sociaal domein en de omgevingswetgeving. En tegelijkertijd is er een roep om het beter beschermen van gegevens, met name vertrouwelijke gegevens. De externe digitale dreigingen zoals hacks, ransomware en phishing nemen sinds de coronapandemie explosief toe. Andere ontwikkelingen die van belang zijn voor het verder inrichten van de informatiebeveiliging zijn de volgende:

2.1 Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten geeft een actueel zicht op incidenten en factoren uit het verleden. Het dreigingsbeeld richt zich op de ambtelijke organisatie, het bestuur, de politiek, de inwoners en de ondernemers. De dreigingen zijn uitgewerkt in bijlage 3 en zijn van invloed op de informatiebeveiliging.

2.2 De basis op orde (GGI-veilig)

Met de Gemeentelijke Gemeenschappelijke Infrastructuur (GGI) bouwen gemeenten aan een veilige, samenhangende digitale infrastructuur die samenwerken tussen gemeenten en andere overheden beter, veiliger en gemakkelijker maakt. Eén van de programma’s binnen GGI is GGI-Veilig, bedoeld om de veiligheid en de digitale weerbaarheid te verhogen. GGI-Veilig bestaat uit 3 percelen gericht op detectie, preventie en ondersteuning. We sluiten aan bij het programma van GGI-Veilig (deels via SSC-ONS).

2.3 Common Ground

Met de visie Common Ground leggen gemeenten een basis voor een toekomstgerichte informatievoorziening die gemeenten in staat stelt op een flexibele en moderne manier maatschappelijke vraagstukken, dienstverlening en bedrijfsvoering op te pakken.
Door de gegevenshuishouding volgens de Common Ground principes in te richten is het mogelijk om snel en flexibel te vernieuwen, te voldoen aan privacywetgeving en efficiënt om te gaan met gegevens. We kiezen er voor om Common Ground als leidend inrichtingsprincipe te hanteren.

2.4 Agenda Digitale Veiligheid

In de Agenda Digitale Veiligheid 2020 – 2024 hebben gemeenten gezamenlijk vast gelegd wat het actieplan is om het vertrouwen van inwoners en ondernemers in hun digitale veiligheid te vergroten en vast te houden.

In vier samenhangende thema’s (awareness, governance, risicogericht handelen en één overheid/samen organiseren) zijn tien actielijnen gerubriceerd.

2.5 Applicaties en toepassingen zijn standaard en bewezen

Voor de ondersteuning van de bedrijfsprocessen gebruiken we standaard applicaties die meegroeien met ontwikkelingen. We zetten daarom in op het gebruik van bewezen oplossingen die door meerdere partijen gebruikt worden. Tevens borgen we hiermee de toekomstbestendigheid, omdat we meegroeien met de ontwikkelingen.

2.6 Internet of things (IoT) en smart city

Smart city-projecten dragen bij aan het vergroten van de leefbaarheid en veiligheid binnen de gemeente. Voorheen ‘domme’ objecten, worden slim (IoT) en maken het besturen makkelijker. Bijvoorbeeld een camera die zwerfafval herkent en verkeersmetingen. Maar dit zet ook de informatieveiligheid en privacybescherming verder onder druk.

De IoT-apparatuur en -software die we hiervoor inzetten, zorgt voor meer risico’s en kwetsbaarheden. Zeker als ook de scheiding tussen gemeentelijke ICT en IoT niet goed wordt geregeld, een verouderd camerasysteem in het gemeentelijke netwerk kan dan de ongewilde entree zijn tot gegevens en systemen van de gemeente.

2.7 Artificiële intelligentie

Bij artificiële intelligentie (AI) gaat het om de mogelijkheid (zelfstandig) te leren en beslissingen te nemen. Hiervoor worden bepaalde algoritmen gevolgd. Algoritmen, de ‘recepten’ die de basis vormen voor veel software, zijn niet per definitie neutraal (bijvoorbeeld bij de inzet van Robotic Process Automation (RPA). Nederlandse gemeenten zetten in toenemende mate AI in voor uiteenlopende taken**.** Met AI en de relevante data kunnen we problematische schulden vroegtijdig signaleren, fraudes detecteren en betere diagnoses stellen in de zorg.

Maar AI heeft ook een andere kant. Met de inzet van AI kunnen grondrechten in het gedrang komen. Daarom staan mensenrechten en publieke waarden bij de toepassing en ontwikkeling van deze technologie centraal: AI moet belangrijke waarden – zoals transparantie, non-discriminatie, privacy en veiligheid – borgen en waar mogelijk versterken. Menselijke alertheid en controle is nodig om ongewenste effecten te voorkomen.

2.8 Cyber security

Cybersecurity is het verdedigen van computers, servers, mobiele apparaten, elektronische systemen, netwerken en gegevens tegen schadelijke aanvallen. Methodes die aanvallers gebruiken om de controle te krijgen over computers of netwerken, zijn virussen, wormen, spyware, trojans, phishing, hacken, malware (ransomware), DDos-aanvallen of diefstal van identiteit of informatie, al dan niet via social engineering. De manieren om cyberaanvallen uit te voeren worden groter. Cyber security heeft ook een menselijke component. Daar moeten we aan werken door het bewustzijn en de kennis van de medewerkers te vergroten.

In de huidige digitale wereld is het niet de vraag of een organisatie te maken krijgt met een cyberincident, maar wanneer. Cybercriminelen richten hun pijlen namelijk graag op overheidssystemen, vanwege de enorme hoeveelheid aan persoonlijke gegevens die ze bevatten. We beschermen ons door de computers, netwerken en overige ICT infrastructuur blijvend te voorzien van actuele antispamfilters, virusscanners, malwaredetectie en crypto grafische protocollen en updates en te blijven werken aan het bewustzijn.

3 Strategisch informatiebeveiligingsbeleid

3.1 Uitgangspunten

De gehele gemeentelijke leiding speelt een cruciale rol bij het uitvoeren van dit strategische informatiebeveiligingsbeleid. De leiding maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente heeft, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn.

Op basis hiervan zet de leiding dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

3.1.1 4 pijlers

Het informatiebeveiligingsbeleid kent vier pijlers:

- beschikbaarheid;
- integriteit;
- vertrouwelijkheid;
- controleerbaarheid.

Voor de gemeente is het belangrijk dat informatie **beschikbaar** is wanneer medewerkers en (keten)partners deze nodig hebben om hun taak uit te voeren. En dat burgers en bedrijven over informatie kunnen beschikken om diensten te verlenen of te benutten. Beschikbare informatie moet uiteraard wel **integer** zijn, dus juist en actueel. En **vertrouwelijke** informatie moet voldoende worden beschermd. Tenslotte moeten handelingen en besluiten aantoonbaar en daardoor **controleerbaar** zijn, zodat rapporteren en eventueel auditen mogelijk is.

3.1.2 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

- Het college van B en W is verantwoordelijk voor de goedkeuring van het informatiebeveiligingsbeleid. De gemeenteraad wordt geïnformeerd over dit beleid.
- De gemeentesecretaris is eindverantwoordelijk voor de uitvoering van het beveiligingsbeleid.
- De uitvoering van de informatiebeveiliging is gemandateerd aan het lijnmanagement (afdelingshoofd). Alle informatiebronnen en -systemen die gebruikt worden hebben een interne eigenaar die de vertrouwelijkheid bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Bij samenwerking in ketens, bij uitbesteed werk of in samenwerkingsverbanden blijft de gemeente verantwoordelijk voor de informatiebeveiliging.
- De Baseline Informatiebeveiliging Overheid (BIO) is de basis voor de inrichting van de informatiebeveiliging.
- Binnen het kader van de BIO gaan we voor het beheersen van risico's tegen acceptabele kosten, waarbij we een zorgvuldige en transparante afweging maken van informatiebeveiliging en het recht op privacy versus de gewenste transparantie en het 'in één keer goed' onze diensten kunnen leveren.

- Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit[2] van de informatievoorziening verankerd binnen de gemeente. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan zijn de verbeteracties die we willen oppakken voor een periode van één tot twee jaar, geformuleerd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
- Informatiebeveiliging is een continu verbeterproces dat om toezicht en onderhoud vraagt. Het is een integraal onderdeel van de bedrijfsvoering. ‘Plan, do, check en act’ vormen samen het managementsysteem van informatiebeveiliging.
- We hebben een systeem waarin (beveiligings-)incidenten worden vastgelegd. Dit systeem geeft waardevolle informatie om van te leren. Daarom worden evaluaties van incidenten uit het verleden ook nadrukkelijk gebruikt bij het actualiseren van het beleid. Het is aan de leidinggevenden om deze incidenten bespreekbaar te maken op de eigen afdeling zodat er een verbeterslag kan plaatsvinden en bewustwording kan groeien.
- De benodigde mensen en middelen worden beschikbaar gesteld om de gemeentelijke eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- Medewerkers gaan verantwoord om met persoonsgegevens en andere informatie.
- De informatiesystemen moeten voldoen aan een beschikbaarheid tijdens kantoortijd van minimaal 95%. Buiten kantoortijd zijn er geen beschikbaarheidseisen met uitzondering van voorzieningen in het kader van rampenbestrijding en voor doorlopende processen (handhaving). In het geval van uitval van bedrijfsprocessen en/of informatiesystemen ten gevolge van een calamiteit dient de dienstverlening binnen 48 uur hersteld te zijn.

3.1.3 Invulling uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het college van B en W stelt het strategisch informatiebeveiligingsbeleid vast.
- Het managementteam Zwolle (MTZ) stelt jaarlijks het informatiebeveiligingsplan vast.
- Het MTZ is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- Het MTZ ziet erop toe dat de afdelingshoofden adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de Directie, voorafgaand aan de P&C-gesprekken (begroting, jaarrekening etc.).
- Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportage van de CISO. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen. Regulier stemt de CISO zijn bevindingen af in het 3e - lijn controleoverleg met concern control, Verbijzonderde Interne Controle (VIC) en de Functionaris Gegevensbescherming (FG).
- Hoewel de (basis)registraties (zoals BRP, PNIK, SUWI, BAG, BGT, BRO) belangrijk zijn in het kader van informatiebeveiliging, krijgen de primaire processen binnen de gemeente voorrang.

[2] Kwaliteit betreft de kernpunten van informatiebeveiliging: beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van de informatie.

Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de gemeente en het behalen van de doelen die zijn gesteld.
- De medewerkers die werken met de informatiesystemen van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement (zie paragraaf 3.5). Proceseigenaren (afdelings- of sectiehoofd) voeren een baselinetoets uit om het beveiligingsniveau van het informatiesysteem vast te stellen. Het beveiligingsniveau bepaald het aantal te nemen maatregelen vanuit de BIO. Bij kleinere wijzigingen volstaat een quickscan.

3.1.4 Randvoorwaarden

Randvoorwaarden voor een goede uitvoering van het informatiebeveiligingsbeleid zijn:
- Benodigde capaciteit en middelen worden ter beschikking gesteld.
- Informatiebeveiliging maakt deel uit van afspraken met ketenpartners.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie wordt actief bevorderd en geborgd.
- Jaarlijks wordt een informatiebeveiligingsplan opgesteld onder leiding van de CISO, gebaseerd op:
  - het dreigingsbeeld gemeenten van de Informatiebeveiligingsdienst (IBD);
  - De door de afdelingshoofden ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn;
  - De evaluatie van de (informatiebeveiliging)incidenten.

3.2 Strategische doelen

De strategische doelen van het informatiebeveiligingsbeleid zijn:
- Het managen van de informatiebeveiliging.
- Het minimaliseren van risico’s van menselijk gedrag.
- Het garanderen van betrouwbare en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op en afhandelen van incidenten.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Het waarborgen van de naleving van dit beleid.

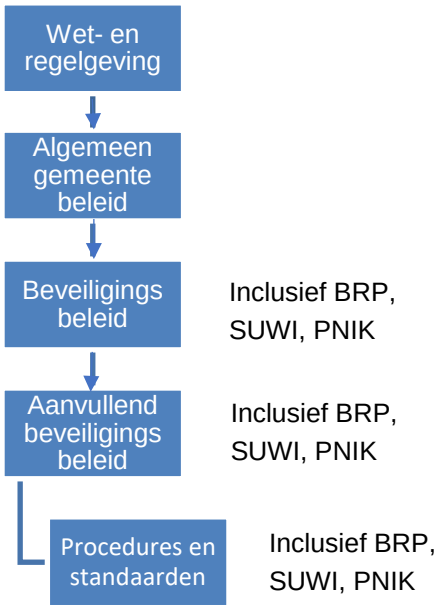
3.3 Scope

Dit beleid is van toepassing op de gehele organisatie, alle processen, objecten, informatiesystemen, gegevens(verzamelingen) en externe partijen ((keten)partners). Het borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het politieke bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties. Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

Bij deze samenwerking is sprake van uitwisseling van informatie, waarvan de gemeente eigenaar of beheerder is. Informatiebeveiliging dient onderdeel te zijn van de samenwerkingsovereenkomst en deze mag niet strijdig zijn met het informatiebeveiligingsbeleid van de gemeente. Bijzondere aandacht is er voor de samenwerking met het Shared Service Centrum (SSC) ONS, dat ICT-taken voor de gemeente uitvoert en voor Dimpact dat bijvoorbeeld het zaaksysteem (e-Suite) voor de gemeente heeft ingekocht.

Dit strategisch Informatiebeveiligingsbeleid is een algemene basis. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld voor de Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), de gemeentelijke basisregistraties en de beveiligingsnorm DigiD). Deze worden in aanvullende documenten geformuleerd.

Bewust wordt in dit beleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar dit strategisch beleid gelegd. In onderstaande figuur is een overzicht gegeven van de samengevoegde eisen in één set beleidsdocumenten.



3.4 Baseline Informatiebeveiliging Overheid

Vanaf 1-1-2020 is de Baseline Informatiebeveiliging Overheid (BIO) van toepassing voor alle overheidsinstellingen en dus ook voor de gemeente Zwolle. De BIO is de standaardnorm voor de informatiebeveiliging. Actueel is versie 1.04. Gemeenten baseren hun informatiebeveiligings-beleid en hun verantwoording aan de gemeenteraad en de toezichthouders vanuit het Rijk (middels ENSIA) op deze BIO. Eind 2021 is een nulmeting over de organisatie van de informatiebeveiliging door een extern bureau uitgevoerd. Deze nulmeting dient als leidraad om de informatiebeveiliging verder op orde te krijgen.

3.4.1 De 10 principes voor informatiebeveiliging

De VNG heeft 10 principes voor informatiebeveiliging opgesteld. Deze principes zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder/manager zichzelf oplegt. Deze principes ondersteunen de manager bij de verantwoordelijkheid voor goed risicomanagement. Het is aan de manager om de risicobereidheid te bepalen en daarmee ook te controleren of de maatregelen binnen de organisatie de risico's terugbrengen tot een voor de bestuurder acceptabel niveau. Overschrijding van dat niveau vereist expliciete besluitvorming.

De principes zijn als volgt:

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

De principes zijn uitgewerkt in bijlage 4.

3.5 Risicobenadering

Het invoeren van maatregelen gebeurt vanuit een risicobenadering: de effecten van de maatregelen moeten in verhouding staan tot de noodzakelijke beveiliging. Informatiebeveiliging is immers risicomanagement. De BIO heeft als doel het lijnmanagement bruikbare handvatten te geven bij het afdekken van risico's met betrekking tot informatiebeveiliging.

De proceseigenaar (afdelings- of sectiehoofd) bepaalt welke maatregelen genomen moeten worden op basis van een risicoanalyse, waarbij de kans en het effect (impact) het risico bepalen. De door de proceseigenaar gemaakte risicoafweging, tussen enerzijds het risico en anderzijds de kosten en consequenties van de maatregelen conform de beschermingseisen, wordt vastgelegd in het risicoregister door het invullen van een Risico Acceptatie Overeenkomst (RAO), evenals de te treffen maatregelen.

Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen gebruiken we beveiligingsclassificaties. Deze geven aan welk beschermingsniveau noodzakelijk is voor welke proces en/of informatiesysteem, en maakt duidelijk welke maatregelen genomen moeten worden. Het beschermingsniveau is gebaseerd op de classificatie van data.

Het Nationaal Cyber Security Centrum (NCSC) heeft een aantal maatregelen gepubliceerd die helpen cyberaanvallen tegen te gaan. Deze maatregelen ondersteunen het risicomanagement, maar komen er niet voor in de plaats.

3.6 Werking en geldigheidsduur

Strategisch beleid moet volgens de BIO-eisen minimaal om de 4 jaar worden herzien. De aanvullende beleidsdocumenten kunnen aangepast worden wanneer dat nodig is. Voor de

beoordeling en bijstelling van procedures wordt geen termijn gegeven, in de praktijk zullen deze vaker wijzigen.

3.7 Relevante wet- en regelgeving

De wettelijke basis van informatieveiligheid valt af te leiden uit Europese richtlijnen en landelijke wet- en regelgeving, zoals (niet uitputtend):

- Auteurswet;
- Telecommunicatiewet;
- Ambtenarenwet;
- Wet computercriminaliteit;
- Wet op de jaarrekening;
- Algemene verordening gegevensbescherming (AVG);
- Archiefwet / Archiefregeling;
- Beveiligingsnorm DigiD;
- eIDAS-verordening;
- Wet elektronisch bestuurlijk verkeer;
- Wet elektronische handtekeningen;
- Wet algemene bepalingen Burgerservicenummer;
- Wet Politie Gegevens (WPG)
- Paspoortwet (Paspoort Uitvoeringsregeling Nederland (PUN));
- Wet basisregistratie personen (Wet BRP);
- Wet openbaarheid van bestuur (Wob) (vanaf 2022 vervangen door de Wet open overheid (Woo));
- Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI);
- Wet Basisregistratie Adressen en Gebouwen (BAG);
- Wet Basisregistratie Grootschalige Topografie (BGT);
- Wet Basisregistratie Ondergrond (BRO);
- Wet op de ruimtelijke ordening (Wro).
- Wet hergebruik van overheidsinformatie (Who)

Op grond van bovenstaande wet- en regelgeving worden er eisen gesteld aan het niveau van informatieveiligheid, de beheersmaatregelen en de controle (interne audit) daarop.

Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

Onderstaande wetten zullen in de komende jaren invloed hebben op de informatiebeveiliging.

3.7.1 Wet Digitale Overheid (WDO)

De maatschappij verandert steeds meer in een informatie- en netwerksamenleving. De Wet digitale overheid is gericht op het verbeteren van de digitale overheid door standaarden voor elektronisch verkeer verplicht te stellen. Ook geeft het regels over informatieveiligheid en over de toegang van burgers en bedrijven tot online dienstverlening bij de (semi)overheid. Begin 2020 is de wet aangenomen door de Tweede Kamer. Behandeling in de Eerste Kamer heeft geleid tot aanpassingen in de wetgeving, waardoor de herziene wet (novelle) opnieuw is aangeboden aan de Tweede Kamer in juni 2021, waar het tot op heden in behandeling is.

De Wet digitale overheid (WDO) heeft als doel het regelen van het veilig en betrouwbaar kunnen inloggen voor Nederlandse burgers en bedrijven bij de (semi-)overheid. Met veilig en betrouwbaar inloggen wordt bedoeld dat burgers elektronische identificatiemiddelen (eID) krijgen met een hogere mate van betrouwbaarheid dan het huidige DigiD. Deze identificatiemiddelen geven publieke dienstverleners meer zekerheid over iemands identiteit. De wet stelt daarnaast open standaarden verplicht. Hiermee implementeert Nederland de EU richtlijn over toegankelijkheid van overheidswebsites en apps.

3.7.2 Wet modernisering elektronisch bestuurlijk verkeer (Wmebv)

De wet elektronisch bestuurlijk verkeer regelt dat burgers en bedrijven het recht krijgen om elektronisch zaken te doen met de overheid. Degenen die dat willen, moeten een digitale kanaal kunnen kiezen voor hun contact met de overheid. Om te waarborgen dat iedereen met de overheid kan (blijven) communiceren, is het belangrijk dat communicatie op papier mogelijk blijft. Medio 2022 wordt naar verwachting de Wet modernisering elektronisch bestuur ingevoerd.

4 Organisatie

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de gemeente. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD).

Het college van B&W stelt middels het informatiebeveiligingsbeleid de kaders voor de organisatie en geeft hiermee richting aan de uitvoering van taken. Het managementteam stuurt de organisatie in de door het college aangegeven richting.

Afdelingshoofden zijn als eigenaar verantwoordelijk voor de praktische uitvoering ervan binnen hun processen en systemen. Leidend hierbij zijn de maatregelen uit de BIO, in specifieke gevallen aangevuld met richtlijnen vanwege Suwinet, DigiD, PNIK, BRP of andere basisregistraties. Bij het vervullen van deze rol ontvangen zij richtlijnen en ondersteuning van de CISO en de adviseurs informatiebeveiliging (ISO's). In een aantal gevallen benoemd de organisatie specifieke functionarissen ter ondersteuning van de uitvoering van informatiebeveiliging. Denk bijvoorbeeld aan de Security Officer Suwinet. De organisatie van de informatiebeveiliging is opgenomen in bijlage 5.

4.1 Aansturing: het managementteam

Het managementteam (MTZ) zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een afdelingshoofd. Het MTZ zorgt dat de afdelingshoofden zich verantwoorden over de beveiliging van de informatie die onder hen berust. De Directie zorgt dat de verantwoordelijke portefeuillehouder binnen het college gevraagd en ongevraagd geïnformeerd wordt over de mate waarin informatiebeveiliging een onderdeel is van het handelen binnen de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.

Het MTZ stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. Het MTZ draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO van de gemeente. Het MTZ autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging zien we als een integraal onderdeel van risicomanagement. Voordat IB-onderwerpen worden voorgelegd aan het MTZ worden ze eerst besproken in het MT-IV.

4.2 Uitvoering: de afdelingshoofden

Informatiebeveiliging (IB) valt onder de verantwoordelijkheden van alle afdelingshoofden. IB behoort tot de primaire taken. Om deze verantwoordelijkheid waar te maken worden zij ondersteund door ambassadeurs IB, het ISMS en vanuit de tweede lijn. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal één eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn.

Afdelingshoofden rapporteren aan het MTZ over de onder hun verantwoordelijkheid uitgevoerde informatiebeveiligingsactiviteiten en risico's. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging te bespreken in het afdelingsoverleg. Voorbereiding en coördinatie van dit afdelingsoverleg ligt bij de CISO.

Taken van de afdelingshoofden in het kader van informatiebeveiliging zijn:

- Uitvoeren van de periodieke baselinetoets van alle processen (systemen) waarvoor het afdelingshoofd verantwoordelijk is.
- Het vaststellen van het basisbeveiligingsniveau (BBN) dat van toepassing is voor het betreffende proces.
- Het leveren van input voor wijzigingen op maatregelen en procedures op basis van geconstateerde risico's uit de baselinetoets.
- Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid en de daaraan gerelateerde procedures.
- Het signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

4.2.1 Samenwerkingspartners en leveranciers

Voor de uitvoering van bepaalde ICT-taken vallen we terug op samenwerkingspartners of leveranciers. Onze belangrijkste ICT-leverancier is het Shared Service Centrum ONS (SSC ONS). Het SSC ONS heeft het mandaat om producten vanuit GGI-Veilig af te nemen en in te zetten.

4.3 Controle en verantwoording

Dit strategisch beleid is een verantwoordelijkheid van het bestuur van de gemeente Zwolle. De bestuurders en managementteam van de gemeente Zwolle zullen volgens de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.

Het informatiebeveiligingsbeleid wordt uitgewerkt in het informatiebeveiligingsplan. Het informatiebeveiligingsplan is een compact actieplan. Dit vormt de praktische leidraad voor de te implementeren maatregelen van de Baseline Informatiebeveiliging Overheid door de beveiligingsorganisatie onder verantwoordelijkheid van de CISO. Naast het formuleren van specifieke verbeteracties worden onder andere de uitvoerders, de kosten en de planning in het informatiebeveiligingsplan vastgelegd.

Om de voortgang van de implementatie van de informatiebeveiliging te monitoren zijn een viertal structurele rapportages opgezet. Daarnaast zal in geval ven kritische IB incidenten of crisis apart worden gerapporteerd.

Rapportage	Frequentie	Doel	Verantwoordelijk
Bedrijfsvoering rapportage	Halfjaarlijks	Bedrage aan P&C cyclus	Directie
IB rapportage	Kwartaal	Voortgang implementatie BIO	CISO
ENSIA	Jaarlijks	Verantwoording	College B&W
Jaarverslag	Jaarlijks	Voortgang informatiebeveiliging	College B&W
Incidentele rapportage	Incidenteel	Incident- en crisismanagement	CISO

4.3.1 Eenduidige Normatiek Single Information Audit (ENSIA)

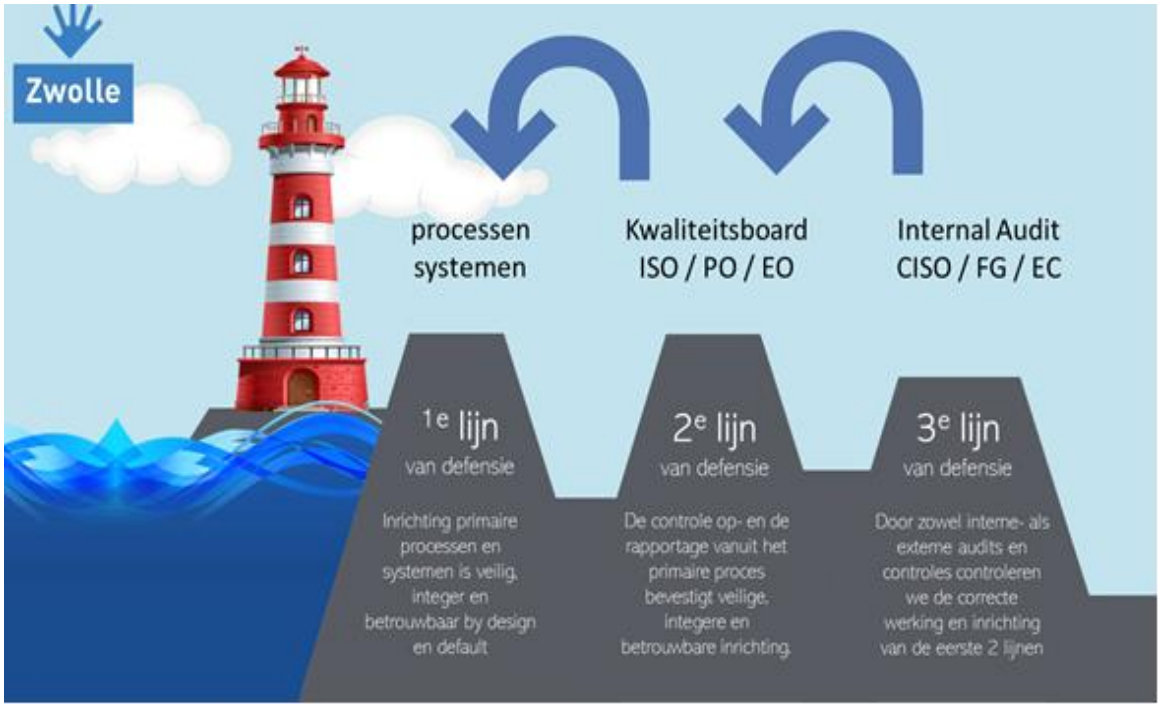
Het college van B&W verantwoordt zich, middels de collegeverklaring DigiD en Suwinet via de ENSIA-systematiek. Tevens stelt zij de verantwoordingsrapportages vast van de basisregistraties BAG, BGT, BRO en WOZ. Jaarlijks wordt een ENSIA-coördinator aangewezen. De ENSIA-coördinator begeleidt dit traject en onderhoudt de contacten met de auditor. Dit proces heeft een jaarlijkse deadline en kent geen vrijblijvend karakter.

4.3.2 Jaarverslag

In het jaarverslag van de gemeente is een paragraaf opgenomen over informatiebeveiliging. In deze paragraaf wordt over de voortgang op het gebied van informatiebeveiliging gerapporteerd. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen.

4.4 Governance

De governance voor informatiebeveiliging is gebaseerd op het ‘three lines of defence’ (3LoD) model. In dit model is het lijnmanagement verantwoordelijk voor de eigen processen. De tweede lijn (security en privacy officers) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor, de CISO en FG van een objectief oordeel voorzien met mogelijkheden tot verbetering.



Functie	Rol	Grondslag	3-LoD
College B & W	Stelt kaders, richting en beleid vast	Bestuurlijk verantwoordelijk	Bestuur
Gemeentesecretaris	Ambtelijk portefeuillehouder IB	Gemandateerd bestuurlijk verantwoordelijk	Bestuur
Lijnmanager (afdelingshoofd)	Lijnverantwoordelijk bedrijfsproces (domein)	Lijnverantwoordelijk	1e lijn
ISO	Tactisch en operationeel IB	BIO	2e lijn
CISO	Strategisch IB, onafhankelijk, toetsende en toezichthoudende rol	Strategische organisatie, toetsing en toezicht BIO	3e lijn
Verbijzonderde Interne Controle (VIC)	Interne controle	P&C cyclus	3e lijn
SSC ONS	Externe ICT leverancier	IT continuïteit	Extern

5 Bevordering beveiligingsbewustzijn

5.1 Inleiding

Naast het kunnen beschikken over de juiste middelen, vraagt informatiebeveiliging om een bewuste houding en gedrag:

- bewust van de kansen die digitaal werken biedt voor burgers en bedrijven;
- bewust van de risico's ten aanzien van vertrouwelijke en persoonlijke gegevens, waarmee die kansen worden gerealiseerd;
- bewust van de middelen die de organisatie aanbiedt om de kansen veilig te benutten.

Een bewuste houding ontstaat niet vanuit het niets. Medewerkers worden geïnformeerd over de aanwezigheid van ondersteunende middelen en hoe deze praktisch en veilig benut kunnen worden. Daarnaast krijgen de medewerkers informatie over de mogelijke bedreigingen waar onze informatiehuishouding tegenwoordig aan blootstaat. Uiteraard wordt geleerd hoe deze bedreigingen het hoofd kunnen worden geboden.

Bewustwording wordt vaak gemeten in een volwassenheidsniveau ook wel maturity-level genoemd. Vanuit het gewenste jaarlijkse volwassenheidsniveau worden de benodigde maatregelen ingezet om het niveau te bereiken, in samenwerking met de interne stakeholders HR en Communicatie.

De maturity-levels zien er als volgt uit:

Jaar	2021	2022	2023	2024
Maturity-levels	Organisatie is zich bewust van de risico's van informatie-verwerking.	Organisatie is reactief bezig met de bescherming en verwerking van informatie.	Organisatie is proactief bezig met de bescherming en verwerking van informatie.	Organisatie heeft het beschermen en verwerken van informatie geïnternaliseerd.

Op de verschillende niveaus worden specifieke workshops ontwikkeld waarin genoemde vaardigheden in relatie tot de gevraagde huidige competentie (bijvoorbeeld cybersecurity), onder de aandacht komen van betreffende doelgroep.

We willen het bewustzijn laten groeien van onbewust onbekwaam naar onbewust bekwaam.

5.2 Doelgroepen

Niet alle delen van het informatiebeveiligingsbeleid zijn voor iedereen even relevant. We onderscheiden verschillende doelgroepen:

1. Medewerkers die werken met de informatiesystemen.
2. Managers, leidinggevenden en bestuurders.
3. Beheerders (technisch en functioneel beheerders).

5.2.1 Medewerkers

Door het plaatsen van berichten over informatiebeveiliging op het intranet en het houden van een bewustwordingscampagne geven we invulling aan het informeren van de medewerkers. Het is de verantwoordelijkheid van iedere medewerker om de aangeboden kennis tot zich te nemen en toe te passen.

Doel: elke medewerker weet wat informatiebeveiliging en privacy inhoudt en is zich ervan bewust dat hij/zij een duidelijke eigen verantwoordelijkheid heeft. Zowel in het zelf veilig omgaan met en uitwisselen van informatie, als in het melden van (informatiebeveiliging)incidenten.

5.2.2 Managers, leidinggevenden en bestuurders

Sturen op veilig gedrag, naast sturen op snel, efficiënt en kosteneffectief werken, vergt doorlopende aandacht van de leiding. Geen medewerker wil een datalek, hack of storing veroorzaken. Toch gebeurt dat af en toe wel omdat de beschikbare middelen niet aansluiten bij de behoefte van medewerkers of men niet wordt beoordeeld op veilig gedrag. Het is zaak een digitale veiligheidscultuur te cultiveren waarin veilig werken beloond wordt, medewerkers niet schromen om onveilige situaties te melden en waarin onveilige situaties ook daadwerkelijk worden voorkomen of verholpen.

Het is aan de leidinggevenden om de professionele houding van de medewerkers te ondersteunen en waar nodig te stimuleren. Daarbovenop is het aan de leidinggevenden om keuzes te maken, want alle risico's 100% afdichten is een utopie. Het is belangrijk om informatiebeveiligingsincidenten te bespreken, te evalueren en waar nodig het proces bij te stellen.

5.2.3 Beheerders

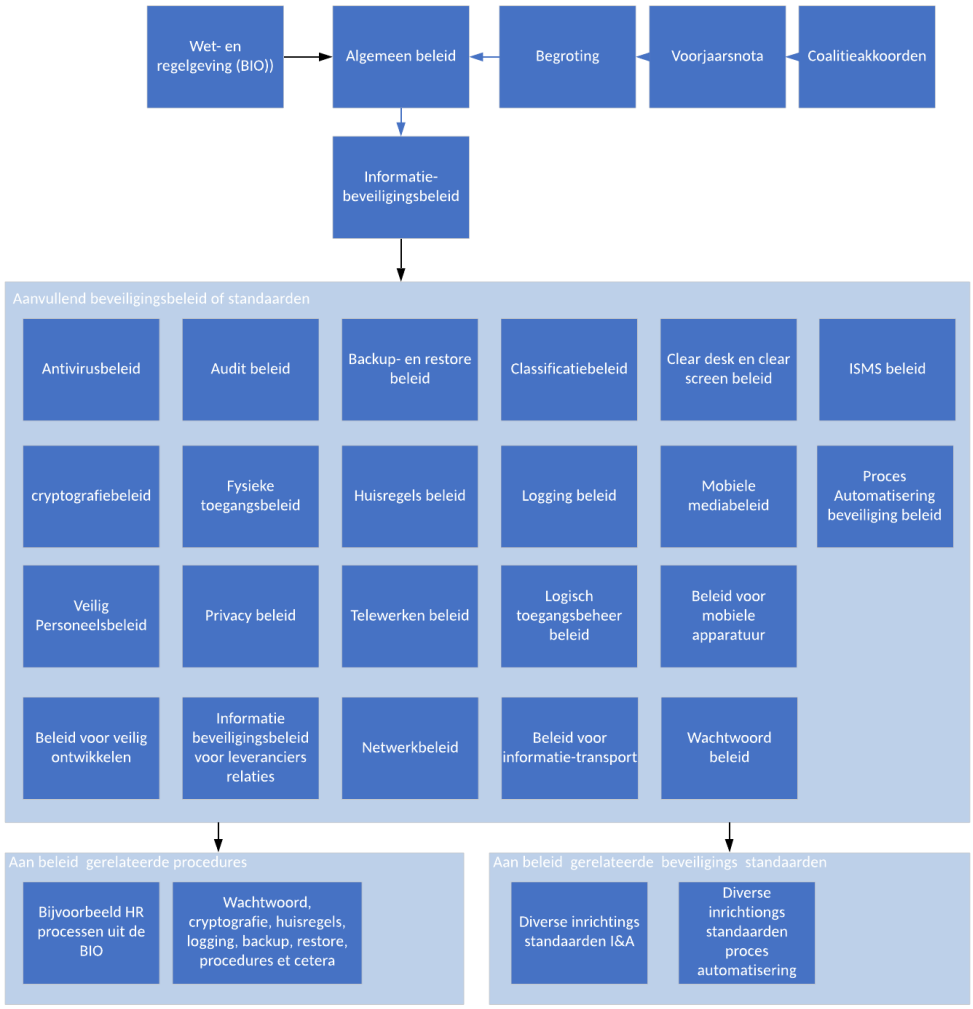
Specifieke aandachtspunten voor de beheerders zijn:

- De bijzondere positie van de beheerder en de risico's.
- Omgang met beheerdersaccounts en wachtwoorden.
- Beheren op afstand.
- Bedrijfscontinuïteit.
- Privacy.
- IT-beveiligingsprocessen en procedures zoals incidentmanagement, CMDB, wijzigingsbeheer, et cetera.

Bijlagen

Bijlage 1: Uitwerking structuur beveiligingsbeleid

Een aanpak is het ‘kapstokmodel’. Vanuit de kapstok, het overkoepelend strategisch informatiebeveiligingsbeleid, volgt aanvullend beleid per BIO-thema, proces of zelfs informatiesysteem. Dit heeft ook voordelen voor de onderhoudbaarheid van het beleid; de kans dat alle beleidsdocumenten gewijzigd moeten worden is immers niet zo groot. Als dit grafisch wordt weergegeven ziet het er op basis van de baseline BIO als volgt uit:



Figuur 1: structuur van beveiligingsbeleid

Bijlage 2: Volwassenheidsniveaus informatiebeveiliging

Volwassenheidsniveau 1	Volwassenheidsniveau 2	Volwassenheidsniveau 3	Volwassenheidsniveau 4	Volwassenheidsniveau 5
Initieel	**Herhaalbaar**	**Gedefinieerd**	**Beheerst en meetbaar**	**Continu verbeteren**
Beheersingsmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.	Beheersingsmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd.	Beheersingsmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst.	De effectiviteit van de beheersingsmaatregelen wordt periodiek geëvalueerd.	De beheersingsmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering.
• Geen of beperkte controls geïmplementeerd. • Niet of ad-hoc uitgevoerd. • Niet /deels gedocumenteerd. • Wijze van uitvoering afhankelijk van individu.	• Control is geïmplementeerd. • Uitvoering is consistent en standaard. • Informeel en grotendeels gedocumenteerd.	• Control gedefinieerd o.b.v. risico assessment. • Gedocumenteerd en geformaliseerd. • Verantwoordelijkheden en taken eenduidig toegewezen. • Opzet, bestaan en effectieve werking aantoonbaar. • Rapportage van uitvoering van beheersingsmaatregel aan management. • Effectieve werking van controls wordt periodiek getoetst, gebaseerd op het risicoprofiel van de organisatie. • De toetsing toont aan dat de control effectief is.	• Periodieke (control) evaluatie en opvolging vindt plaats. • Evaluatie is gedocumenteerd en geformaliseerd. • Frequentie waarop wordt geëvalueerd is gebaseerd op het risicoprofiel van de onderneming en is minimaal jaarlijks. • Rapportage van de evaluatie aan management.	• Continu evalueren van de beheersingsmaatregelen om de effectiviteit te verbeteren. Gebruik makend van resultaten uit Self-assessment, gap en root cause analyses. • De getroffen beheersingsmaatregelen worden gebenchmarkt en zijn 'Best Practice' in vergelijking met andere organisaties. • Real time monitoring. • Inzet automated tooling.

Bijlage 3: Uitwerking dreigingsbeeld informatiebeveiliging Nederlandse gemeenten

De gemeentelijke informatievoorziening is kwetsbaar. We onderscheiden daarin een aantal categorieën van dreigingen in volgorde van belangrijkheid.

Intern en onbedoeld
In de eerste plaats zijn er dreigingen door onbedoelde neveneffecten van logisch menselijk handelen. Medewerkers van gemeenten doen hun best om het werk snel, efficiënt en kwalitatief goed te doen. Bureaucratie is ‘uit’ en ondernemerschap is ‘in’. De kortste weg naar het resultaat is er vaak één met valkuilen. Voorbeelden van dergelijke dreigingen zijn e-mails met gevoelige gegevens aan de verkeerde geadresseerde, verloren USB-sticks en het per ongeluk wissen van bestanden.

Extern, bedoeld maar ongericht
Verreweg het grootste deel van de incidenten vanuit een externe actor komt voort uit geautomatiseerde bulkaanvallen. Kwaadwillenden scannen het internet af op bekende zwakheden in hard- en software, proberen veelvoorkomende gebruikersnaam-wachtwoordcombinaties of sturen honderdduizenden phishing-berichten aan elk adres dat ze tot hun beschikking hebben. Gemeenten zijn dan gewoonweg het slachtoffer omdat ze aangesloten zijn op het internet, doorgaans niet omdat ze de Nederlandse overheid zijn. De gevolgen van ongerichte aanvallen kunnen groot zijn: de meeste aanvallen met gijzel-software zijn in eerste instantie ongericht. Het komt voor dat buitgemaakte inloggegevens van ongerichte aanvallen worden aangeboden aan de hoogste bieder. In zo’n geval kan een ongerichte aanval het opstapje vormen voor een gerichte aanval.

Extern, bedoeld en gericht
Veel aandacht gaat uit naar gerichte dreigingen van hackers en criminelen. Dit fenomeen levert spannende verhalen op in de media. Dit zijn tevens de gevallen die we maar heel moeilijk kunnen ontdekken en die we relatief weinig tegenkomen. Een dergelijke gerichte aanval start vaak met onderzoek door de hacker naar informatie die kan worden gebruikt bij een hack. Op sociale media zoals LinkedIn is veel op het oog onschuldige zakelijke informatie te ontdekken waar een kwaadwillende zijn voordeel mee kan doen. De wat meer gesloten bronnen leveren nog meer informatie op. Er circuleren lijsten met miljarden gestolen gebruikersnamen en wachtwoorden van eerdere hacks. De IBD krijgt meldingen van doelgerichte inlogpogingen op systemen of gerichte phishingmails met een keurige aanhef en een plausibele aanleiding met het doel om geld of (inlog) gegevens buit te maken. Digitaal vandalisme zoals het platleggen van websites scharen we ook onder deze dreigingscategorie.

Intern en bedoeld
De meest riskante dreiging komt van binnen de organisatie. Medewerkers met kwade bedoelingen kunnen uit hoofde van hun functie bij veel gegevens en systemen. Vooral medewerkers met verhoogde toegangsrechten zoals ICT-beheerders en management kunnen grote schade aanrichten. Deze dreiging is nog moeilijker te ontdekken. Interne medewerkers kennen de interne processen en controlemechanismen en kunnen die daarom beter omzeilen dan iemand van buiten.

We weten niet wat we niet weten

Het feit dat er in een gemeente weinig of geen incidenten lijken te zijn, hoeft niet te betekenen dat er niets gebeurt. Besef dat er in elke organisatie incidenten zijn. Als de directie en de leiding die niet kennen, dan is dat zorgelijk. Het boven tafel krijgen van incidenten vereist een open cultuur waarin medewerkers zich vrij voelen om situaties te melden. Daarnaast is er ook een technische component: systematisch in de gaten houden wat er gebeurt in de gemeentelijke systemen, afwijkingen herkennen en hier vervolgens adequaat op reageren.

Bijlage 4: Uitwerking principes voor informatiebeveiliging

Gemeenten wisselen op alle beleidsterreinen informatie uit en beheren dat op vele manieren, zowel binnen de eigen organisatie, maar ook daarbuiten. Als professionele organisatie past hierbij dat we ook de beveiliging van informatie adequaat organiseren. Informatie moet immers beschikbaar, actueel, volledig en betrouwbaar zijn en mag alleen door bevoegden zijn in te zien. Bij de uitwisseling moeten we te allen tijde rekening houden met beveiligings- en privacyaspecten omdat ze een maatschappelijke en wettelijke verantwoordelijkheid[3] heeft om de gegevens van de inwoners onder alle omstandigheden te beschermen.

De principes gaan vooral over de rol van het management bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen de manager bij de verantwoordelijkheid voor goed risicomanagement. Het is aan de manager om de risicobereidheid te bepalen en daarmee ook te controleren of de maatregelen binnen de organisatie de risico's terugbrengen tot een voor de bestuurder acceptabel niveau. Overschrijding van dat niveau vereist expliciete besluitvorming.

Risicomanagement staat daarmee aan de basis van informatiebeveiliging. Er dient een continu proces van identificatie en beoordeling van risico's plaats te vinden om te bepalen wat nodig is om informatie adequaat te beschermen. Hierbij moet worden opgemerkt dat het risico *nul* niet bestaat en dat het aan het bestuur is om te bepalen hoeveel of welk risico acceptabel is. En de risico's zijn talrijk: privacy schendingen door een datalek, economische schade door het uitlekken van vertrouwelijke plannen, fysieke schade door storingen in systemen in de openbare ruimte.

Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

Bestuurlijke aanvulling op de normen en regels
De principes gaan over waarden die de bestuurder/manager zichzelf oplegt. Deze waarden zijn verbonden aan de waarden van de organisatie. Informatiebeveiliging creëert waarde, voorkomt schade en draagt bij aan de bedrijfsdoelstellingen van de organisatie.

Om dat te bewerkstelligen zijn de volgende principes belangrijk:

1 Bestuurders bevorderen een veilige cultuur

Menselijk gedrag en cultuur beïnvloeden op significante wijze alle aspecten van risicomanagement op elk niveau en in elk stadium. Zonder open cultuur waar iedereen vrij is om te spreken is het niet goed mogelijk om risico's te identificeren en als de risico's niet bekend zijn, kunt u ze ook niet adresseren. Als de organisatie een cultuur bevordert waarin mensen zich vrij voelen om risico's te melden en maatregelen voor te stellen, dan kunnen we adequaat reageren op dreigingen en samenhangende risico's.

[3] O.a. de Algemene Verordening Gegevensbescherming (AVG), Wet BRP, PUN, DigiD, BAG, BGT en SUWI

2 Informatiebeveiliging is van iedereen

Passende en tijdige betrokkenheid van belanghebbenden maakt het mogelijk dat hun kennis, opvattingen en percepties in aanmerking worden genomen. Dit resulteert in een verbeterd bewustzijn en goed geïnformeerd risicomanagement.

Iedereen moet betrokken worden bij risicomanagement, in alle lagen van de organisatie. Maak gebruik van de kennis en verantwoordelijkheid van proces- en systeem eigenaren. Gebruik de (Chief) Information Security Officer ((C)ISO), Functionaris Gegevensbescherming (FG) en Verbijzonderde Interne Controle (VIC) als onafhankelijke adviseur

Laat uw interne communicatie aandacht besteden aan het verspreiden van de boodschap, het belang en het voordeel van risicomanagement binnen de organisatie. Goed uitgevoerd risicomanagement creëert waarde voor de organisatie omdat de kwaliteit van besluiten toeneemt en de kans op falen afneemt.

3 Informatiebeveiliging is risicomanagement

Risicomanagement wordt bewust toegepast bij alle organisatie-activiteiten. Risicomanagement werkt alleen als het geïntegreerd is in alle werkprocessen van de organisatie. Dat kan alleen bereikt worden als risico's regelmatig op de agenda staan en als risico's een plek/paragraaf krijgen in alle bestuurlijke documenten. Maak lijnmanagers verantwoordelijk voor risicomanagement door afspraken met ze te maken over uw risicobereidheid. Lijnmanagers zijn verantwoordelijk voor de maatregelen en rapportage daarover.

4 Risicomanagement is onderdeel van de besluitvorming

Risicomanagement is onderdeel van alle besluiten en risicomanagement is 'chefsache'. U kunt als bestuurder alleen de juiste richting aangeven als informatie u bereikt. Door dreigingen en risico's mee te nemen in de vragen die u stelt aan uw managers kunt u er in uw beslissingen ook rekening mee houden. Zo kunt u bijsturen voordat risico's manifest worden en escalatie voorkomen.

5 Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking

Het risicomanagementproces moet passen bij de organisatie en ondersteunen aan de organisatiedoelstellingen. De keten is zo sterk als de zwakste schakel. De gemeente dient met ketenpartners en leveranciers regelmatig het gesprek te voeren over risico's en de maatregelen die ervoor zorgen dat de risico's tot een acceptabel niveau worden teruggebracht.

6 Informatiebeveiliging is een proces

Risico's kunnen ontstaan, veranderen of verdwijnen als de externe en interne context van een organisatie verandert. Risicomanagement detecteert en anticipeert op die veranderingen en gebeurtenissen op een gepaste en tijdige manier.

Risicomanagement moet een cyclisch, iteratief en terugkerend proces zijn, want dreigingen veranderen, doelstellingen veranderen, de omgeving verandert en wetgeving verandert. Indien u in uw risicomanagement geen rekening houdt met een veranderende omgeving, dan zijn uw maatregelen op termijn wellicht niet doeltreffend of doelmatig.

7 Informatiebeveiliging kost geld

Risico's moeten behandeld worden en er zijn vele manieren om veiligheid te realiseren, maar aan alle zijn kosten verbonden.

Risico's kunt u ontwijken, mitigeren, overdragen of wegnemen door het nemen van preventieve-, repressieve-en/of correctieve maatregelen. Welke strategie u ook kiest, ze kosten allemaal middelen in termen van tijd en geld. Voor maatregelen kan derhalve een kosten-batenanalyse worden gemaakt.

8 Onzekerheid dient te worden ingecalculeerd

De input voor risicomanagement is gebaseerd op historische en actuele informatie, evenals op toekomstige verwachtingen. Risicomanagement houdt expliciet rekening met eventuele beperkingen en onzekerheden die aan dergelijke informatie en verwachtingen zijn verbonden. Informatie moet tijdig, duidelijk en beschikbaar zijn voor relevante belanghebbenden.

Zonder goede informatie kunt u geen goede risico-inschattingen en besluiten nemen. Zonder goede en tijdige informatie bent u niet bekend met de risico's die uw organisatie loopt.

9 Verbetering komt voort uit leren en ervaring

Risicobeheer wordt voortdurend verbeterd door leren en ervaring.

Risicomanagement gedijt het beste in een organisatie die leert van ervaringen en op basis hiervan verbeteringen doorvoert. Hoe goed de informatiehuishouding ook beveiligd is, incidenten zullen altijd voorkomen. Door te zoeken naar verbeterpunten en de wil om te leren bouwt u doorlopend aan het verhogen van uw digitale weerbaarheid.

10 Het bestuur controleert en evalueert

Risicomanagement is het controleren en evalueren van resultaten, evenals het nemen van eindverantwoordelijkheid en het doorhakken van lastige knopen.

Controle is belangrijk om goed inzicht te krijgen in de mate waarin het informatiebeveiligingsbeleid en risicomanagement ingebed zijn in de organisatie. Naast verslagen en managementrapportages zijn incidenten, en dan vooral de manier waarop ze afgewikkeld worden, een goede graadmeter om te zien hoe de organisatie omgaat met het onderwerp. Medewerkers kunnen erop vertrouwen dat besluiten op bestuursniveau genomen worden, wanneer de situatie daar om vraagt.

Bijlage 5: Informatiebeveiligingsorganisatie

5.1 Functionarissen en hun rol ten aanzien van informatiebeveiliging

Chief Information Security Officer (CISO)

De CISO is verantwoordelijk voor het geheel van informatiebeveiliging en legt hierover verantwoording af aan de Directie en het college; geeft opdracht tot het formuleren van beleid en het implementeren daarvan binnen de lijnprocessen; is verantwoordelijk voor bewustwording en voor incidentmanagement. Vertegenwoordigt de gemeente Zwolle in het BTO Security Board van het SSC-ONS. De CISO is de vertrouwenscontactpersoon (VCIB) naar de Informatiebeveiligingsdienst (IBD) tevens sectorale Computer Emergency Response Team.

Information Security Officer (ISO)

De (ISO) is verantwoordelijk voor het vertalen van beleid en richtlijnen in de werkprocessen binnen de afdelingen; ondersteunt hiertoe risicoanalyses in opdracht van het lijnmanagement en adviseert maatregelen om geduide risico's te mitigeren. De ISO legt het geheel van risico's, beveiligingsmaatregelen en -acties vast in het ISMS, voert regie op de voortgang van de acties en rapporteert hierover aan het lijnmanagement. De ISO adviseert bij projecten, organiseert een bewustwordingsprogramma en -trainingen.

Ambassadeur IB

Ambassadeurs IB helpen om de informatiebeveiligingsmaatregelen te implementeren binnen een afdeling. De ambassadeur is afkomstig uit het betreffende netwerkteam. De ambassadeur fungeert ook als de 'oren en ogen' voor de informatiebeveiliging en maakt informatiebeveiligingsincidenten bespreekbaar. Binnen het Information Security Management System treedt de ambassadeur op als reporter. De ambassadeur IB is vaak een key-user.

Functionarissen met een specifieke beveiligingsfunctie

Beveiligingsbeheerder BRP

De beveiligingsbeheerder BRP is verantwoordelijk voor de inrichting, organisatie en uitvoering van het informatiebeveiligingsbeleid voor de gemeentelijke voorziening van de BRP. Deze functie is vastgelegd en beschreven in de Regeling beheer en toezicht Basisregistratie Personen.

Beveiligingsfunctionaris reisdocumenten

De beveiligingsfunctionaris reisdocumenten is aangesteld voor het beheer van en het toezicht op de naleving van de beveiligingsprocedures reisdocumenten en rijbewijzen.

Security Officer Suwinet

De Security Officer Suwinet bevordert en bewaakt, in opdracht van de interne eigenaar, het veilig gebruiken van Suwinet door medewerkers (in- en extern) van de gemeente.

Beheerders van basisregistraties

Voor elke basisregistratie waarvan gemeente bronhouder is, draagt een beheerder de verantwoordelijkheid voor het inwinnen en bijhouden van de authentieke en niet-authentieke gegevens in een basisregistratie en voor het borgen van de kwaliteit van die gegevens.

Functioneel beheerders

De functioneel beheerder is verantwoordelijk voor het optimaal functioneren van één of meerdere informatiesystemen. Hij draagt onder andere zorg voor de continuïteit van het systeem.

Informatiemanager IV
De informatiemanager vertaalt de informatiebehoefte, die vanuit de verschillende werk- en bedrijfsprocessen ontstaan, in informatievoorziening. De informatiemanager is de ambassadeur voor informatiebeveiliging (IB) en intermediair vanuit de afdeling informatievoorziening, verantwoordelijk voor ondersteuning bij de (door-)ontwikkeling van strategische doelen van hun toegewezen afdeling.

5.2 Overlegfora

Intern
Werkgroep Informatiebeveiliging
Doel: gemeentebrede afstemming van activiteiten en beleid t.a.v. informatiebeveiliging.
Frequentie: minimaal vier keer per jaar. De CISO is voorzitter. Deelname door ambassadeurs voor het thema informatiebeveiliging vanuit: Burgerzaken; Informatievoorziening (Dataprotectie; Functioneel beheer; Gegevensmanagement; Informatieveiligheid), HR, Interne Controle, Inkoop, Privacy, Services, Suwinet en Website (Team Digitale Regie).

Kwaliteit board
De kwaliteit board wordt gevormd door vertegenwoordigers van de verschillende aspecten van informatievoorziening: security, privacy, informatiemanagement, recordmanagement en architectuur. De kwaliteit board stemt de verschillende aspecten van informatievoorziening, strategische en tactische activiteiten op elkaar af en toetst de verschillende plannen van de organisatie (en haar (keten)partners/verbonden partijen) integraal op beleid/principes, risico's en/of bedrijfscontinuïteit.

Overleg Privacy en Informatiebeveiliging
Doel:
- Voortgang en afstemming interne privacy en informatiebeveiligingszaken
- Voorbereiden beleidsstukken
- Frequentie is driewekelijks. Deelnemers zijn de CISO (voorzitter), FG, ethisch officer, Privacy Officer en de ISO's.

Extern
BTO security board
Deelnemers aan de BTO security board zijn de CISO (voorzitter), de Technical Information Security Officer van het SSC-ONS en IB-vertegenwoordigers van de partners.
Doel:
- voortgang en afstemming IT-security zaken binnen het SSC-ONS in relatie tot ontwikkelingen bij de deelnemende partners;
- planning en voortgang van projecten en audits;
- voorbereiden SPO adviespunten m.b.t. informatiebeveiliging.

Overleg met andere gemeenten (regionaal samenwerkingsverband)
- CISO kring IJsselland, in oprichting, ten behoeve van (C)ISO's van de gemeenten binnen IJsselland.
- Integraal veiligheidsoverleg IJsselland onder leiding van de coördinator integrale veiligheid (gastheer Deventer); de CISO neemt hier aan deel.
- Expertteam Cyber Overijssel met CISO's, cyberexperts Centrum voor Criminaliteitspreventie en Veiligheid (CCV) en Politie.

5.3 Managementsysteem

Information Security Management System (ISMS)

Het aangeschafte ISMS is een goed hulpmiddel voor de implementatie van de BIO en ondersteunt de borging van het IB proces.

Bijlage 6: Bronvermelding

Naam	Bron	Locatie
Informatiebeveiliging onder controle	Van Houten, Spruit en Wolters	4e druk ISBN 978-90-430-3672-6
Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2021/2022	Informatie-beveiligingsdienst	www.informatiebeveiligingsdienst.nl
Gemeenten. Bewustzijn. Privacy	Van de Merwe, Schoemaker en Havinga	1e druk ISBN 978-90-828604-4-3
Handreiking Informatiebeveiligings-beleid BIO	Informatie-beveiligingsdienst	Versie 1.2 licentie CC BY-NC-SA 4.0 www.informatiebeveiligingsdienst.nl
Visie en Strategie Informatievoorziening Zwolle Digitaal 2019 - 2022	MT Zwolle	Portal.zwolle.nl
Veilig in de cloud Cloudsecuritybeleid	IB Zwolle	Portal.zwolle.nl
De 10 bestuurlijke principes voor informatiebeveiliging	VNG realisatie	www.vng.nl
Agenda Digitale Veiligheid 2020 – 2024	VNG	www.vng.nl

Bijlage 7: Begrippenlijst

Begrip	Uitleg
Applicatie	Computerprogramma (toepassing) voor de eindgebruiker.
Audit	Het door een onafhankelijke deskundige kritisch beoordelen van de opzet, het bestaan en de werking van de (beveiligings-) voorzieningen en de organisatie voor informatietechnologie op betrouwbaarheid, doeltreffendheid en doelmatigheid.
Authentiseren	Het proces waarbij wordt nagegaan of een gebruiker daadwerkelijk is wie hij beweert te zijn. Bij de authenticatie wordt gecontroleerd of een opgegeven bewijs van identiteit overeenkomt met echtheidskenmerken (bijvoorbeeld een in het systeem geregistreerd bewijs).
Autoriseren	Het toekennen van rechten aan (groepen van) personen, processen en/of systemen. De autorisatie wordt toegekend door de eigenaar van het systeem.
Beschikbaarheid (of continuïteit)	Het zorgdragen voor het beschikbaar zijn van informatie en informatie-verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de geautoriseerde gebruikers.
Classificatie	De indeling in risicoklassen voor de aspecten beschikbaarheid, integriteit en vertrouwelijkheid.
Controleerbaarheid	Waarborgen dat de beoogde toegang tot gegevens en de juiste werking van systemen continu alsook achteraf te controleren is.
Dataclassificatie	Classificatie (of rubricering) van data geeft antwoord over de hoeveelheid maatregelen die genomen moeten worden om die data adequaat te beschermen.
ENSIA	Eenduidige Normatiek Single Information Audit heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus.
Functiescheiding	Het scheiden van gerelateerde taken en bevoegdheden om fouten en fraude te voorkomen.
IBD	De Informatiebeveiligingsdienst voor gemeenten (IBD) werkt aan het verhogen en op peil houden van de informatiebeveiliging van Nederlandse gemeenten. De IBD is een initiatief van alle Nederlandse gemeenten. Alle gemeenten kunnen gebruik maken van de diensten van de IBD.
Identificeren	Het vaststellen van de identiteit van een persoon. De identiteit wordt gebruikt om de toegang van het subject tot een object te beheersen. Identificatie is de eerste stap in het toegangscontroleproces.
Informatie	Een verzameling van gegevens (met of zonder context) opgeslagen in gedachten, geschriften en/of digitale informatiedragers.
Integriteit (of betrouwbaarheid)	Het waarborgen van de correctheid (juistheid), volledigheid, tijdigheid en geoorloofdheid van informatie en informatieverwerking oftewel het in overeenstemming zijn van informatie met de werkelijkheid.
Persoonsgegeven	Ieder gegeven dat is te herleiden tot een individuele persoon.
Privacy	Privacy is de persoonlijke levenssfeer die onszelf en ons handelen, eigenschappen en informatie onderscheidt en afschermt van anderen.
Systeem	Entiteit samengesteld uit meerdere kleinere, met elkaar samenhangende of op elkaar inwerkende componenten.
Vertrouwelijkheid (of exclusiviteit)	Het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

Bijlage 8: Gebruikte afkortingen

Afkorting	Betekenis
AI	Artificiële Intelligentie
AVG	Algemene Verordenng Gegevensbescherming
BAG	Basisregistratie Adressen en Gebouwen
BBN	Basisbeveiligingsniveau
B en W	Burgemeester en Wethouders
BGT	Basisregistratie Grootschalige Topografie
BIO	Baseline Informatiebeveiliging Overheid
BRO	Basisregistratie Ondergrond
BRP	Basisiregistratie Personen
BTO	Bedrijfsvoerend Tactisch Overleg
CISO	Chief Information Security Officer
CMDB	Configuration Management Database
DDoS	Distributed Denial of Service
DigiD	Digitale Identiteit
eID	Elektronische identificatiemiddelen
ENSIA	Eenduidige Normatiek Single Information Audit
FG	Functionaris Gegevensbescherming
GGI	Gemeentelijke Gemeenschappelijke Infrastructuur
HR	Human Resources
IB	Informatiebeveiliging
IBD	Informatiebeveiligingsdienst
ICT	Informatie en Communicatie Technologie
IoT	Internet of Things
ISO	Information Security Officer
ISMS	Information Security Management System
IT	Informatie Technologie
IV	Informaite Voorziening
LoD	Line of Defence
MTZ	Managementteam Zwolle
NCSC	Nationaal Cyber Security Centrum
P&C	Planning & Control
PDCA	Plan, Do, Check, Act
PNIK	Paspoorten en Nederlandse Identiteitskaarten
PO	Privacy Officer
RAO	Risico Acceptatie Overeenkomst
RPA	Robotic Process Automation
SaaS	Software as a Service
SSC ONS	Shared Service Center ONS
SPO	Strategisch Partner Overleg
SUWI	Structuur Uitoeringsorganisatie Werk en Inkomen
VIC	Verbijzonderde Interne Controle
WD	Waarde documenten
WDO	Wet digitale overheid
Who	Wet hergebruik van overheidsinformatie
Wmebv	Wet modernisering elektronisch bestuurlijk verkeer
Wob	Wet openbaarheid van bestuur
Woo	Wet open overheid
WOZ	Basisregistratie Waardering Onroerende Zaken
Wro	Wet op de ruimtelijke ordening