Strategisch informatiebeveiligingsbeleid

2025 - 2028

Versiebeheer

Versie	Datum	Door	Wijzigingen
1.0	02-10-2024	L. van Remunt (CISO)	Eerste versie
1.1	07-11-2024	L. van Remunt (CISO)	Voorgelegde versie

Inhoudsopgave

Versiebeheer....2
1. Inleiding....4
1.1. Visie....5
1.2. Ambitie....5
1.3. Definitie informatiebeveiliging....7
1.4. Baseline Informatiebeveiliging Overheid....8
1.5. Doel van beleid....9
1.6. Scope en bereik....10
1.7. Beheer van dit document....11
2. Strategische uitgangspunten....11
2.1. Wettelijke basis informatiebeveiliging....11
2.2. Forum standaardisatie....12
2.3. De 10 bestuurlijke principes voor informatiebeveiliging....12
2.4. Ontwikkelingen....14
2.5. Uitgangspunten ten aanzien van informatiebeveiliging....14
3. Governance en organisatie....16
3.1. Verantwoordelijkheden....16
3.2. Rollen en verantwoordelijkheden....17
3.3. Toezicht....20
4. Informatiebeveiligingsproces en risicomanagement....22
4.1. Informatiebeveiligingsproces (PDCA-cyclus)....22
4.2. Aansturen van het proces....26
5. Evaluatie, toetsing en verantwoording....27
5.1. Evaluatie....27
5.2. Toetsing....27
5.3. Verantwoording....27
6. Bewustwording....29
6.1. Zwakste en sterkste schakel....29
6.2. Activiteiten om de beveiligingsbewustwording te vergroten....30
Bijlage A De 10 bestuurlijke principes voorinformatiebeveiliging (VNG)....31
Bijlage B Rollen en verantwoordelijkheden....36
Bijlage C Afkortingen en begrippenlijst....44

1. Inleiding

Gemeente Boxtel voert verschillende publieke taken uit die zijn verankerd in wet- en regelgeving. We realiseren ons dat we een belangrijke rol hebben in het beschermen van de informatie dieons is toevertrouwd door onze inwoners, ondernemers en (keten)partners. Zij moeten kunnen uitgaan van een betrouwbare en goed functionerende overheid.

De wereld verandert snel en digitaliseert in hoog tempo. Gemeente Boxtel gaat mee in deze verandering, maar houdt ook oog voor risico's. Het behalen van onze maatschappelijke doelstellingen gaat gepaard met een goed en betrouwbaar functionerende informatievoorziening. Door technologie veilig en verantwoordin te zetten dragen we bij aan de 'Principes voor de Digitale Samenleving' (VNG, 2022)[1]. Dit alles maakt informatiebeveiliging van strategisch belang. De VNG benadrukt in 'De 10 bestuurlijke principes voor informatiebeveiliging' dat informatiebeveiliging een bestuurlijke verantwoordelijkheidis. We moeten ervoor zorgen dat informatie onder alle omstandigheden tijdig, correct, volledig en alleen voor de juiste personen beschikbaar is. En als er onverwachts iets misgaat, dan merken we dat snel op en zorgen we voor herstel.

Dit strategische informatiebeveiligingsbeleid vervangt het vorige beleid en geldt voor de periode 2025 tot en met 2028. Het geeft richting en stelt kaders zodat informatiebeveiliging een bijdrage levert aan onze (strategische) organisatiedoelen. We werken hierbij met risicomanagement wat de basis is van informatiebeveiliging: zonder inzicht in de belangrijkste risico's kun je geen effectieve maatregelen treffen. Het beleid maakt verderduidelijk hoe onze informatiebeveiligingsorganisatie in elkaar zit.

Het strategische beleid geeft géén antwoord op wat we de komende vier jaren precies, op welk moment, en op welke wijze gaan doen. Deze meer praktische invullingen volgen uit de tactische en operationele documenten.

1 Gemeentes willen met de 'Principes voor de Digitale Samenleving' (VNG, 2022) de democratische besluitvorming centraal stellen bij digitalisering en ethiek en risico's een vaste plek geven in die besluitvorming.

1.1. Visie

Gemeente Boxtel staat voor een aantal grote maatschappelijke opgaven en ontwikkelingen, die nieuwe antwoorden en vaardigheden van ons vragen. Technologische ontwikkelingen, digitalisering en toepassingen van kunstmatige intelligentie kunnen bijdragen aan de maatschappelijke opgaven waarvoor wij staan. Daarvan gaan we meer gebruik maken. Deze opgaves en ontwikkelingen kunnen alleen succesvol zijn in een veilige en betrouwbare omgeving. Een omgeving die ruimte biedt aan technologische ontwikkelingen en innovatieve toepassingen faciliteert. We maken dit mogelijk door informatiebeveiliging slim in te zetten.

Zo voeren we informatiebeveiliging uit op basis van risicomanagement en treffen noodzakelijke beveiligingsmaatregelen voor de belangrijkste risico's. We beveiligen informatie bij de bron, zorgen voor een sterke toegangsbeveiliging, en bieden een technische infrastructuur die nieuwe technologische toepassingen mogelijk maakt. De informatiebeveiligingsorganisatie ondersteunt de organisatie hierbij door inzicht te bieden in de kansen en dreigingen.

We werken samen aan een dienstverlenende organisatie waarin de basis op orde is en we strategisch daadkrachtig zijn. Informatiebeveiliging is een onderdeel van die 'basis op orde' en daarmee een randvoorwaarde voor onze dienstverlening en strategische doelen. Informatiebeveiliging is een natuurlijk onderdeel van ons vakmanschap, onze werkzaamheden en onze samenwerkingsverbanden. We nemen eigenaarschap door onze taken voor informatiebeveiliging gedegen uit te voeren. Om succesvol mee te kunnen in een tijd waarin digitalisering en complexiteit van ons werk steeds groter worden, is het belangrijk dat medewerkers over 21e-eeuwse vaardigheden beschikken. Behalve basale ICT-kennis en informatievaardigheden, moeten medewerkers zich ook bewust zijn van hun manier van handelen en welke risico's dit met zich meebrengt. Door de samenwerking op te zoeken werken we met elkaar om ons werk niet alleen efficiënter en effectiever te maken, maar ook om onze digitale weerbaarheid stapsgewijs te verhogen.

Het fundament voor informatiebeveiliging wordt gevormd door het (hoogste) management. Informatiebeveiliging is Chefsache! Informatiebeveiligingsbewustzijn is essentieel in al ons handelen en voor iedereen. Om voldoende urgentie te creëren, geven we inzicht in de risico's rond onze informatievoorziening en de mogelijke gevolgen die een bedreiging voor onze organisatie kan hebben.

Onze visie op informatiebeveiliging luidt daarom als volgt:

"Wij zijn een betrouwbare overheid. Informatiebeveiliging is een randvoorwaarde voor al ons handelenen is integraal onderdeel van ieders werk."

1.2. Ambitie

Inwoners, ondernemers en (keten)partners moeten kunnen uitgaan van een betrouwbare en goed functionerende overheid. Gemeente Boxtel streeft erna om de basis van informatiebeveiliging goed op orde te hebben. We volgen hiervoor de landelijke Baseline Informatiebeveiliging Overheid (BIO), het verplichte normenkader voor informatiebeveiliging. Ook het voldoen aan de komende NIS2 wetgeving is een speerpunt. Met de basis op orde voldoen we niet alleen aan wet- en regelgeving, maar creëren we ook de randvoorwaarden voor technologische ontwikkelingen en innovatieve toepassingen. Daarnaast zorgen we ervoor dat onze bestuurlijke en organisatorische doelstellingen worden gehaald door de informatieveiligheid risico's te verkleinen tot een acceptabel niveau.

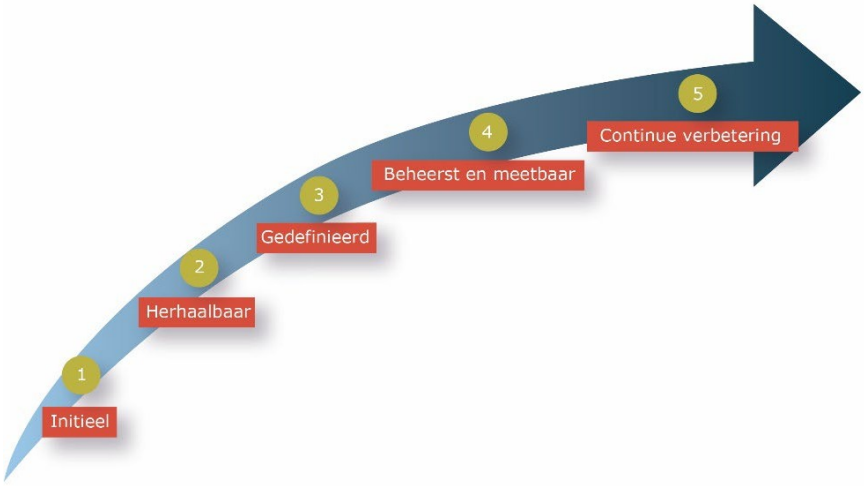
Een volwassen benadering van informatiebeveiliging begint ermee dat we de BIO niet slechts als afvinklijst hanteren.[2] Het voldoen aan de vereisten vraagt om een internalisering in alle geledingen van onze organisatie: medewerkers moeten zich de regels eigen maken, zodat deze niet langer worden ervaren als extern opgelegde voorschriften, maar als richtlijnen die ze zelf hebben gekozen. De afgelopen jaren hebben we beperkt geïnvesteerd in het op niveau brengen van onze informatiebeveiliging maar in de periode 2025 tot en met 2028 zal er structureel geïnvesteerd worden. Door gebruik te maken van een volwassenheidsmodel[2] voor informatiebeveiliging hebben we niet alleen een krachtig instrument om te meten hoe volwassen Gemeente Boxtel om gaat met informatiebeveiliging, maar ook een stuurinstrument in handen waarmee we onze informatiebeveiliging stapsgewijs en planmatig kunnen verbeteren. Door het volwassenheidsniveau periodiek te meten en inzichtelijk te maken kunnen we beter de dialoog voeren met het management en de medewerkers.

Ons ambitieniveau te bereiken aan het einde van dit beleidsstuk voor informatiebeveiliging is Niveau 3, Gedefinieerd, voor zover Gemeente Boxtel daar zelf invloed op heeft. Niveau 3 is tevens het minimum om te kunnen stellen dat we aan de BIO voldoen. Met deze 'basis op orde' hebben we informatiebeveiliging organisatie breed ingericht en realiseren we een belangrijke randvoorwaarde voor onze dienstverlening en strategische doelen. Daar waar wet- en regelgeving vraagt om beheersing en meting (niveau 4) of continue verbetering (niveau 5), wordt een hoger niveau toegepast.

[2] Te hanteren model het Capability Maturity Model (CMM) voor het vaststellen van het volwassenheidsniveau.

Onze ambitie is als volgt samen te vatten:

"Beheersingsmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst."



Figuur 1: volwassenheidsniveaus informatiebeveiliging

1.3. Definitie informatiebeveiliging

Onder informatiebeveiliging verstaan we het proces van het vaststellen van de vereiste betrouwbaarheid van informatiesystemen[3] in termen van beschikbaarheid, integriteit en vertrouwelijkheid (BIV), alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen, om de veiligheid van de informatievoorziening[4] aantoonbaarte waarborgen. Het begrip 'aantoonbaar' houdt in dat Gemeente Boxtel in staat is om te bewijzen dat de beveiligingsmaatregelen zijn beschreven (opzet), worden uitgevoerd (bestaan), en over een langere periode zijn uitgevoerd (werking).

[3] De Nederlandse Overheid Referentie Architectuur (NORA) definieert een informatiesysteem als een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur, alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.
[4] Een informatievoorziening bestaat uit een organisatie brede verzameling van wel of niet samenhangende informatiesystemen met elk een duidelijke eigenaar.

Informatiebeveiliging heeft niet alleen betrekking op de beveiliging van informatie in digitale of analoge (bijvoorbeeld papieren) vorm, maar ook in de vorm van kennis van individuele medewerkers. Bewustwording is dus essentieel. Verder zijn alle onderdelen van een informatiesysteem in scope. We lichten de termen beschikbaarheid,integriteit en vertrouwelijkheid hieronder toe.

- **Beschikbaarheid**: het waarborgen dat geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen).
- **Integriteit**: het waarborgen van de juistheid en volledigheid van informatie en de verwerking ervan.
- **Vertrouwelijkheid**: het waarborgen dat informatie alleen toegankelijk is voor diegenen die hiertoe zijn geautoriseerd.

Informatiebeveiliging versus gegevensbescherming

De termen informatiebeveiliging en gegevensbescherming lijken hetzelfde, maar zijn niet synoniem aan elkaar. Informatiebeveiliging richt zich primair op het beschermen van informatie van de organisatie (organisatiebelang), terwijl gegevensbescherming gaat over het beschermen van mensen tegen misbruik van hun gegevens (persoonsbelang). Verder is informatiebeveiliging vastgelegd in een standaard (BIO voor de overheid), terwijl gegevensbescherming is vastgelegd in wetgeving (AVG en aanverwante wetgeving). Dit leidt er onder andere toe dat er bij gegevensbescherming niet alleen rekening gehouden moet worden met de aspecten beschikbaarheid, integriteit en vertrouwelijkheid, maar dat er ook sprake moet zijn van rechtmatigheid bij het gebruik van gegevens. Er is dus een overlap tussen informatiebeveiliging en privacy, omdat beide zich richten op de organisatorische en technische maatregelen voor het beschermen van persoonsgegevens[11].

1.4. Baseline Informatiebeveiliging Overheid

De Baseline informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging voor alle overheidslagen, inclusief gemeentes. Deze verplichte overheidsstandaard is gebaseerd op de standaarden NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017. Gemeenten baseren hun beleid voor informatiebeveiliging op de BIO en leggen hierover verantwoording af aan de gemeenteraden en de toezichthouders vanuitde rijksoverheid.

De BIO biedt:

- Een beschrijving van de maatregelen die vereist zijn om een basisniveau van beveiliging te garanderen op het gebied van fysieke beveiliging van onze gebouwen en werkomgeving, maar ook op het gebied van personeelsbeleid, inkoop en ICT;
- Een baseline waarop, indien nodig, aanvullend extra beveiligingsmaatregelen kunnen worden getroffen;
- Een normenkader dat bij aanbestedingen met een ICT-component als basis voor informatiebeveiliging wordt gebruikt.

Controls en verplichte overheidsmaatregelen

De BIO bestaat uit 14 beveiligingsgebieden, elk met specifieke 'controls' en verplichte overheidsmaatregelen om de beheerdoelstellingen te bereiken. De BIO bevat twee strategische beveiligingshoofdstukken (hoofdstuk 5 en 6) die in dit strategische informatiebeveiligingsbeleid worden uitgewerkt. De overige 12 hoofdstukken, namelijk 7 t/m 18, zijn de tactische categorieën die worden behandeld in het tactische beleid. Wij nemen de controls en verplichte overheidsmaatregelen onverkort over. Door al deze maatregelen te implementeren voldoen we aan wet- en regelgeving, waarborgen we de gemeenschappelijke veiligheid van overheidsketens en leggen we de basis voor een betrouwbare informatievoorziening.

Pas toe of leg uit

Afwijken van de BIO kan beperkt, namelijk conform het pas-toe-of-leg-uit-principe. Een proces- of systeemeigenaar mag alleen op punten afwijken als er onvoldoende mogelijkheden bestaan om aan alle maatregelen te voldoen of om een andere zwaarwegende reden. De afwijking en de reden daarvan moeten dan worden vastgelegd. Dit is de betekenis van ‘leg uit’. De proceseigenaar moet daarbij het volgende scherp in de gaten houden: de maatregelen hangen met elkaar samen en het weglaten van één maatregel kan het geheel aan maatregelen ondermijnen met de kans dat het risico juist toeneemt in plaats van afneemt.

1.5. Doel van beleid

Het doel van dit strategische informatiebeveiligingsbeleid is om een kader en richtlijnen te bieden voor passende organisatorische en technische maatregelen ter bescherming van onze informatievoorziening. Het beleid moet ervoor zorgen dat het lijnmanagement voor de juiste aansturing van en steun voor informatiebeveiliging zorgt. Dit nieuwe beleid vervangt het vorige informatiebeveiligingsbeleid en geldt voor de periode 2025 tot en met 2028.

1.6. Scope en bereik

Het informatiebeveiligingsbeleid is van toepassing op het gehele proces van informatievoorziening, en geldt gedurende de gehele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Behalve kantoorautomatisering (ICT) maken we ook gebruik van procesautomatisering (PA)[5] voor operationele processen in de fysieke wereld. Denk bijvoorbeeld aan de aansturing van camera's, toegangssystemen, gemalen, riolering en verkeerslichten. Dit beleid is ook van toepassing op procesautomatisering.

Het terrein van informatiebeveiliging beperkt zich niet tot bepaalde functies of functionarissen, maar geldt voor alle medewerkers en voor alle (mondelinge en schriftelijke) informatie. Het strekt zich uit over zowel de strategische, tactische als operationele organisatieniveaus. Tenslotte is het informatiebeveiligingsbeleid ook van toepassing op de externe partijen waarmee Gemeente Boxtel samenwerkt en de ketens van informatiesystemen die zich kunnen uitstrekken tot buiten onze organisatie. De verantwoordelijkheden van deze zogeheten informatieketens worden toegelicht.

Dit strategische beleid vormt de basis voor de beleidsdocumenten op tactisch[6] en operationeel niveau. Het beleid geeft géén antwoord op de vraag wat we de komende beleidsperiode precies, op welk moment, en op welke wijze gaan doen. Deze meer praktische invullingen volgen uit de tactische en operationele documenten, die tezamen met dit strategische beleid, het informatiebeveiligingsbeleid van Gemeente Boxtel vormt. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan (IBP). Een afdeling of team is vrij om samen met de CISO een eigen beleid op te stellen dat aanvullend is voor de eigen processen en minimaal aan dit strategische beleid voldoet.

Met dit beleid worden een aantal beveiligingseisen uit wetgeving, zoals de Wet BRP, PUN en SUWI. Aanvullende specifieke beveiligingseisen die op grond van deze wet- en regelgeving gelden voor bepaalde kerntaken, worden in aanvullende documenten geformuleerd.

[5] Procesautomatisering (PA), ook wel bekend onder de naam Operational Technology (OT), is een verzamelnaamvoor verschillende systemen die worden gebruikt voor het beheer van operationele processen in de fysieke wereld, zoals het aansturen en monitoren van (industriële) apparatuur.
[6] Het tactisch beleid behelst uitwerkingen van verschillende onderwerpen, zoals logische toegangsbeveiliging, incidentmanagement, back-up en recovery, cryptografie, leveranciersmanagement, maar ook gedragsregels en fysieke beveiliging.

1.7. Beheer van dit document

Het informatiebeveiligingsbeleid wordt conform de baseline voor informatiebeveiliging (BIO) minimaal één keer per vier jaar, of bij belangrijke wijzigingen als gevolg van een reorganisatie of verandering in de verantwoordelijkheidsverdeling, beoordeeld en zo nodig bijgesteld. Bij deze actualisatie worden nieuwe ontwikkelingen op het gebied van de bedrijfsvoering, wet- en Regelgeving, informatiebeveiliging en privacy meegenomen. De Chief Information Security Officer (CISO) is verantwoordelijk voor het bijstellen en actueel houden van het informatiebeveiligingsbeleid.

Het informatiebeveiligingsbeleid wordt van kracht na vaststelling door de colleges dan wel het dagelijks bestuur. Bij het van kracht worden van dit document vervallen de vorige versies van het informatiebeveiligingsbeleid. De actuele versie wordt gepubliceerd op de digitale werkplek van Gemeente Boxtel en is ook op te vragen bij de CISO.

2. Strategische uitgangspunten

Om de doelstelling van informatiebeveiliging in onze organisatie te verwezenlijken en tot een weloverwogen en organisatie breed gedragen informatiebeveiligingsbeleid te komen, is het essentieel om een aantal strategische uitgangspunten te benoemen. De uitgangspunten geven richting aan de wijze waarop informatiebeveiliging ingericht moet worden.

Allereerst geldt dat de uitgangspunten van het informatiebeveiligingsbeleid moeten voldoen aan wet -en regelgeving. Daarnaast stelt de Baseline Informatiebeveiliging Overheid (BIO) eisen aan hoe we informatiebeveiliging organisatorisch en technisch moeten inrichten. De VNG heeft op basis van de BIO voor het college en de raad ‘De 10 bestuurlijke principes voor informatiebeveiliging’ geschreven. Deze principes worden door Gemeente Boxtel onderschreven. We benoemen welke ontwikkelingen voor informatiebeveiliging de komende periode relevant zijn. Op basis van al deze bronnen formuleren weeen aantal uitgangspunten voor informatiebeveiliging die niet alleen in lijn liggen met de BIO, maar ook tegemoetkomen aan de behoeftes van onze organisatie.

2.1. Wettelijke basis informatiebeveiliging

De wettelijke basis voor informatiebeveiliging bestaat uit Europese en nationale wet- en regelgeving. Onderstaande niet-limitatieve lijst van wet- en regelgeving stelt eisen aan het niveau van informatiebeveiliging, de beheersmaatregelen en de controle daarop.

- Auteurswet;
- Telecommunicatiewet;
- Ambtenarenwet 2017;
- Wet computercriminaliteit;
- Algemene verordening gegevensbescherming (AVG);
- Uitvoeringswet Algemene verordening gegevensbescherming (UAVG)
- Archiefwet/Archiefregeling;
- Databankenwet;
- Wet modernisering elektronisch bestuurlijk verkeer;
- Wet elektronische handtekeningen;
- Wet algemene bepalingen Burgerservicenummer (WABB);
- Paspoortwet;
- Wet basisregistratie personen (Wet BRP);
- Wet digitale overheid (Wdo);
- 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 Kenbaarheid Publiekrechtelijke Beperkingen (WKPB);
- Wet Politiegegevens (Wpg);
- Omgevingswet.

Nota bene: hoewel de Baseline Informatiebeveiliging Overheid (BIO) verplicht is voor alle overheden, zal deze pas in 2025 een wettelijke basis krijgen met de ontwikkelingen van de Europese NIS2 wetgeving die naar nationaal niveau vertaald moet worden in een Nederlandse wet. In datzelfde jaar zullen gemeentes ook moeten voldoen aan de Europese Netwerk- en Informatiebeveiligingsrichtlijn (NIS2[7]), die strengere eisen stelt aan essentiële diensten van zowel bedrijven als overheden.

2.2. Forum standaardisatie

Forum Standaardisatie[8] biedt een overzicht van verplichte en aanbevolen (ICT-)standaarden voor de overheid. Twee van deze verplichte standaarden zijn de normen NEN-ISO/IEC 27001:2013 en NEN-ISO/IEC 27002:2013 waarop de Baseline Informatiebeveiliging Overheid (BIO) is gebaseerd. We implementeren de verplichte standaarden volgens het pas-toe-of-leg-uit-principe.

2.3. De 10 bestuurlijke principes voor informatiebeveiliging

Het bestuur is verantwoordelijk voor de informatiebeveiliging binnen onze organisatie. Bestuurders moeten zich daarom bewust zijn van de risico's van en voor de organisatie. In aanvulling op de Baseline Informatiebeveiliging Overheid (BIO) heeft de VNG daarom een tiental principes voor bestuurders opgesteld. De principes gaan over de waarden die de bestuurders zichzelf opleggen. Deze waarden moet in verbinding staan met de waarden van onze organisatie. Gemeente Boxtel onderschrijft de 10 bestuurlijke principes voor informatiebeveiliging. Hieronder worden ze kort opgesomd. Voor eenuitgebreide toelichting op de principes, zie bijlage A.

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.

[7] NIS2 is de afkorting voor de Network & Information Systems Directive (NIS2), de opvolger van de NIS1. De Nederlandse overheid moest deze richtlijn vóór oktober 2024 omzetten in nationale wetgeving maar heeft vertraging opgelopen. Het is nog onduidelijk welke kritieke gemeentelijke processenonderdeel uitmaken van deze richtlijn. Dit zal medio 2025 in werking moeten treden en daarbij ook duidelijkheid wat er word verwacht van ons
[8] www.forumstandaardisatie.nl

2.4. Ontwikkelingen

De wereld verandert snel en digitaliseert nog sneller, mede ook door de coronacrisis. Gemeente Boxtel gaat mee in deze verandering. We zien onder andere bij ICT-leveranciers een verschuiving van on-premise naar de cloud. Mede daarom hebben we een cloudstrategie opgesteld om richting te geven aan het moderniseren van onze ICT. Een andere ontwikkeling is het data gedreven werken waarbij data wordt gebruikt om meer doelgericht, vollediger en adequater beslissingen te nemen op alle niveaus in de organisatie.

2.5. Uitgangspunten ten aanzien van informatiebeveiliging

Uitgangspunten ten aanzien van informatiebeveiliging kunnen als volgt worden samengevat:

1. Gemeente Boxtel hanteert de BIO. De BIO wordt op basis van het pas-toe-of-leg-uit-principe geïmplementeerd. Bij afwijking van de BIO wordt getoetst of dit tot aanvullende risico's leidt voor andere organisaties in de keten;
2. Het bestuur stelt kaders en bepaalt welke risico's het bereid is om te nemenbij het realiseren van zijn strategische doelstellingen; (risicobereidheid)
3. Informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement[9];
4. De CISO is autoriteit op het gebied van informatiebeveiliging. Hij adviseert en rapporteert aan zowel het lijnmanagement als het bestuur. Zijn advies is zwaarwegend bij het nemen van beslissingen omtrent informatiebeveiliging;
5. Alle processen, inclusief bedrijfsmiddelen én bijbehorende risico's, moeten een eigenaar hebben, zodat er altijd iemand, in overeenstemming met dit beleid en de risicobereidheid van de organisatie, verantwoordelijk is voor de bescherming van het proces of bedrijfsmiddel;
6. Informatiebeveiligingskaders en maatregelen worden organisatie breed afgesproken en ingezet. In uitzonderingsgevallen wordt na een risicoafweging in overleg en conform procedure afgeweken;

   Informatiebeveiliging is een continu verbeterproces met risicomanagement als primair uitgangspunt. Door organisatie brede planning, het implementeren van maatregelen, het ondersteunen van gebruikers bij het juiste gebruik van bedrijfsmiddelen, het periodiek controleren en het coördineren van dit proces, zorgen we voor verankering van informatiebeveiliging in de organisatie;

[9] Zie ook 'factsheet lijnmanager' van de Informatiebeveiligingsdienst (IBD).

7. Informatiebeveiliging is onderdeel van de gehele levenscyclus van informatiesystemen, inclusief voorzieningen zoals mobiele apparaten;
8. Het bestuur, de directie en de concern en team managers dragen het beleid uit en sturen op de implementatie van beveiligingsmaatregelen;
9. Verantwoord en bewust gedrag van medewerkers is essentieel voor een goede informatiebeveiliging. Gemeente Boxtel moet hiervoor gedragsregels voor de digitale werkomgeving ontwikkelen;
10. Gemeente Boxtel zorgt voor een open cultuur waarin medewerkers zich vrij en veilig voelen om onveilige situaties, incidenten of ongelukken te melden, en we met elkaar kunnen leren van incidenten;
11. Beveiligingsincidenten worden gemeld, geregistreerd, onderzocht en geëvalueerd;
12. Iedere medewerker heeft slechts die toegangsrechten die nodig zijn voor het uitvoeren van zijn taken (need-to-know-principe);
13. Technische en organisatorische maatregelen worden getroffen in de eerste stadia van het ontwerpproces, zodat informatiebeveiliging in de basis geregeld is. Dit noemen we 'security-by-design';
14. Systemen zijn standaard geconfigureerd om maximale beveiliging te bieden zonder dat gebruikers extra stappen moeten ondernemen. Dit noemen we 'security-by-default';
15. Kennis en expertise zijn essentieel voor een toekomstbestendige informatiebeveiliging en moeten geborgd worden;
16. Gemeente Boxtel voert altijd regie op haar eigen data, ongeacht waar die data opgeslagen is. Denk hierbijbijvoorbeeld aan de regie op data bij ketensamenwerkingen;
17. Bij het implementeren van beveiligingsmaatregelen moet aandacht zijn voor de balans tussen beveiliging en productiviteit. De risicobereidheid en operationele behoeftes van de organisatie moeten hierbij tegen elkaar worden afgewogen;
18. Er worden periodiek onafhankelijke audits uitgevoerd om vast te stellen of de vereiste beveiligingsmaatregelen in voldoende mate zijn geborgd;
19. Gemeente Boxtel verbeteren de digitale weerbaarheid door de maatregelen uit het ondersteuningspakket 'Verhoging Digitale Weerbaarheid' (VDW) van de Informatiebeveiligingsdienst (IBD) te implementeren.

3. Governance en organisatie

Gemeente Boxtel is verantwoordelijk voor de beveiliging van haar informatievoorziening. Om deze verantwoordelijkheid goed in te vullen is transparantie en verantwoording over besluitvorming rondom informatiebeveiliging nodig.

Dit hoofdstuk waarborgt de rollen en verantwoordelijkheden op het gebied van informatiebeveiliging en benadrukt de (eind)verantwoordelijkheid van de lijnorganisatie. Er wordt beschreven hoe Gemeente Boxtel de doelstellingen in dit informatiebeveiligingsbeleid borgt en hoe de relevante wet- en regelgeving wordt geïmplementeerd en gehandhaafd. We geven hiermee tevens invulling aan het principe 'Transparantie centraal' uit de 'Principes voor de Digitale Samenleving' (VNG, versie 2022).

3.1. Verantwoordelijkheden

3.1.1. LIJNVERANTWOORDELIJKHEID

De Baseline Informatiebeveiliging Overheid (BIO) stelt dat informatiebeveiliging een lijnverantwoordelijkheid is. Elke lijnmanager is eindverantwoordelijk voor een adequate beveiliging van zijn informatie in processen, ketens en applicaties/systemen. Het is aan de lijnmanager om, eventueel met ondersteuning, te beoordelen welke informatie vertrouwelijk is, welke risico's gepaard gaan met het verwerken van deze informatie en hoe deze risico's het beste kunnen worden beperkt. Er wordt centraal vastgelegd welke lijnmanager als 'eigenaar' fungeert voor de gemeentelijke processen en applicaties en daarmee ook verantwoordelijk is voor de bijbehorende informatiebeveiliging. Processen, applicaties en systemen zonder eigenaar worden door het dagelijks bestuur of concernmanager toegewezen aan een lijnmanager, zodat de verantwoordelijkheden altijd belegd zijn.

Als een lijnmanager taken laat uitvoeren door een andere organisatie, bijvoorbeeld een leverancier, shared service center of ketenpartner, dan zorgt hij ervoor dat de belangen van Gemeente Boxtel in het kader van informatiebeveiliging gewaarborgd is door middel van een schriftelijke overeenkomst, zoals een dienstverlenings-, verwerkers- of gegevensleveringsovereenkomst (GLO). Daarnaast controleert hij periodiek of de afspraken op papier in de praktijk worden nagekomen. Organisaties die geen onderdeel zijn van de overheid zijn niet direct gebonden aan de BIO. In dat geval bepaalt de opdrachtgever samen met de CISO aan welke informatiebeveiligingseisen een externe organisatie moet voldoen. Deze eisen zullen in het contract met de externe organisatie moeten worden vastgelegd.

3.2. Rollen en verantwoordelijkheden

Hieronder worden de rollen opgesomd die bijdragen aan het proces van informatiebeveiliging bij Gemeente Boxtel. Een uitgebreide beschrijving van de verantwoordelijkheden en bevoegdheden is terug te vinden in bijlage B. Basis voor de rolverdeling en de verdeling van de verantwoordelijkheden zijn de BIO en geldende wet- en regelgeving.

- **Gemeenteraden**: Zijn bevoegd voor de controle en toetsing op de werking van beleid binnen de gemeente, zo ook voor informatiebeveiliging. De colleges van burgemeester en wethouders leggen middels de Eenduidige Normatiek Single Information Audit (ENSIA) jaarlijks verantwoording af aan de raden middels de zelfevaluaties over de BIO, BRP, Reisdocumenten,WOZ, BAG, BGT en BRO. Aan de raden wordt ook verantwoording afgelegd via de ENSIA- collegeverklaringen waarin de auditor een assurance afgeeft over onze DigiD-aansluitingen enhet gebruik van Suwinet.

- **Dagelijks bestuur Gemeente Boxtel en de Colleges van B&W:** Zijn eindverantwoordelijk voor een passend niveau van informatiebeveiliging in onze organisaties. Het dagelijks bestuur MGD en de colleges stellen met het voorliggende beleidsdocument de kaders vast ten aanzien van informatiebeveiliging. De burgemeester zijn portefeuillehouders voor informatiebeveiliging.

- **Gemeentesecretarissen**: is ambtelijk eindverantwoordelijk voor de implementatie, borging en uitvoering van het informatiebeveiligingsbeleid binnen de organisatie. De gemeentesecretaris stelt in overleg met het college, het management en de CISO het gewenste niveau van informatiebeveiliging vast.

- **Lijnmanager**: is als concern manager of teammanager verantwoordelijk voor de informatiebeveiliging van zijn eigen organisatieonderdeel. De lijnmanager beheerst voor zijn organisatieonderdeel de risico's. Hij stelt de betrouwbaarheidseisen en een samenhangend pakket aan beveiligingsmaatregelen vast voor zijn informatiesystemen (opzet, bestaan en werking).

- **Chief Information Security Officer (CISO)**: adviseert en ondersteunt het lijnmanagement en bestuur bij hun verantwoordelijkheid voor informatiebeveiliging. Zijn advies is zwaarwegend bij het nemen van beslissingen. De CISO is verantwoordelijk voor het actueel houden van het informatiebeveiligingsbeleid, het coördineren van de uitvoering van het beleid.

- **Functionaris voor Gegevensbescherming (FG):** houdt binnen Gemeente Boxtel onafhankelijk toezicht op de naleving van de AVG en aanverwante privacywetgeving en geeft hierover advies.

- **Privacy Officer**: draagt bij aan de privacy compliance van de organisatie. De Privacy Officer

kent een (juridisch-)coördinerende invulling.

- **(Functioneel) applicatiebeheerder**: is namens de systeemeigenaar operationeel verantwoordelijk voor de continuïteit en het optimaal functioneren van één of meerdere informatiesystemen. De (functioneel) applicatiebeheerder voert het beheer uit binnen de kaders van de Baseline Informatiebeveiliging Overheid (BIO), onder andere door ervoor te zorgen dat gebruikers slechts die toegangsrechten hebben die nodig zijn voor het uitvoeren van hun taken (need-to-know-principe).

- **Systeembeheer**: beveiligt de ICT-infrastructuur en waarborgt dat alleen geautoriseerde gebruikers toegang hebben tot informatiesystemen. Beveiliging vindt plaats conform de Baseline Informatiebeveiliging Overheid (BIO).

- **ENSIA-coördinator**: is verantwoordelijk voor het organiseren van de ENSIA-verantwoording. De ENSIA-coördinator is onafhankelijk en rapporteert over de stand van zaken van informatiebeveiliging (en de kwaliteit van gegevens) richting de gemeenteraden en toezichthouders van het Rijk.

- **Teammanager I&A**: stelt de organisatie brede kaders voor de informatievoorziening vast, waaronder architectuur en (informatiebeveiliging)standaarden, en ziet toe op de naleving hiervan. De teammanager ICT bewaakt de samenhang tussen informatievoorziening en projecten.

- **Gebouwenbeheer (Vastgoed Beheer)**: is verantwoordelijk voor de fysieke beveiliging van gebouwen en goederen conform de Baseline Informatiebeveiliging Overheid (BIO).

- **Human Resources (HR)**: is verantwoordelijk voor de screening van alle interne en externe medewerkers en zorgt voor de organisatie brede training en educatie van nieuwe en bestaande medewerkers. HR wijst, in samenwerking met de lijnmanager, medewerkers bij aanstelling of functiewisseling op hun verantwoordelijkheden ten aanzien van informatiebeveiliging.

- **Inkoop**: is verantwoordelijk voor het inkoopproces en borgt dat informatiebeveiligingseisen expliciet opgenomen zijn in (inkoop)contracten.

- **Medewerkers (inclusief externen)**: is verantwoordelijk voor het zorgvuldig omgaan met (vertrouwelijke) informatie. De medewerker is zich bewust van de eisen die gesteld worden ten aanzien van informatiebeveiliging en houdt zicht aan de gedragscodes van Gemeente Boxtel. Iedere medewerker is verplicht om periodiek de basismodule en training voor informatiebeveiliging te volgen.

Externe partijen

- **Externe ICT leveranciers**: beveiligt de ICT-infrastructuur en waarborgt dat alleen geautoriseerde gebruikers toegang hebben tot informatiesystemen. De dienstenleverancier rapporteert over informatiebeveiligingsincidenten aan de opdrachtgever. Commerciële dienstenleveranciers maken geen deel uit van de overheid en zijn daarom niet gebonden aan de BIO. In dit geval moeten de beveiligingseisen apart contractueel worden vastgelegd.

- **Rekenkamercommissie:** ondersteunt de gemeenteraden bij zijn controlerende taken door onderzoek te doen naar de doeltreffendheid, doelmatigheid en rechtmatigheid van het gemeentelijk beleid. De rekenkamercommissie kan zelfstandig een onderzoek (laten) uitvoeren naar de informatiebeveiliging van onze organisatie en rapporteert hierover aan de gemeenteraden.

- **Externe partij in samenwerkingsverband:** is verantwoordelijk om de gegevens die Gemeente Boxtel uitwisselt in de keten te beveiligen. Dit kan bijvoorbeeld een ketenpartner[10] of een gemeenschappelijke regeling[11] zijn. Publieke partijen zijn verplicht zich te houden aan de BIO, terwijl private partijen niet direct gebonden zijn aan de BIO en zich daarom aan een schriftelijke dienstverlenings-, verwerkers- of gegevensleveringsovereenkomst (GLO) moeten houden. Nota bene: conform de AVG blijft Gemeente Boxtel eindverantwoordelijke voor de bescherming van persoonsgegevens als de ketenpartner ten opzichte van Gemeente Boxtel een verwerker is.

[10] Een ketenpartner is volgens de NORA een organisatie die deel uitmaakt van een samenwerkingsverband tussen publieke en/of private organisaties (keten), die naast hun eigen doelstellingen, één of meer gemeenschappelijk gekozen (of door de politiek opgelegde) ketendoelstellingen nastreven.
[11] Een gemeenschappelijke regeling (GR) is conform de Wet gemeenschappelijke regelingen (Wgr) een samenwerking tussen bestuursorganen van gemeenten, provincies, waterschappen, rechtspersonen of andere openbare lichamen ter behartiging van een of meer bepaalde belangen van die bestuursorganen.

3.3. Toezicht

Gemeente Boxtel hanteert het Three Lines of Defense (3LoD) model[12] als leidraad bij het inrichten van de informatiebeveiligingsorganisatie. Dit model levert een positieve bijdrage aan onze risicocultuur[13], het nemen van verantwoordelijkheden bij het beheersen van risico's, en het creëren van transparantie in het besluitvormingsproces. Het model sluit hierdoor goed aan op het principe 'Transparantie centraal' van de 'Principes voor de Digitale Samenleving' (VNG, 2022).

- De eerste lijn ('first line of defense') wordt vertegenwoordigd door het lijnmanagement: de secretarissen, concern managers en teammanagers, eventueel ondersteund door de beveiligingsbeheerders. De eerste lijn geeft leiding en sturing aan acties (inclusief risicomanagement) en de inzet van middelen om de doelstellingen van de organisatie te realiseren. Uitgangspunt is dat het lijnmanagement (de business) verantwoordelijk is voor haar eigen processen en dus ook de risicobeheersing en de aantoonbare naleving van wet- en regelgeving. De eerste lijn beheerst de risico's binnen de door de gestelde uitgangspunten.

- De tweede lijn ('second line of defense') wordt gevormd door de rollen die de eerste lijn van kaders, beleid, advies en ondersteuning voorzien, en bewaken of het management zijn verantwoordelijkheden daadwerkelijk neemt en het beleid naleeft. De tweede lijn staat hierbij niet op afstand, maar werkt als businesspartner nauw samen met de eerste lijn. De CISO maakt deel uit van deze lijn en adviseert over informatiebeveiligingsvraagstukken, met name als die een organisatie brede aanpak vereisen. Verder houdt de CISO-toezicht op de eerste lijn en signaleert risico's. In de tweede lijn bevinden zich behalve de CISO, ook de ISO en de privacy officers.

[12] Het Three Lines of Defense model van het Institute of Internal Auditors (IIA) is een wereldwijd gebruikt raamwerk voor risicobeheer en compliance en draagt bij aan een effectieve informatiebeveiliging.
[13] Onder risicocultuur wordt de manier verstaan waarop risico's deel uitmaken van de organisatiecultuur en hoe de organisatie reageert op in- en externe uitdagingen (KPMG).

- De derde lijn (‘third line of defense’) bestaat uit onafhankelijke interne en externe auditors. Deze lijn controleert of het samenspel tussen de eerste en tweede lijn goed functioneert en geeft een objectief en onafhankelijk oordeel met suggesties voor eventuele verbeteringen. Idealiter is de derde lijn belegd bij een team Internal Audit dat onafhankelijk van andere organisatieonderdelen kan opereren. De functionaris voor gegevensbescherming is ook onderdeel van deze lijn.

Figuur 2: Three Lines of Defense (3LoD) model

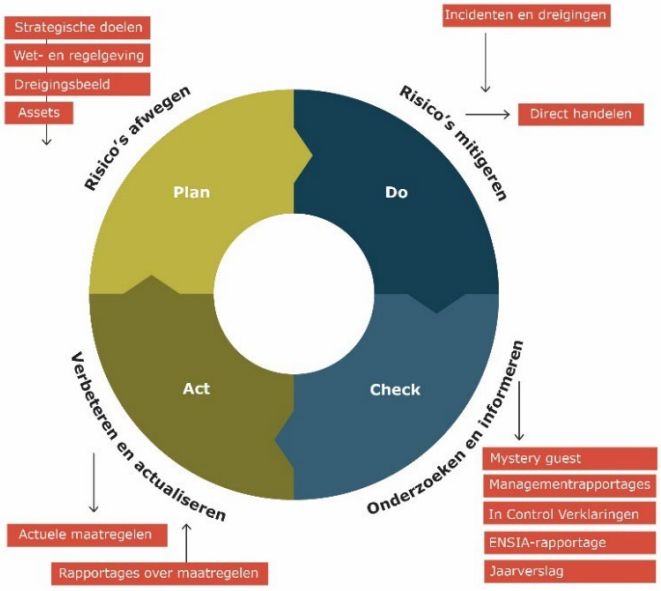
4. Informatiebeveiligingsproces en risicomanagement

Dit hoofdstuk beschrijft het informatiebeveiligingsproces, risicomanagement en het gemeenschappelijk informatiebeveiligingsniveau. Het doel is om inzicht te bieden in het proces van informatiebeveiliging, de aansturing van dit proces en de samenhang met de bedrijfsprocessen van Gemeente Boxtel.

4.1. Informatiebeveiligingsproces (PDCA-cyclus)

Informatiebeveiliging is een continu verbeterproces. Het informatiebeveiligingsproces, beter bekend onder de naam Information Security Management System (ISMS), is conform ISO 27001[15] ingericht op basis van de Plan-Do-Check-Act-cyclus, zie onderstaand figuur. Aan de hand van de PDCA-cyclus zorgen we voor periodieke toetsing van de werking en de noodzaak van gekozen maatregelen en werken we aan een continue verbetering van onze informatiebeveiliging. Dat betekent dat maatregelen worden geïmplementeerd op basis van risicomanagement en een bewuste kosten-batenafweging. Op deze manier zorgen we voor een optimale beveiliging tegen minimale kosten.

De PDCA-cyclus wordt afgestemd op de P&C-cyclus, zodat informatiebeveiliging in lijn is met onze andere verantwoordingen. Door organisatie brede planning, uitvoering, evaluatie en verbeteringen wordt niet alleen informatiebeveiliging, maar ook de kwaliteit van de informatievoorziening verankerd in onze organisatie.



Figuur 3: informatiebeveiligingsproces

[15] ISO 27001 is een internationale informatiebeveiligingsstandaard, die in Nederland is uitgebracht als NEN-ISO/IEC 27001. De ISO 27001 beschrijft het proces van informatiebeveiliging (ISMS) en is daarmee een belangrijke basis voor de BIO. De norm maakt deel uit van Forum Standaardisatie en is daarmee verplicht voor alle overheden.

Het informatiebeveiligingsproces bestaat uit vier deelprocessen, namelijk:

1. Risico's afwegen (Plan)
2. Risico's mitigeren/beperken (Do)
3. Onderzoeken van en informeren over restrisico's (Check)
4. Verbeteren en actualiseren van maatregelen (Act)

4.1.1. RISICO'S AFWEGEN (PLAN)

Risicomanagement
Risicomanagement is het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van Beschikbaarheid, Integriteit en Vertrouwelijkheid alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.

Het informatiebeveiligingsproces begint met het maken van een expliciete en schriftelijke risicoafweging. Bij deze afweging wordt de mogelijke schade ingeschat als een informatiesysteem (tijdelijk) niet beschikbaar is, informatie niet integer is of in verkeerde handen valt. Daarnaast wordt ook rekening gehouden met de dreigingen waartegen bescherming nodig is. De combinatie van de ingeschatte schade en dreigingen leidt tot de beveiligingseisen waarmee het risico kan worden beperkt. Deze eisen worden afgedekt door adequate maatregelen te treffen of het (rest)risico te accepteren.

Betrouwbaarheidsniveaus (BBN's)
De Baseline Informatiebeveiliging Overheid (BIO) vereenvoudigt het proces van risicomanagement en ondersteunt het lijnmanagement bij het nemen van de eigen verantwoordelijkheid. De BIO definieert een aantal basisbeveiligingsniveaus (BBN's) die proportioneel zijn aan de te beschermen belangen en relevante dreigingen. Voor elk informatiesysteem bepaalt het lijnmanagement het benodigde BBN aan de hand van een risicoafweging, bijvoorbeeld met behulp van de Baselinetoets BBN BIO of de Quickscan Information Security (QIS). De BIO onderscheidt drie BBN's, namelijk:

- BBN1: bij dit laagste betrouwbaarheidsniveau gaat het om wat minimaal van de overheid verwacht mag worden voor de bescherming van haar informatie. Met BBN1 is het mogelijk om voor eenvoudigere bedrijfsprocessen zonder vertrouwelijke informatie aan minder complexe verantwoordingseisen en risicomanagement te voldoen, waarbij nog altijd wel een minimum beveiligingsniveau wordt gewaarborgd;
- BBN2: dit standaardniveau is van toepassing op vrijwel alle informatie(systemen) van onze gemeentelijke organisatie. Het gaat om maatregelen die horen bij goed huisvaderschap van informatie. Alleen met een goede en vastgelegde onderbouwing kan bij individuele informatiesystemen hiervan afgeweken worden;

- BBN3: dit hoogste betrouwbaarheidsniveau vraagt om aanvullende maatregelen als weerstand tegen statelijke actoren, criminele organisaties of vergelijkbare actoren nodig is. De BIO schrijft geen standaard maatregelen voor op dit niveau. Maatwerk is dus nodig. Dit niveau is niet of nauwelijks van toepassing is op gemeentelijke organisaties. Omdat in enkele gevallen toch een hoger niveau nodig is dan BBN2, heeft de Informatiebeveiligingsdienst (IBD) een extra niveau toegevoegd: BBN2+. Dit niveau is voorzien van een aanvullende set maatregelen op de BIO.

Controls en verantwoordelijkheden

De BIO beschrijft per BBN aan welke controls[16] uit de ISO 27002[17] moet worden voldaan. Voor alle controls geldt dat op basis van een individuele risicoafweging bepaald moet worden hoe aan de beveiligingsdoelstelling van de control kan worden voldaan. Een aantal controls zijn uitgewerkt in verplichte en concrete overheidsmaatregelen. Alle controls zijn toegewezen aan specifieke rollen, zodat de verantwoordelijkheden makkelijker verdeeld kunnen worden. Op deze manier kan bijvoorbeeld de dienstenleverancier, die de vereiste deskundigheid heeft, bepalen welke specifieke maatregelen genomen moeten worden om invulling te geven aan de control.

Risicoafweging of -analyse

Indien op basis van een risicoafweging of –analyse blijkt dat het beveiligingsniveau van de BIO niet toereikend is[18], dan bepaalt de systeemeigenaar door middel van een diepgaande risicoanalyse welke aanvullende maatregelen boven op de BIO moeten worden getroffen voor zijn informatiesysteem. Op basis van risicomanagement zal dan een kostenafweging moeten worden gemaakt om te bepalen of de maatregelen doeltreffend zijn.

Risicoafwegingen die leiden tot het (tijdelijk) afwijken van de BIO worden uitgewerkt in een risicoanalyse, na afstemming met de CISO voorgelegd aan de bevoegde lijnmanager en vastgelegd ten behoeve van de periodieke zelfevaluatie. Afdeling overstijgende afwijkingen worden voorgelegd aan de directie en de CISO en/of de FG.

[16] Een control is een beheersmaatregel met als doel om een beveiligingsrisico te beheersen. Een deel van de controls is in de BIO uitgewerkt in verplichte overheidsmaatregelen.
[17] ISO 27002 is een internationale informatiebeveiligingsstandaard die in Nederland is uitgebracht als NEN-ISO/IEC 27002. Deze standaard geeft handreikingen voor de implementatie van de ISO 27001-maatregelen (controls) en is verplicht voor alle overheden.
[18] De BIO dekt alleen maatregelen af op niveaus BBN1 en BBN2.

Principes bij risicomanagement

Gemeente Boxtel hanteert de volgende principes bij risicomanagement:

- Het lijnmanagement bepaalt in overleg met de CISO wat goed is op basis van het afwegen van risico's, kosten, reputatieschade en eventuele andere factoren;
- 100% veilig bestaat niet! Het is onmogelijk om alle risico's uit te bannen;
- Gemeente Boxtel kiezen een beveiligingsbeleid waarbij de kosten van maatregelen in verhouding staan metde te beschermen belangen en de ernst van dreigingen;
- De keten is zo sterk als de zwakste schakel: een kwetsbaarheid in de beveiliging bij het ene organisatieonderdeel mag niet leiden tot onacceptabele risico's voor een ander organisatieonderdeel. Het accepteren van restrisico's geschiedt op het niveau dat bevoegd is op het hele domein waar de kwetsbaarheid tot schade kan leiden.

4.1.2. RISICO'S MITIGEREN/BEPERKEN (DO)

De lijnmanager brengt (rest)risico's terug tot een aanvaardbaar niveau door:

- Het nemen van maatregelen;
- Te reageren op incidenten uit de bedrijfsprocessen;
- Aan het begin van een project of wijziging met een ICT-component expliciet de betrouwbaarheidseisen mee te nemen bij de aanschaf en/of ontwikkeling van een informatiesysteem en gebruik te maken van een informatiebeveiligingsarchitectuur.

Documentatie maatregelen en aantoonbaarheid

Alle maatregelen die zijn gekozen op basis van de risicoanalyse, in reactie op incidenten, of voorgeschreven door de BIO, moeten worden gedocumenteerd. Van maatregelen moet de effectiviteit aantoonbaar zijn.

4.1.3. ONDERZOEKEN EN INFORMEREN (CHECK)

In het kader van de P&C-cyclus wordt minstens een keer per jaar onderzocht of de effectiviteit van de getroffen maatregelen nog is zoals bedoeld en of er voortgang is geboekt op openstaande verbetertrajecten met betrekking tot de BIO-zelfevaluatie (ENSIA), evenals andere beveiligingsonderzoeken zoals kwetsbaarheidsscans, pentesten, phishingcampagnes en audits. Elk team moet ervoor zorgen dat de informatiebeveiliging up-to-date is. Indien een afdeling eigenaaris van een informatiesysteem dan moeten contracten met een informatiebeveiligingsparagraaf en/of Service Level Agreement (SLA) worden gecontroleerd op naleving. Eventuele bevindingen worden aan het management gerapporteerd en kunnen leiden tot het actualiseren van de maatregelen en/of het beveiligingsproces. De CISO kan de lijnmanager adviseren naar aanleiding van de uitkomsten.

4.1.4. VERBETEREN EN ACTUALISEREN (ACT)

De afhankelijkheid en kwetsbaarheid van informatiesystemen verandert voortdurend als gevolg van ontwikkelingen in de maatschappij, bedrijfsprocessen en techniek. Beleid, betrouwbaarheidseisen en maatregelen moeten daarom nauwlettend in de gaten gehouden worden en periodiek, of naar aanleiding van incidenten, dreigingen, audits, zelfevaluaties of andere onderzoeken, herzien en eventueel aangepast worden. Om de kans op beveiligingsincidenten te verkleinen en reputatieschade te voorkomen, dienen verbetertrajecten (bijvoorbeeld inzake de BIO) tijdig te worden uitgevoerd.

4.2. Aansturen van het proces

Informatiebeveiliging gaat in essentie om het voortdurend bepalen van risico’s, het nemen van passende maatregelen op basis van risicomanagement en het tijdig reageren op incidenten. Om deze risico’s te bewaken en te beheersen moet een informatiebeveiligingsproces zijn ingericht. Dit informatiebeveiligingsproces wordt aangestuurd door het lijnmanagement (de business), omdat daar de verantwoordelijkheid ligt voor informatiebeveiliging. De lijnmanagers worden eventueel ondersteund door de beveiligingsbeheerders in de eerste lijn, en de CISO en ISO in de tweede lijn. Voor meer informatie zie het Three Lines Model in hoofdstuk 3.

5. Evaluatie, toetsing en verantwoording

In dit hoofdstuk worden de evaluatie, verantwoording, toetsing en toezicht beschreven. Het doel van dit hoofdstuk is om inzicht te krijgen in hoe Gemeente Boxtel zich op een transparante wijze verantwoord over informatiebeveiliging.

5.1. Evaluatie

Het strategische informatiebeveiligingsbeleid en bijbehorende uitgangspunten worden minimaal één keer per vier jaar, of bij belangrijke wijzigingen beoordeeld en zo nodig bijgesteld. Het lijnmanagement evalueert en actualiseert de informatiebeveiliging van de eigen informatiesystemen minimaal een keer per jaar, of eerder bij belangrijke wijzigingen.

5.2. Toetsing

Er vinden periodiek audits, zelfevaluaties, kwetsbaarheidsscans, penetratietesten, phishingcampagnes en mysteryguest-onderzoeken plaats om de opzet, het bestaan en de werking van beveiligingsmaatregelen te controleren en te beoordelen of aan de beveiligingsnormen van de BIO wordt voldaan. In het kader van de cloudstrategie zal het controleren van Cloud leveranciers een steeds prominentere rol moeten krijgen. Als normen niet correct of volledig zijn uitgevoerd, dan moeten deze normen mogelijk alsnog achteraf worden uitgevoerd. Zowel interne (bijvoorbeeld de proces- of systeemeigenaar) of externe partijen (bijvoorbeeld de rekenkamercommissie) kunnen opdracht geven om een toetsing uit te voeren en een rapportage op te leveren.

De CISO biedt periodiek inzicht in de stand van zaken op het gebied van informatiebeveiliging door middel van managementrapportages. Op basis van de managementrapportages kan het management de betrouwbaarheidseisen en het beveiligingsprocesaanpassen en daarmee sturen op de informatiebeveiliging.

5.3. Verantwoording

In lijn met de P&C-cyclus verantwoordt Gemeente Boxtel zich jaarlijks over informatiebeveiliging. De zelfevaluaties en audits vanuit ENSIA, de In Control Verklaringen[32] van de verschillende organisatieonderdelen, en andere onderzoeken vormen tezamen de basis voor de organisatie brede In Control Verklaring en dus het organisatie brede informatiebeveiligingsbeeld. Gemeente Boxtel is zo in staat om te laten zien hoe ze ervoor staat op het gebied van informatiebeveiliging, wat de grootste risico’s zijn op het gebied van compliance én de daadwerkelijke informatiebeveiliging.

Horizontale en verticale verantwoording

In het kader van ENSIA vindt horizontale verantwoording plaats aan de gemeenteraden en verticale verantwoording aan de stelselhouders van het Rijk, waar het gaat om het gebruik van de landelijke voorzieningen.

6. Bewustwording

Dit laatste, maar misschien wel meest belangrijke hoofdstuk gaat over bewustwording: zijn wij ons wel bewust van ons handelen en welke risico's dit met zich meebrengt? Bewustwording onder alle medewerkers zorgt ervoor dat iedereen zijn verantwoordelijkheid neemt en een bijdrage levert aan het verbeteren van onze veiligheidscultuur.

6.1. Zwakste en sterkste schakel

'If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology'.

Bruce Schneier[19]

Een goede informatiebeveiliging vereist niet alleen technische maatregelen, maar vraagt ook om het juiste gedrag van medewerkers. Onze informatiesystemen kunnen technisch nog zo goed zijn beveiligd zijn, verkeerd gedrag kan de beste beveiliging verzwakken of tenietdoen. Flexibel werken met mobiele apparatuur zoals smartphones, tablets en laptops biedt veel mogelijkheden, maar schept ook de noodzaak om op een integere en zorgvuldige wijze hiermee om te gaan. Informatie kan immers met een paar klikken op straat belanden.

De beveiligingsketen is zo sterk als de zwakste schakel. Het gedrag van medewerkers blijkt vaak de zwakste schakel, omdat medewerkers zich niet bewust zijn van hun manier van handelen en welke risico's dit met zich meebrengt. Denk bijvoorbeeld aan het gebruik van gratis apps op smartphones en gratis diensten in de cloud en de risico's bij openbare Wifi-netwerken. Technische maatregelen zijn niet altijd in staat deze problemen op te lossen. Daarom is het belangrijk om medewerkers bewust te maken van veilig gedrag en hen erop te wijzen welke risico's verbonden zijn aan hun werkzaamheden. Dit betekent niet alleen dat zij vertrouwelijke informatie als zodanig herkenbaar maken voor anderen, maar ook dat zij vertrouwelijke informatie slechts delen met anderen die deze informatie nodig hebben voor hun werkzaamheden (need-to-know in plaats van nice-to-know), en ervoor zorgen dat onbevoegden geen kennis kunnen nemen van deze informatie. Denk bij dit laatste bijvoorbeeld aan het veilig opbergen van informatie, het handhaven van het cleandesk- en clearscreen-principe, en informatie versleuteld verzenden.

[19] Bruce Schneier is een gerenommeerd Amerikaans deskundige op het gebied van informatiebeveiliging. Hij benadrukt dat technologie slechts een onderdeel is van het brede gebied van informatiebeveiliging

6.2. Activiteiten om de beveiligingsbewustwording te vergroten

Gemeente Boxtel zorgt voor beveiligingsbewustzijn door informatiebeveiliging als belangrijk en verplicht onderwerp mee te nemen in een gestructureerd Onboarding-proces voor nieuwe Medewerkers, bijvoorbeeld door middel van een basismodule of training. Nieuwe medewerkers krijgen zo niet alleen inzicht in de belangrijkste risico's en dreigingen, zoals het gebruik van onveilige wachtwoorden en phishing-aanvallen, maar krijgen ook praktische tips hoe deze risico’s vermeden kunnen worden.

Bewustwording is geen eenmalige activiteit en vraagt om permanente aandacht. Daarom vergroten we de bewustwording bij bestaande medewerkers door periodiek (jaarlijks) een basismodule of training verplicht te stellen en regelmatig gerichte activiteiten te organiseren. Denk hierbij bijvoorbeeld aan bewustwordingsprogramma’s in de vorm van inspiratiesessies, trainingen, campagnes, presentaties, gedragscodes en de nieuwsvoorziening. Zo zorgen we ervoor dat informatiebeveiliging altijd top-of-mind is.

Lijnmanagement

De lijnmanagers geven het goede voorbeeld en verlenen hun medewerking aan en ondersteunen de bewustwordingsactiviteiten. Daarnaast is de lijnmanager zelf ook verantwoordelijk voor het vergroten van de bewustwording van de eigen medewerkers. Dit kan bijvoorbeeld door het belang van informatiebeveiliging extra te benadrukken tijdens de eerste weken en maanden van een nieuwe medewerker of door informatiebeveiliging bespreekbaar te maken in werkoverleggen en in functioneringsgesprekken.

Bijlage A De 10 bestuurlijke principes voor informatiebeveiliging (VNG)

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.

   Ik ben mij bewust van de voorbeeldfunctie van een bestuurder en ik draag uit dat risicomanagement van iedereen is. Ik zorg daarom voor een cultuur waarin iedereen vrij is om dreigingen waar te nemen en te melden. In eerste instantie bij de verantwoordelijke, maar indien nodig ook bij mij als bestuurder. Ik spoor managers aan om voorwaarden te scheppen zodat iedereen binnen de organisatie deelgenoot wordt van het proces van risicomanagement. Ik zorg ervoor dat fouten besproken kunnen worden en dat daarmee een lerende organisatie ontstaat. Ten slotte geef ik in mijn eigen doen en laten het goede voorbeeld van hoe je verantwoordelijk omgaat met informatie.

   Toelichting
   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 u in uw organisatie een cultuur bevordert waarin mensen zich vrij voelen om risico's te melden en maatregelen voor te stellen, dan kunt u adequaat reageren op dreigingen en samenhangende risico's.

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.

   Ik maak medewerkers bewust van de risico's van het werken met informatie en ik maak risicomanagement onderdeel van het MT-overleg en laat het anderen in vergaderingen agenderen. Ik zorg ervoor dat iedereen risicomanagement toepast en dat het gezien wordt als vanzelfsprekend en nuttig. Ik ben transparant naar de raad en zorg ervoor dat hij ook zijn rol kan pakken op dit onderwerp.

Toelichting

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 uw Chief Information Security Officer (CISO), Functionaris Gegevensbescherming (FG) en Controller als onafhankelijke adviseur en laat ze samenwerken in een risicoteam, waar u vanzelfsprekend ook zitting in heeft. Laat uw interne communicatie aandacht besteden aan het verspreiden van de boodschap, het belang en het voordeel van risicomanagement binnen uw 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.

Ik zorg dat risicomanagement een onderdeel is van het bestuurlijk overleg en dialoog. Daarnaast zal ik het integreren in het risicobewustzijn van alle medewerkers en het onderdeel laten zijn van de samenwerking met partners en ik zorg ervoor dat risicomanagement integraal onderdeel uitmaakt van uitbestedingen en samenwerkingen. Ik zorg ervoor dat risicomanagement geformaliseerd wordt binnen de hele organisatie met een duidelijke verdeling van verantwoordelijkheden en heldere besluitvorming.

Toelichting

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.

Ik maak medewerkers mede-eigenaar van het risicoproces op het vlak van informatieveiligheid en ik maak informatiebeveiliging onderwerp van alle overlegstructuren. Ik draag er zorg voor dat besluiten ten aanzien van de omgang met risico's expliciet genomen en vastgelegd worden. Ik laat risicomanagement naadloos aansluiten op de strategische en beleidsmatige doelstellingen van de organisatie. Op deze wijze bied ik een duidelijk kader waarbinnen de medewerkers kunnen opereren.

Toelichting
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 is aangepast en staat in verhouding tot de externe en interne context van de organisatie die verband houdt met haar doelstellingen.

Ik zorg dat ik de risico's ken die een gevaar vormen voor de informatievoorziening van de bedrijfsvoering van de gemeente en ik anticipeer op risico's die voortkomen uit het werken in ketens en ik houd rekening met de complexiteit, de onzekerheid en ambiguïteit in de samenwerking met anderen. Bij samenwerken of uitbesteden van (delen) van de organisatie of processen zorg ik ervoor dat de risico's in kaart gebracht zijn, verantwoordelijkheden verdeeld en dat de juiste maatregelen getroffen worden.

Toelichting
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.

Ik zorg ervoor dat risicomanagement cyclisch is en daarmee kan ik reageren op veranderingen en toekomstgericht sturen. Het staat daarom regelmatig op de agenda.

Toelichting
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.

Ik zorg ervoor dat er voldoende middelen beschikbaar zijn om de onderkende risico's op een adequate manier te behandelen. Als gebleken is dat een risico een bedreiging is voor de organisatiedoelstellingen en er maatregelen genomen moeten worden, dan zorg ik er ook voor dat de middelen beschikbaar zijn om deze maatregelen uit te voeren.

Toelichting
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.

Risicomanagement is gebaseerd op de best beschikbare informatie vanuit mijn organisatie en vanuit mijn samenwerkingen. Ik zorg ervoor dat alle belanghebbenden op een gestructureerde en voorspelbare wijze informatie delen die bijdraagt aan risicomanagement.

Toelichting
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.

Door mijn inzet zorg ik ervoor dat risico gestuurd werken doorontwikkeld wordt. Ik reflecteer op ervaringen en ik nodig medewerkers uit tot het delen van ervaringen met betrekking tot de risico's die de informatievoorziening bedreigen. Ik zorg ervoor dat de organisatie kan leren van incidenten en dat de organisatie leert te ontdekken wat wel en wat niet werkt.

Toelichting

Risicomanagement gedijt het beste in een organisatie die leert van ervaringen en op basis hiervan verbeteringen doorvoert. Hoe goed u uw informatiehuishouding ook beveiligt, 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.

Ik geef opdracht om de werking van risicomanagement binnen mijn organisatie op effectiviteit en efficiency te (laten) controleren. Naast managementrapportages zijn (externe) controles de manier om te weten te komen of en hoe het beleid in de praktijk uitwerkt. Als bestuurder weeg ik goed geïnformeerd risico's en belangen af en neem ik mijn verantwoordelijkheid om knopen door te hakken.

Toelichting
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 B Rollen en verantwoordelijkheden

Binnen het brede terrein van de informatievoorziening zijn er verschillende partijen actief die allemaal verantwoordelijkheid dragen voor de beveiliging van onze voorzieningen en informatie. Deze verantwoordelijkheden komen voort uit de Baseline Informatiebeveiliging Overheid (BIO) en geldende wet- en regelgeving. Hieronder worden de verschillende rollen en bijbehorende verantwoordelijkheden voor informatiebeveiliging beschreven. De rollen en verantwoordelijkheden bij een cybercrisis worden apart beschreven in het cybercrisisplan.

Gemeenteraden

De gemeenteraden zijn bevoegd voor de controle en toetsing op de werking van beleid binnen de gemeente, zo ook voor informatiebeveiliging. De colleges van B en W leggen middels de Eenduidige Normatiek Single Information Audit (ENSIA) jaarlijks verantwoording af aan de raden middels de zelfevaluaties over de BIO, BRP, Reisdocumenten, WOZ, BAG, BGT en BRO. Aan de raad wordt ook verantwoording afgelegd via de collegeverklaring ENSIA waarin de auditor een assurance afgeeft over onze DigiD-aansluitingen en het gebruik van Suwinet. Verder vindt er in het jaarverslag verantwoording plaats in de paragraaf over informatiebeveiliging en privacy.

Colleges van burgemeesters en wethouders en het dagelijks bestuur

De colleges van burgemeesters en wethouders en het dagelijks bestuur zijn eindverantwoordelijke voor een passend niveau van informatiebeveiliging in onze organisatie. Zij stellen met het voorliggende beleidsdocument de kaders vast ten aanzien van informatiebeveiliging. De burgemeesters zijn portefeuillehouder voor informatiebeveiliging.

Gemeentesecretarissen

- Zijn ambtelijk eindverantwoordelijk voor de implementatie, borging en uitvoering van het informatiebeveiligingsbeleid door alle lijnmanagers, inclusief concernmanagers en teammanagers;
- Stelt in overleg met het college, het management en de CISO het gewenste niveau van informatiebeveiliging vast.

Derde lijn) fraude en/of fouten kunnen worden voorkomen en transparantie in de besluitvorming is gewaarborgd;
- Laat controleren of de getroffen beveiligingsmaatregelen overeenstemmen met de betrouwbaarheidseisen en dreigingen en of deze beveiligingsmaatregelen voldoende bescherming bieden;
- Ziet toe op de naleving van het informatiebeveiligingsbeleid bij de verschillende organisatieonderdelen;
- Rapporteert minimaal een keer per jaar aan het college over informatiebeveiliging.

Lijnmanager
- Is verantwoordelijk voor de implementatie, uitvoering en naleving van het informatiebeveiligingsbeleid binnen het eigen organisatieonderdeel;
- Is eindverantwoordelijk voor de informatiebeveiliging van de processen, systemen en gegevens binnen het eigen organisatieonderdeel;
- Zorgt dat de eigen medewerkers zich bewust zijn van hun verantwoordelijkheid voor informatiebeveiliging in hun dagelijkse werkprocessen, dat ze weten hoe zorgvuldig om te gaan met (vertrouwelijke) informatie, en dat ze de risico's begrijpen die op dit gebied aanwezig zijn;
- Is verantwoordelijk voor adequaat autorisatiebeheer (logisch en fysiek) van de eigen medewerkers, zodat zij slechts die toegangsrechten hebben die nodig zijn voor het uitvoeren van hun taken (need-to-know-principe);
- Stelt aan de hand van een expliciete risicoafweging de betrouwbaarheidseisen (uitgedrukt in een betrouwbaarheidsniveau) vast voor elk informatiesysteem waarvan men eigenaar is, en kiest en beschrijft op basis daarvan een samenhangend pakket van bijbehorende maatregelen;
- Laat een dataclassificatie uitvoeren bij het ad hoc uitwisselen van data waarvan men eigenaar is, en kiest en beschrijft op basis daarvan een samenhangend pakket van bijbehorende maatregelen;
- Draagt zorg voor de implementatie van de beveiligingsmaatregelen en laat periodiek (minimaal jaarlijks) controleren of de getroffen maatregelen aantoonbaar overeenstemmen met de betrouwbaarheidseisen en dat de maatregelen worden nageleefd;
- Waarborgt de continuïteit van zijn kritische processen[35] door aan de hand van een business continuïteitsplan (BCP) processen, procedures en passende beheersmaatregelen vast te stellen, te implementeren en periodiek (jaarlijks) te verifiëren, beoordelen en evalueren op doeltreffendheid;
- Zorgt ervoor dat nieuwe medewerkers binnen drie maanden een verplichte basismodule en training hebben gevolgd en dat bestaande medewerkers periodiek (jaarlijks) een verplichte basismodule en training voor informatiebeveiliging volgen;

- Betrekt de CISO of ISO bij de informatiebeveiliging van (te implementeren) informatiesystemen. Het advies van de CISO is zwaarwegend bij het nemen van beslissingen;
- Neemt informatiebeveiliging als paragraaf op in het afdelingsplan, zodat jaarlijks duidelijk wordt hoe informatiebeveiliging wordt verbeterd;
- Is eindverantwoordelijkheid voor de melding en afhandeling van incidenten en inbreuken op de informatiebeveiliging binnen zijn organisatieonderdeel;

Chief Information Security Officer (CISO)

- Ontwikkelt en actualiseert de visie, kaders en richtlijnen voor informatiebeveiliging en adviseert het lijnmanagement hierover;
- Adviseert het lijnmanagement en het bestuur gevraagd én ongevraagd over informatiebeveiliging en de risico's van (voorgenomen) wet- en regelgeving, investeringen, beleids- en uitvoeringstrajecten, informatieprocessen en -systemen;
- Draagt bij aan de ontwikkeling van standaarden, normen en beleidsinstrumenten op het gebied van informatiebeveiliging;
- Draagt het beleid en de normen uit door middel van presentaties, voorlichting, communicatiecampagnes en workshops;
- Ontwikkelt en actualiseert het organisatie brede risicobeeld met betrekking tot informatiebeveiliging;
- Ontwikkelt de informatiebeveiligingsfunctie op basis van het informatiebeveiligingsbeleid;
- Monitort en controleert het informatiebeveiligingsbewustzijn binnen de organisatie en zorgt voor het vergroten van het bewustzijn;
- Bewaakt dat het informatiebeveiligingsbeleid wordt nageleefd voor nieuwe en bestaande ICT-oplossingen door projecten en wijzigingen te (laten) beoordelen op correcte toepassing van de gestelde kaders;
- Ziet toe op en evalueert de uitvoering van het informatiebeveiligingsbeleid conform de Plan-Do-Check-Act-cyclus;
- Rapporteert vanuit een onafhankelijke positie aan het lijnmanagement en bestuur;
- Beoordeelt of informatiebeveiliging toereikend is;
- Onderhoudt relaties met de Informatiebeveiligingsdienst (IBD), onder andere in het kader van dreigingen die verband houden met de informatiebeveiliging van Gemeente Boxtel;
- Volgt de interne en externe invloeden die van invloed zijn op het informatieveiligheidsbeleid.

Functionaris voor Gegevensbescherming (FG): houdt binnen Gemeente Boxtel onafhankelijk toezicht op de naleving van de AVG en aanverwante privacywetgeving en geeft hierover advies.

Privacy Officer: draagt bij aan de privacy compliance van de organisaties. De Privacy Officer kent een (juridisch-)coördinerende invulling.

(Functioneel) applicatiebeheerder

- Is operationeel verantwoordelijk voor de beschikbaarheid en kwaliteit van het informatiesysteem/de applicatie;
- Zorgt, in afstemming met de proceseigenaar, dat iedere medewerker slechts die toegangsrechten heeft die nodig zijn voor het uitvoeren van zijn taken (need-to-know-principe);
- Zorgt dat de applicatie voldoet aan het security-by-design- en security-by-default-principe;
- Richt organisatorische of technische beveiligingsmaatregelen in op basis van het informatiebeveiligingsbeleid;
- Richt beveiligingsmaatregelen in afstemming met de systeemeigenaar in;
- Zorgt voor bewustwording en creëert draagvlak zodat gebruikers rekening houden met informatiebeveiliging bij het gebruik van de applicatie;
- Rapporteert beveiligingsincidenten bij de helpdesk en de betreffende proces- en/of systeemeigenaar;
- Is aanspreekpunt voor het lijnmanagement, dienstenleveranciers en gebruikers bij de informatiebeveiliging van de applicatie;
- Vervult een proactieve rol en is aanspreekpunt voor zijn applicatie bij beveiligingsincidenten of dreigingen;
- Controleert twee keren per jaar of alle autorisaties nog actueel zijn en stemt dit af met de proces- en/of systeemeigenaar;
- Rapporteert minstens twee keren per jaar over informatiebeveiliging aan de systeemeigenaar.

Interne dienstenleverancier

- Beveiligt de IT-infrastructuur en waarborgt dat alleen geautoriseerde gebruikers toegang hebben tot informatiesystemen (need-to-know-principe);
- Past de principes security-by–design en security-by–default toe bij de aanschaf, ontwikkeling en onderhoud van systemen;
- Houdt bij de aanschaf, ontwikkeling en onderhoud rekening met de inkoopbeleidsregels (onder andere GIBIT) en maatregelen uit de BIO;
- Voldoet aan de verplichte (ICT-)standaarden van Forum Standaardisatie;
- Legt periodiek (jaarlijks) verantwoording af door middel van een In Control Verklaring (ICV);
- Rapporteert over informatiebeveiligingsincidenten aan de opdrachtgever.

ENSIA-coördinator

- Coördineert het ENSIA-proces voor de verantwoording over informatiebeveiliging (en de kwaliteit van gegevens) aan de gemeenteraden en aan de rijksoverheid waar het gaat om het gebruik van landelijke voorzieningen;
- Interviewt proceseigenaren en andere relevante rollen en verwerkt de antwoorden in ENSIA;
- Stelt rapportages op en stemt de resultaten af met het lijnmanagement en de CISO;
- Stelt op basis van de rapportages verbetervoorstellen voor aan de CISO;
- Coördineert de auditwerkzaamheden en is aanspreekpunt van de auditor;
- Voert de rapportages op voor de (horizontale) verantwoording aan de gemeenteraden;
- Voert de rapportages op in ENSIA ten behoeve van de (verticale) verantwoording aan de landelijke toezichthouders.

Teammanager ICT

- Ontwikkelt en onderhoudt de organisatie brede architectuur en standaarden;
- Bewaakt de samenhang in de informatievoorziening en ICT-projecten door applicatie- en Projectportfoliomanagement (PPM) toe te passen met een overzicht van alle informatiesystemen en hun eigenaars;
- Signaleert aan het betrokken organisatieonderdeel en de CISO als een organisatieonderdeel een nieuw informatiesysteem in productie wil nemen en een risicoanalyse ontbreekt.

Gebouwenbeheer

- Is verantwoordelijk voor de fysieke beveiliging van gebouwen en goederen;
- Stelt fysieke beveiligingszones vast ter bescherming van gevoelige of essentiële informatie;
- Zorgt voor fysieke toegangsbeveiliging zodat alleen bevoegd personeel toegang krijgt;
- Stelt maatregelen vast en implementeert deze om fysieke bescherming te bieden tegen bedreigingen van buitenaf, zoals kwaadwillige aanvallen, ongelukken of natuurrampen.

Personeel en Organisatie (P&O)

- Is in het kader van informatiebeveiliging verantwoordelijk voor de Onboarding van nieuwe medewerkers en de periodieke (jaarlijkse) organisatie brede training en educatie van bestaande medewerkers;
- Faciliteert en onderhoudt een online leeromgeving waar medewerkers (verplichte) kennis kunnen opdoen van informatiebeveiliging;
- Zorgt dat alle interne en externe medewerkers een specifiek voor de functie verstrekte Verklaring Omtrent het Gedrag (VOG) overleggen;
- Wijst, in overleg met de lijnmanager, medewerkers bij aanstelling of functiewisseling op hun verantwoordelijkheden ten aanzien van informatiebeveiliging.

Inkoop

- Is verantwoordelijk voor het inkoopproces en borgt dat informatiebeveiligingseisen expliciet opgenomen zijn in (inkoop)contracten.

Medewerker (inclusief externen)

- Is verantwoordelijk voor de toevertrouwde informatie, ICT-middelen en de daarop van toepassing zijnde informatiebeveiligingsmaatregelen;
- Krijgt enkel toegang tot informatiesystemen na identificatie, authenticatie en autorisatie door de bevoegde lijnmanager;
- Neemt eigen verantwoordelijkheid ten aanzien van de informatiebeveiliging en handelt volgens de gedragscode;
- Volgt zowel de richtlijnen en instructies[20] van Gemeente Boxtel als die van de leidinggevende op;
- Is verplicht om binnen drie maanden na indiensttreding de basismodule en training voor informatiebeveiliging te volgen;
- Is verplicht om periodiek (jaarlijks) de basismodule en training voor informatiebeveiliging te volgen;
- Rapporteert beveiligingsincidenten bij de helpdesk en de betreffende proces- en/of systeemeigenaar.

[20] Denk bijvoorbeeld aan de maatregel dat informatie volgens de cleandesk- en clearscreenpolicy wordt afgeschermd voor onbevoegden en niet onbeheerd mag worden achtergelaten.

Externe partijen

Externe dienstenleverancier

- Beveiligt de IT-infrastructuur en waarborgt dat alleen geautoriseerde gebruikers toegang hebben tot informatiesystemen (need-to-know-principe);
- Past de principes security-by–design en security-by–default toe bij de aanschaf, ontwikkeling en onderhoud van systemen;
- Voldoet aan de inkoopbeleidsregels (zoals de GIBIT) en de beveiligingsmaatregelen op basis van de BIO;
- Voldoet aan de verplichte (ICT-)standaarden van Forum Standaardisatie;
- Legt verantwoording af door middel van een In Control Verklaring (ICV of deel-ICV), assurancerapport, certificering of right-to-audit op basis van het type dienst en de zekerheid die de opdrachtgever vereist. Denk hierbij bijvoorbeeld aan een ISO 27001-certificaat inclusief Verklaring van Toepasselijkheid (VvT) voor de kwaliteit van het informatiebeveiligingsproces, een Statement of Compliance om de BIO-maatregelen af te dekken bij private partijen, eventueel een ISO22301-certificaat voor bedrijfscontinuïteitsbeheer, maar denk ook aan een ISAE3402-verklaring (SOC1, type I of II) voor beheersmaatregelen die relevant zijn voor de jaarrekening, en een ISAE3000-verklaring (SOC2 of SOC3, type I of II) voor beheersmaatregelen die relevant zijn voor de informatiebeveiliging, beschikbaarheid van systemen, verwerkingsintegriteit, vertrouwelijkheid en/of privacy van klantgegevens;
- Rapporteert over informatiebeveiligingsincidenten aan de opdrachtgever.

Rekenkamercommissie: ondersteunt de gemeenteraden bij zijn controlerende taken door onderzoek te doen naar de doeltreffendheid, doelmatigheid en rechtmatigheid van het gemeentelijk beleid. De rekenkamercommissie kan zelfstandig een onderzoek (laten) uitvoeren naar de informatiebeveiliging van onze organisatie en rapporteert hierover aan de gemeenteraden.

Externe partij in samenwerkingsverband

- Is verantwoordelijk om de gegevens die Gemeente Boxtel uitwisselt in de keten te beveiligen;
- Past de principes security-by–design en security-by–default toe bij de aanschaf, ontwikkeling en onderhoud van systemen;
- Is eindverantwoordelijk voor de bescherming van persoonsgegevens als deze conform AVG-verwerkersverantwoordelijke is;
- Voldoet, indien onderdeel van overheid, aan de beveiligingsmaatregelen van de BIO en anders aan de beveiligingsmaatregelen op basis van de BIO;
- Legt verantwoording af door middel van een In Control Verklaring (ICV of deel-ICV), assurancerapport (verklaring), certificering of right-to-audit op basis van het type dienst en de zekerheid die de opdrachtgever vereist. Denk hierbij bijvoorbeeld aan een ISO 27001-certificaat inclusief Verklaring van Toepasselijkheid (VvT) voor de kwaliteit van het informatiebeveiligingsproces, een Statement of Compliance om de BIO-maatregelen af te dekken bij private partijen, eventueel een ISO22301-certificaat voor bedrijfscontinuïteitsbeheer, maar denk ook aan een ISAE3402-verklaring (SOC1, type I of II) voor beheersmaatregelen die relevant zijn voor de jaarrekening, en een ISAE3000-

verklaring (SOC2 of SOC3, type I of II) voor beheersmaatregelen die relevant zijn voor de informatiebeveiliging, beschikbaarheid van systemen, verwerkingsintegriteit, vertrouwelijkheid en/of privacy van klantgegevens;

- Rapporteert over informatiebeveiligingsincidenten aan de betrokken samenwerkingspartijen.

Bijlage C Afkortingen en begrippenlijst

Afkorting/begrip	Definitie
AP	Autoriteit Persoonsgegevens
Baseline	Basisniveau, minimumniveau.
Baseline Informatiebeveiliging Overheid	Het verplichte basisnormenkader voor informatiebeveiliging voor alle overheidslagen.
Beschikbaarheid	Het waarborgen dat geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen).
BBN	Basis Beveiligings Niveau
BCM	Bedrijfscontinuïteitsbeheer (Business Continuity Management)
BCP	Zie business continuïteitsplan
BIO	Zie Baseline Informatiebeveiliging Overheid
BIV	Acroniem voor Beschikbaarheid, Integriteit en Vertrouwelijkheid
Business continuïteitsplan	Een business continuïteitsplan beschrijft welke procedures en instructies gevolgd moeten worden om te kunnen blijven opereren tijdens een ongeplande onderbreking van de bedrijfsvoering of dienstverlening. Het plan maakt onderdeel uit van bedrijfscontinuïteitsbeheer.
CISO	Chief Information Security Officer
Datalek	Een beveiligingsincident waarbij persoonsgegevens zijn betrokken.
Eenduidige Normatiek Single Information Audit	Verantwoordingproces dat gemeenten volgen om zich te verantwoorden over informatiebeveiliging aan de gemeenteraden en het Rijk.
ISO	Information Security Officer
ENSIA	Zie Eenduidige Normatiek Single Information Audit
FG	Functionaris voor Gegevensbescherming
IBD	Zie Informatiebeveiligingsdienst
IBP	Informatiebeveiligingsplan
In Control Verklaring	Met een In Control Verklaring (ICV) of In Control Statement (ICS) verklaart de organisatie (of een onderdeel ervan) dat zij voor haar bedrijfsvoering aan de beveiligingseisen voldoet. De ICV geeft inzicht aan welke beveiligingsnormen wordt voldaan en voor welke beveiligingsnormen een uitzondering is gedefinieerd.
Informatiebeveiligingsdienst	De Informatiebeveiligingsdienst is het Computer Emergency Response Team (CERT) voor alle Nederlandse gemeenten en is onderdeel van de Vereniging van Nederlandse Gemeenten.
Informatiebeveiligingsincident	Een gebeurtenis waardoor de vertrouwelijkheid, integriteit of beschikbaarheid van de informatievoorziening of informatie

	Ernstig gevaar loopt of die zich al als zodanig heeft voorgedaan.
Information Security Management System	Het Information Security Management System is een proces voor informatiebeveiliging dat gebaseerd is op de ISO 27001.
Informatiesysteem	Een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur, alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.
Informatievoorziening	Een informatievoorziening bestaat uit een verzameling, mogelijk samenhangende, informatiesystemen met elk een duidelijke eigenaar.
Integriteit	Het waarborgen van de juistheid en volledigheid van informatie en de verwerking ervan.
ISMS	Zie Information Security Management System
ISO	Information Security Officer
ISO 27001	ISO 27001 is een internationale informatiebeveiligings-standaard, die in Nederland is uitgebracht als NEN-ISO/IEC 27001. De ISO 27001 beschrijft het proces van informatiebeveiliging (ISMS) en is daarmee een belangrijke basis voor de BIO. De norm maakt deel uit van Forum Standaardisatie en is daarmee verplicht voor alle overheden.
ISO 27002	ISO 27002 is een internationale informatiebeveiligings-standaard die in Nederland is uitgebracht als NEN-ISO/IEC 27002. Deze standaard geeft handreikingen voor de implementatie van de ISO 27001-maatregelen (controls) en is verplicht voor alle overheden.
3LoD	Zie Three Lines of Defense
NORA	De Nederlandse Overheid Referentie Architectuur (NORA) is het interoperabiliteitsraamwerk voor de Nederlandse overheid en vertaalt daartoe wetgeving, beleid en standaarden naar architectuurprincipes, beschrijvingen en modellen.
Operational Technology	Operational Technology (OT), ook wel bekend onder de naam Procesautomatisering (PA), is een verzamelnaam voor verschillende systemen die worden gebruikt voor het beheer van operationele processen in de fysieke wereld, zoals het aansturen en monitoren van (industriële) apparatuur.
OT	Zie Operational Technology
PO	Privacy Officer
PPM	Projectportfoliomanagement
Procesautomatisering (PA)	Zie Operational Technology
Risico	De kans op het optreden van een ongewenste gebeurtenis of situatie vermenigvuldigd met de daaruit voortvloeiende schade (impact)
Risicomanagement	Het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van Beschikbaarheid, Integriteit en Vertrouwelijkheid alsmede het treffen, onderhouden en controleren van een samenhangend pakket Van bijbehorende maatregelen.

Three Lines of Defense (3LoD)	Het Three Lines of Defense model is een wereldwijd gebruikt raamwerk voor risicobeheer en compliance en draagt bij aan een effectieve informatiebeveiliging.
VDW	Zie Verhogen Digitale Weerbaarheid
Verhogen Digitale Weerbaarheid	Modules die door de Informatiebeveiligingsdienst worden aangeboden om de basis van informatiebeveiliging op orde te krijgen.
Vertrouwelijkheid	Het waarborgen dat informatie alleen toegankelijk is voor diegenen die hiertoe zijn geautoriseerd.