de BUCH

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 1158

11 november 2020

Officiële uitgave van de gemeenschappelijke regeling Werkorganisatie BUCH

Strategisch Gemeentelijk Informatiebeveiligingsbeleid Werkorganisatie BUCH 2020 - 2023

De BUCH werkt voor de gemeenten Bergen, Uitgeest, Castricum en Heiloo

Verspreiding

Functie	Actie	v0.9	V0.95	V0.99	V1.0
CISO	Concept opstellen	13-05-2020			
CISO	Concept definitief maken				18-06-2020
Privacy Officer	Afstemmen t.a.v. privacy en vorm/inhoud		28-05-2020	06-06-2020	
Domein manager bedrijfsvoering					29-5-2020
PH en AD BUCH	Afstemmen voordat het de besluitvormingsroute ingaat				
MT BV	Besluiten voorleggen aan MT BUCH				1-7-2020
AJZ	Juridische afstemming, intrekken oude documenten en publicatie		2-6-2020		
Control					
MT BUCH	Kennis van nemen en voorleggen aan bestuur BUCH				
Bestuur BUCH	Vaststellen voor de BUCH en besluiten ter besluitvorming voor te leggen aan Het college				
Colleges B&W	Vaststellen voor de gemeente en besluiten de raden te informeren				
Gemeenteraad	Kennis nemen				

Goedkeuring

Versie	Datum	Opmerkingen	Akkoord (naam, datum, paraaf)
0.90 0.95 0.99	13-05-2020 28-05-2020 06-06-2020	Concept Concept 2 definitief Concept 3	
1.0	18-06-2020	Definitief	

1. Inleiding

De Werkorganisatie BUCH en de gemeentelijke organisatie valt of staat met informatie. Over de gehele breedte van de organisatie en de gemeenten, kunnen we niets zonder informatie en informatiesystemen. Daarom is het van belang dat wij onze informatie beveiligen tegen ongewenste toegang, ongewenste wijziging, ongewenste aantasting en de beschikbaarheid garanderen. Daarnaast kunnen onze inwoners geen andere overheid kiezen en vertrouwen er dus op dat we hun vertrouwelijke gegevens afdoende beveiligen. Daarom werken we continue aan de Informatiebeveiliging binnen onze gemeenten. Het gehele bestuur van de Werkorganisatie en de BUCH gemeenten, dus zowel de politieke en ambtelijke bestuurders als ook de leidinggevenden, geven een duidelijke richting aan informatiebeveiliging. Dit doen zij door het tonen van betrokkenheid, het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor de hele Werkorganisatie en de BUCH gemeenten. Dit beleid is van toepassing op alle processen, organisatieonderdelen, objecten (zoals ook gebouwen, gemalen en bruggen), informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid van de Werkorganisatie BUCH is in lijn met het algemene beleid van de Organisatie en de BUCH gemeenten en de relevante landelijke en Europese wet- en regelgeving. Het informatiebeveiligingsbeleid zal jaarlijks geëvalueerd worden en in geval van grote incidenten of het nog voldoet aan de behoefte van de BUCH en relevante wet en regelgeving. Dit beleid wordt vastgesteld voor de periode 2020 tot 2023 voor de Werkorganisatie BUCH en de gemeenten Bergen, Uitgeest, Castricum, Heiloo. bestaand informatiebeveiligingsbeleid zal moeten worden ingetrokken ten gunste van dit beleid.

1.1. Reden voor een actueel Strategisch Informatiebeveiligingsbeleid

Een aantal ontwikkelingen maken het noodzakelijk, om het Informatiebeveiligingsbeleid te actualiseren en opnieuw vast te stellen:

1. Informatiebeveiliging is geen vrijblijvendheid meer, gezien de toenemende cybercrime, waarbij hacks op zowel landelijk- als regionaal niveau vrijwel dagelijks voorkomen. Vanuit het Rijk, de landelijke en Europese politiek wordt daarom veel ingezet om de gemeente op dit gebied te professionaliseren. Zie de verplichtingen vanuit de in november 2013 door de gemeenten aanvaarde VNG-resolutie 'Informatiebeveiliging, als randvoorwaarde voor de professionele gemeente', zoals het:
   - Aansluiten op de IBD (Informatiebeveiligingsdienst);
   - Implementeren van en expliciet voldoen aan de 'Baseline Informatiebeveiliging Overheid' (BIO);
   - Het doorvoeren van ENSIA, als horizontale en verticale verantwoordingsstelsel voor de informatiebeveiliging gebaseerd op de BIO.

   De verantwoordingssystematiek over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale Persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet) is samengevoegd en gestroomlijnd. Uitgangspunt van ENSIA is de single information audit. Dit betekent dat maar één keer per jaar de zelfevaluatielijst ingevuld dient te worden en de informatie hieruit wordt gebruikt voor de horizontale verantwoording richting gemeenteraad en de diverse verticale verantwoordingslijnen richting departementen. De horizontale verantwoording bestaat uit de zelfevaluatie, een IT-audit, een verklaring van het College van B&W en een passage over Informatiebeveiliging in het jaarverslag.
2. De opkomst van 'moderne' technologieën', zoals de doorontwikkeling van de digitale (internet)dienstverlening (conform ons 'organisatiedoelen') en cloudoplossingen, die echter ook weer bedreigingen voor de Informatiebeveiliging met zich meebrengen (de zogenaamde, inmiddels beruchte cybercriminaliteit). Denk tevens aan de toenemende inzet van mobiele apparaten zoals smartphones en tablets en de toepassing van Internet of Things in het publiek domein. Zo bieden dergelijke apparaten onze organisatie kansen op het gebied van bereikbaarheid, flexibiliteit en inzet op locatie. Echter, het is zaak om adequaat te handelen in geval bijvoorbeeld een smartphone of tablet ergens 'vergeten' of wellicht ontvreemd is. Een goede beveiliging van de mobiele apparaten en de daarop aanwezige gegevens is van een niet te onderschatten wezenlijk belang.
3. De overheveling van rijkstaken naar de gemeenten, zoals de in 2015 in werking getreden decentralisaties. Het gaat hier niet alleen meer om de lokale gemeentelijke Informatiebeveiliging. De mogelijke bedreigingen en risico's strekken verder dan het eigen gemeentelijk grondgebied. Deze schaalvergroting en het gebruik van uiterst privacygevoelige gegevens binnen het sociaal domein (denk aan de jeugdzorg), vereist een professionele, integrale aanpak en sturing.
4. Het hebben van een vastgesteld, actueel Informatiebeveiligingsbeleid is een wettelijke (audit)verplichting, voortvloeiende vanuit onder andere de BIO en de wetgeving voor respectievelijk BRP, Digid en Suwi.

1.2. Wat is informatiebeveiliging?

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening **aantoonbaar** te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere informatie.

Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente en 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.

1.3. Ambitie en visie van de gemeente op het gebied van Informatiebeveiliging

Informatiebeveiliging moet eraan bijdragen dat de gemeenten en de BUCH haar ambities, doelen en resultaten realiseert, en dus niet de realisatie in de weg mag staan. Informatiebeveiliging is om die reden geen doel op zichzelf, en dient in samenhang gebracht te worden met de doelen van de organisatie. Die doelen zijn onder andere geformuleerd in het concernplan 2017- 2021 Werkorganisatie BUCH.

Visie

1. De data en informative die wij verwerken is in beginsel van en voor de burgers, bedrijven en bezoekers van de BUCH gemeenten
2. De data en informatie die wij verwerken is in beginsel openbaar

3. Wij delen de data en informatie waarover wij beschikken zoveel als mogelijk is, zowel intern als extern
4. Informatieverwerking en informatiebeveiliging maakt integraal onderdeel uit van onze beleidsvorming en -uitvoering, besluitvorming en/of ons handelen
5. Wij maken afwegingen op basis van dialoog en laten ons daarbij leiden door gezond verstand
6. Wet- en regelgeving evenals richtlijnen van bevoegde organen vormen het kader waarbinnen wij handelen.

Om de veiligheid, kwaliteit en de continuïteit van onze dienstverlening te waarborgenborgen worden op het gebied van informatiebeveiliging en privacy continu risicoanalyses uitgevoerd en worden aansluitend passende maatregelen getroffen.

Een solide inrichting van informatiebeveiliging aan de voorkant voorkomt extra tijdsinvestering en herstelkosten achteraf. Om deze solide inrichting te bereiken is het noodzakelijk om op het gebied van informatiebeveiliging te professionaliseren. Het huidige volwassenheidsniveau[1] van informatiebeveiliging van de Werkorganisatie en de BUCH gemeenten ligt tussen niveau 1 en 2. De ambitie is om in 2023 volwassenheidsniveau 4 te bereiken. Zodra dat niveau bereikt is, heeft de organisatie Informatiebeveiliging geborgd binnen haar processen. Zij voldoet aan wet- en regelgeving én heeft voldoende kennis om proactief op ontwikkelingen te anticiperen. Zij weet haar risico's te verkleinen tot een acceptabel niveau in lijn met de ambities uit de strategische agenda. Noodzakelijke randvoorwaarde om deze groei te bereiken, is de beschikbaarheid van kwalitatieve en kwantitatieve resources op de afdelingen.

Met de inrichting van een Informatiebeveiliging en privacy organisatie kan integraal worden gewerkt aan het verbeteren van de Informatiebeveiliging en privacy. Dit strategische informatiebeveiligingsbeleid 2020-2024 is het kader om gemeentelijke informatie te beschermen en draagt bij aan een verdere professionalisering van informatiebeveiliging.

2. Doel Strategisch informatiebeveiligingsbeleid.

Het strategisch beleid wordt gebruikt om de basis te leggen voor het tactische beleid en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau. Dit beleid geldt voor de jaren 2020 tot 2023 en vervangt het "Informatiebeveiligingsbeleid van 2017-2020". Het is aan het bestuurlijk kader om de beschikbaarheid, integriteit en vertrouwelijkheid van de (persoons)gegevens en andere informatie(systemen) te waarborgen, zodat de gemeente voldoet aan relevante wet- en regelgeving.
Dit strategische informatiebeveiligingsbeleid is gericht op het:

- Verstevigen van de governance;
  De verantwoordelijkheid voor informatieveiligheid is primair in de lijn belegd. Dit betekent een centrale rol voor afdelingsmanagers.
- Risico gebaseerd sturen;
  Dit betekent dat het management verantwoordelijk is voor het identificeren van de hoogste risico's, het prioriteren van de risico's en het treffen van maatregelen om deze risico's terug te brengen.

1) conform het volwassenheidsmodel NBA-LIO/NOREA)

- Integratie in de planning- en control cyclus;
  Dit betekent dat informatieveiligheid dient te worden opgenomen in de integrale P&C-cyclus. Implementatie en verantwoording vindt plaats via de planning zoals opgenomen in de bedrijfsvoering kalender. Er vindt een uniforme verantwoording plaats aan interne en externe toezichthouders. Dit beleid draagt bij aan een verdere professionalisering van informatieveiligheid en hiermee aan het behalen van de gestelde doelen in het concernplan 2017- 2021 Werkorganisatie

2.1. Scope van het strategische informatiebeveiligingsbeleid
Dit beleid is van toepassing op de gehele organisatie, alle gemeentelijke processen, informatie, informatiesystemen en gegevens(verzamelingen) van de gemeente en externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur. Het heeft betrekking op het politiek bestuur, alle medewerkers, inwoners, gasten, bezoekers en externe relaties. Het borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen.

2.2. Plaats van het strategisch beleid
Het strategisch beleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven 'Gemeentelijk Informatiebeveiligingsplan/managementreview'.
Voor bepaalde kerntaken gelden op grond van wet-en regelgeving specifieke (aanvullende) beveiligingseisen[2]. Hiervoor gelden specifieke beleidskaders en/of informatiebeveiligingsplannen.

2.3. Grondslagen
Dit strategische informatiebeveiligingsbeleid is gebaseerd op:
- NEN-ISO/IEC 27001:2017
- NEN-ISO/IEC 27002:2017
- Baseline Informatiebeveiliging Overheid (BIO)[3] en de 10 principes voor informatiebeveiliging.

2.3.1. Standaarden informatiebeveiliging
De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2017. De maatregelen worden op basis van "best-practices" bij (lokale) overheden en NEN-ISO/IEC 27002:2017 genomen.

2.3.2. De Baseline Informatiebeveiliging Overheid
De Baseline Informatiebeveiliging Overheid (BIO) is het nieuwe normenkader voor de gehele overheid. De werkwijze van deze BIO is meer gericht op risicomanagement dan de oude Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Dat wil zeggen dat de domein- en/of teammanagers nu moeten werken volgens de aanpak van de ISO 27001. Daarbij is risicomanagement van belang. Dit houdt voor het management in dat men **op voorhand** keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

2.4. Handvatten voor de rol van de bestuurder bij de BIO
VNG heeft aan het gemeentelijk bestuur de 10 principes van informatiebeveiliging (bronvermelding) uitgereikt. Deze principes bieden het bestuur handvatten op welke wijze het zijn rol kan invullen bij het borgen van informatiebeveiliging in de gemeentelijke organisatie Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement bij o.a. beveiligingsincidenten met directe gevolgen voor inwoners en/of medewerkers. De 10 principes voor informatiebeveiliging[4] zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder zichzelf oplegt. 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.

2) zoals BRP, PNIK, DigiD, SUWI, BAG, BGT, BRO, AVG, Privacy beleid
3) uitgebracht door de interbestuurlijke werkgroep Normatiek in 2018
4) https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/01/De-10-bestuurlijke-principes-voor-Informatiebeveiliging_20190109.pdf

9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

2.5. Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van dit informatiebeveiligingsbeleid zijn:

1. Dit beleid vormt samen met het tactische informatiebeveiligingsbeleid en het informatiebeveiligingsplan het kader om informatieveiligheid in de organisatie te borgen.
2. Informatiebeveiliging mag niet ten koste gaan van de veiligheid van personen.
3. Het bestuur van de BUCH en de Gemeenten, de Algemeen Directeur en de (afdelings)managers dragen dit beleid uit en sturen aan op de implementatie van dit beleid.
4. Informatiebeveiliging is georganiseerd. Het management heeft continu aandacht voor het vergroten van het bewustzijn van medewerkers om zo de menselijke schakel te versterken.
5. De rol van de coördinator van informatiebeveiliging (Chief Information Security Officer: CISO), is ingevuld.
6. Regels en verantwoordelijkheden voor het informatiebeveiligingsbeleid zijn vastgesteld.
7. Informatiebeveiliging is een continu verbeterproces. Door organisatiebrede planning, het implementeren van maatregelen, het periodieke controleren én de coördinatie op dit proces is informatieveiligheid binnen de organisatie verankerd.
8. Informatiebeveiliging is een onderdeel van risicomanagement.
9. De gemeente en/of werkorganisatie stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
10. 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.
11. Informatiebeveiliging is een continu verbeterproces. ‘Plan, do, check en act’ vormen samen het managementsysteem van informatiebeveiliging

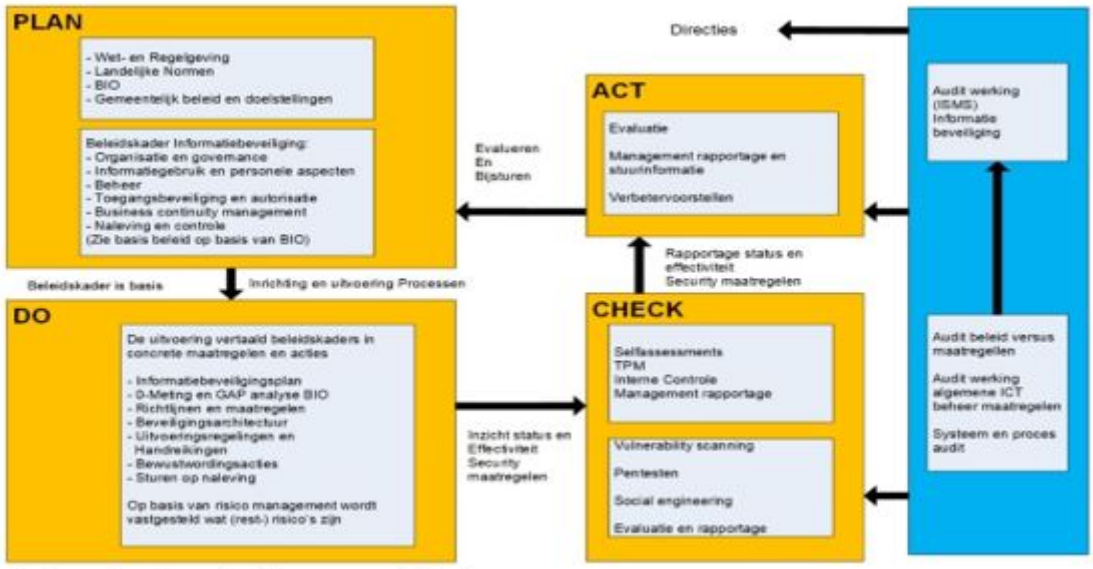
2.6. Praktisch invulling aan de uitgangspunten

- Het college van B&W en het BUCH bestuur stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
- De Algemeen Directeur stelt jaarlijks het informatiebeveiligingsplan/managementreview vast.
- De Algemeen Directeur is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- De Algemeen Directeur is verantwoordelijk voor het vragen om informatie bij de domeinmanagers en ziet erop toe dat de domeinmanagers adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.
- De Chief Information Security Officer (CISO) ondersteunt de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover gevraagd en ongevraagd. Indien de CISO van oordeel is dat zijn of haar adviezen onvoldoende worden opgevolgd, rapporteert hij of zij dat rechtstreeks aan de Algemeen Directeur. De keuze om van deze bevoegdheid gebruik te maken is exclusief voorbehouden aan de CISO.
- Er dient aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportage van de CISO in de beleidsvoorbereiding, besluitvorming en/of het handelen van de organisatie en in het kader van de P&C cyclus in het bijzonder. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen en – bij voldoende substantie – in de risicoparagraaf van de respectievelijke begrotingen voorzien van een risicoafweging, kwantificering en beheersmaatregelen.
- De domeinmanagers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- Hoewel de basiskernregistraties (zoals BRP, PUN, SUWI, BAG, BGT) en toekomstige basisregistraties belangrijk zijn in het kader van informatiebeveiliging, krijgen zij niet meer of minder voorrang dan andere (primaire) processen binnen de gemeente. 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.
- Alle medewerkers van de gemeente worden getraind/geïnformeerd in het gebruik van beveiligingsprocedures.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- Domeinmanagers dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben zoals omschreven in het privacy beleid
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Domeinmanagers voeren de baselinetoetsen (BLT) uit op basis van de BIO om deze risico-afwegingen te kunnen maken.

2.7 Randvoorwaarden

Belangrijke randvoorwaarden om dit beleid te implementeren zijn:

1. De informatiebeveiligingstaken zijn belegd binnen de bedrijfsprocessen en de benodigde kwalitatieve en kwantitatieve resources zijn beschikbaar gesteld.
2. Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures. Medewerkers kennen de beveiligingsprocedures en gebruiken deze procedures. Medewerkers zijn daarnaast op de hoogte van eisen die vanuit wet- en regelgeving aan hun bedrijfsprocessen gesteld worden en kennen deze kaders.
3. De informatiebeveiliging maakt deel uit van afspraken met ketenpartners en dienstenleveranciers.
4. Kennis en bewustzijn van informatiebeveiliging wordt actief bevorderd en geborgd bij alle lagen binnen de organisatie, ketenpartners en externe partijen.
5. Er zijn voldoende maatregelen geïmplementeerd die zorgen dat kwetsbaarheden in bedrijfsprocessen worden verkleind. Hierdoor worden informatiebeveiligingsincidenten verkleind en de effecten van de incidenten beperkt.
6. Periodiek worden onafhankelijke audits uitgevoerd om vast te stellen of de vereiste maatregelen uit het beleid in voldoende mate zijn geborgd.
7. De digitale weerbaarheid wordt verhoogd door de basis op orde te brengen.
8. Security en privacy by design principes worden toegepast bij innovaties. Denk hierbij aan common ground, internet of things (IoT) en Smart City, Omgevingswet.
9. Aanwezigheid van een werkend ISMS systeem waarin risicomanagement volgens PDCA wordt gehanteerd!

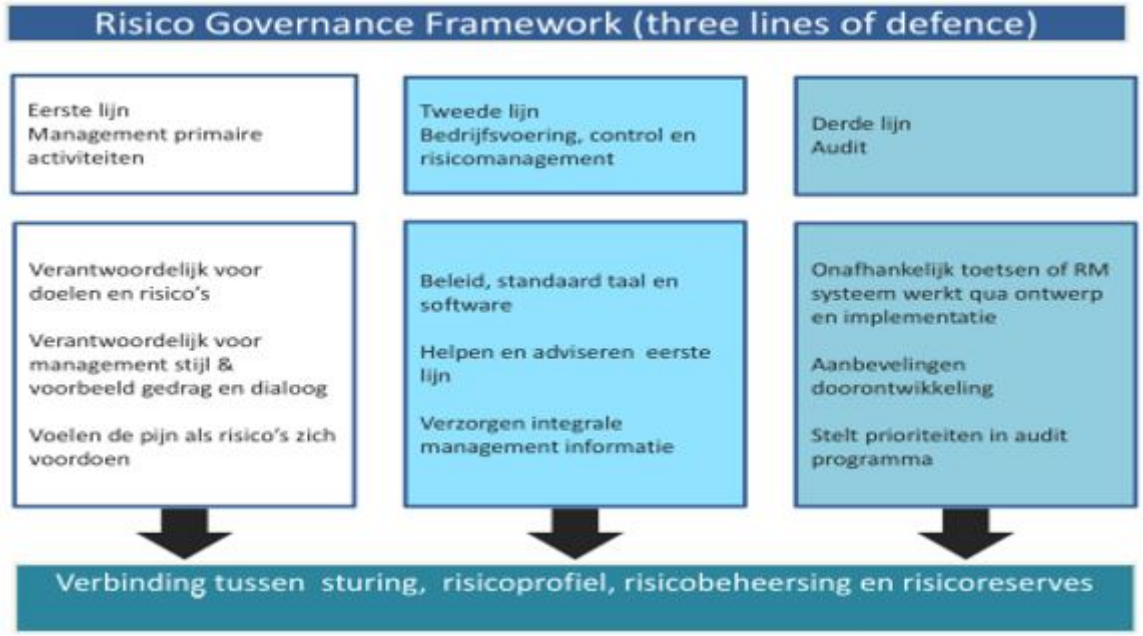


Information Security Management System

3. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD). In dit model is het lijnmanagement verantwoordelijk voor de eigen processen. De tweede lijn de CISO (ambassadeurs), ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

(De CISO is dé spin in het web als het gaat om de beveiliging van informatie van de gemeente. Hij is verantwoordelijk voor het implementeren van, en toezicht houden op het informatiebeveiligingsbeleid. De CISO heeft een centrale rol in het beheren van alle processen die daarmee te maken hebben en moet ervoor zorgen dat de gemeente voldoet aan de BIO; een set van organisatorische en technische beveiligingsmaatregelen die geïmplementeerd en beheerd dient te worden.): https://ib-p.nl/2020/05/ciso-privacy-officer-en-fg-doet-en-mag/



3.1. Aansturing: Algemeen Directeur
De Algemeen Directeur zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een domeinmanager. De Algemeen Directeur zorgt dat de domeinmanagers zich verantwoorden over de beveiliging van de informatie die onder hen berust. De Algemeen Directeur zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging een onderdeel is van het voorbereiden van beleid of besluiten danwel het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.

De Algemeen Directeur stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De Algemeen Directeur draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO van de Werkorganisatie BUCH. De domeinmanager autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de BUCH gezien als een integraal onderdeel van beleidsvoorbereiding en -uitvoering, besluitvorming, bedrijfsvoering en (risico)management.

3.2. Uitvoering: Domeinmanagers
Informatiebeveiliging valt onder de verantwoordelijkheden van alle domeinmanagers. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Domeinmanagers rapporteren aan de Algemeen Directeur over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de teams binnen de domeinen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging te bespreken in het teamoverleg.

Taken van de domeinmanagers in het kader van informatiebeveiliging zijn:
- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het binnen de eigen teams uitdragen van het beveiligingsbeleid, de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

Voorbereiding en coördinatie van het informatiebeveiligingsmoment in het teamoverleg overleg ligt bij de CISO.

3.3. Controle en verantwoording
Dit Strategisch Beleid is een verantwoordelijkheid van het bestuur van de BUCH en de colleges van de BUCH gemeenten. De bestuurders en directeuren van de BUCH 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.
De Algemeen Directeur is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan respectievelijke portefeuillehouders. De Algemeen Directeur rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

3.4 Aansluiting Informatiebeveiligingsdienst Gemeenten

Eén van de doelen van de IBD[5] is het aan gemeenten leveren van concrete ondersteuning in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging.
Wij maken indien nodig gebruik van deze ondersteuning. De IBD informeert de gemeente via vastgestelde contactpersonen namelijk de algemeen contactpersoon informatiebeveiliging (ACIB)[6] en de vertrouwde Contactpersoon Informatiebeveiliging (VCIB)[7]

3.5. ENSIA

Ter afsluiting van het jaarlijkse verantwoordingstraject[8] rapporteren de afdelingsmanagers over de risico's binnen hun bedrijfsprocessen en over de stand van zaken van de implementatie van informatiebeveiliging van het afgelopen jaar. De CISO coördineert dit proces en stelt jaarlijks vóór 1 mei aan de hand van de deelrapportages van de afdelingsmanagers een bestuurlijke rapportage op voor de ambtelijke en bestuurlijke opdrachtgever. De colleges van B&W legt met deze bestuurlijke rapportage, een raadsinformatiebrief én meteen aparte paragraaf in het jaarverslag verantwoording af aan zijn interne toezichthouders de gemeenteraden én aan de externe toezichthouders (Rijk). Op deze wijze kan de ambtelijk en de bestuurlijk opdrachtgever en het college sturen op informatiebeveiliging. Zij kunnen hiermee besluiten nemen om informatiebeveiligingsrisico's tot een acceptabel niveau te brengen

3.6. CISO mandaat

Indien het risico hierom vraagt, informeert en adviseert de CISO onverwijld de Algemeen Directeur in geval van overtreding of dreigende overtreding van wet- en regelgeving of richtlijnen van hogere organen. De Ciso is bevoegd handelend op te treden en in te grijpen. De CISO legt achteraf verantwoording af over het handelend optreden.

3.7. Inwerkingtreding

De beleidsregels Informatieveiligheid zoals vastgesteld op <19 september 2017 <gemeente Bergen (NH), Castricum, Heiloo en Werkorganisatie BUCH> <26 september 2017 gemeente Uitgeest>, wordt ingetrokken. Het Strategisch Informatiebeleid 2020-2023 treedt in werking met ingang van de dag na bekendmaking.

De beleidsregels worden aangehaald als: Strategisch Gemeentelijk Informatiebeveiligingsbeleid Werkorganisatie BUCH 2020 - 2023.

Aldus vastgesteld door het Bestuur van de Werkorganisatie BUCH op 9 september 2020,

De heer D.J. van Huizen
secretaris

De heer T.J. Romeyn
voorzitter

5) De Informatiebeveiligingsdienst voor gemeenten (IBD) is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING).
6) Algemene waarschuwingen en informatie met een niet vertrouwelijk karakter
7) Informatie die vertrouwelijk is van karakter
8) Verantwoording vindt plaats via de landelijk voorgeschreven systematiek ENSIA (Eenduidige Normatiek Single Information Audit)

Bijlage A De 10 principes voor informatiebeveiliging

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 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 en zonder beperkende factoren als beschermend midden management, heilige huisjes en aanverwante organisatie perikelen is het onmogelijk om risicomanagement goed van de grond te krijgen. Als u er in slaagt om "risico denken" en cultuur in alle haarvaten van uw organisatie te laten landen door het geven van voorbeeld gedrag, door het te eisen van uw managers en door helder verwachtingsmanagement, dan heeft u een organisatie die gezond kan reageren op de dagelijkse dreigingen en daarmee 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 zij ook hun rol kunnen 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 CISO, FG en Controller als onafhankelijke adviseur en laat ze samenwerken in het risk-team, 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 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 gaat alleen werken als het geïntegreerd is in alle werkprocessen van de organisatie. Dat kan alleen bereikt worden als het praten over risico's onderwerp is van iedere agenda en daarmee wordt een eerste aanzet gegeven om op een gestructureerde wijze om te gaan met risico's en pro-actief oplossingen te zoeken voor de risico's die aandacht behoeven. Maak lijnmanagers verantwoordelijk voor risicomanagement door afspraken met ze te maken hoe zij risicomanagement in hun dagelijkse praktijk vorm geven en op welke wijze zij daarover rapporteren. Maar bovenal: laat informatiebeveiliging een plek/paragraaf krijgen in alle bestuurlijke documenten.

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 Informatiebeveiliging 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 risicomana-

gement naadloos aansluiten op de strategische en beleidsmatige doelstellingen van de organisatie. Op deze wijze bied ik een duidelijk kader waarbinnen mijn medewerkers kunnen opereren.

Toelichting
Iedereen is ervan of zou ervan moeten zijn, u kunt als bestuurder alleen maar de juiste dingen doen als informatie u bereikt, maar vooral als het op de agenda staat. Door risicomanagement of vragen over dreigingen en risico's mee te nemen in de vragen die u stelt aan uw managers kunt u in uw beslissingen ook rekening houden met deze bedreigingen en risico's en ervoor zorgen dat ze behandeld worden voordat ze 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 bedrijfsdoelstellingen. De gemeente kan pro-actief communiceren en laten zien dat risicomanagement bijvoorbeeld in relatie tot privacy belangrijk is en dat ze er naar streven om zorgvuldig (naar goed huisvaderschap) met persoonsgegevens om te gaan. Bij het uitbesteden of delen van informatie moeten de juiste voorzieningen getroffen worden om ervoor te zorgen dat ook buiten de organisatie de juiste dingen worden gedaan.

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, klanten gaan meer zorgvuldigheid en of transparantie eisen, wetgeving verandert. Kortom, als risicomanagement geen rekening houdt met een veranderende omgeving en de eigen organisatie, dan doet uw organisatie misschien de verkeerde dingen of teveel of misschien wel te weinig.

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

Toelichting
Risico's ontwijken, mitigeren, verzekeren of wegnemen door het nemen van preventieve-, detectieve-, repressieve- en/of correctieve maatregelen. Welke strategie u ook kiest, ze kosten allemaal resources in termen van tijd, geld en mens capaciteit. Als u niet investeert in informatiebeveiliging dan keert het spook zich op termijn waarschijnlijk tegen uw organisatie en worden alle doelstellingen, hoe goed bedoelt ook, vertaalt in luchtkastelen.

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 een gezonde risicomanagement cultuur.

Toelichting
Zonder goede informatie geen goede risico-inschattingen en besluiten. Zonder goede en tijdige informatie lopen uw organisatie en uw primaire processen een mogelijk risico met mogelijk zelfs een verstoring waar uw klanten last van krijgen. Zonder goede en tijdige informatie neemt u de verkeerde beslissingen en doet uw organisatie de verkeerde dingen.

9. Verbetering komt voort uit leren en ervaring
Risicobeheer wordt voortdurend verbeterd door leren en ervaring.

Door mijn inzet zorg ik ervoor dat risicogestuurd 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 is ook de wil om te leren en de wil om te verbeteren. Als die wil er niet is dan heeft u een ad-hoc organisatie die alleen maar kan reageren op incidenten waarbij de energie ontbreekt om te leren en te verbeteren. Incidenten kunnen voorkomen worden door te leren en te verbeteren, het voordeel voor u is geen verassingen, geen raadsvragen en geen pers die u kritische vragen stelt. Als de organisatie verbeterd kunt u ieder risico aan en kunt u aantonen dat uw organisatie (en u) de juiste dingen hebben gedaan.

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 controleer actief binnen mijn organisatie doordat ik opdracht geef om de werking van risicomanagement binnen mijn organisatie op effectiviteit en efficiency te (laten) controleren. Naast management rapportages zijn (externe) controles de manier om te weten te komen of en hoe mijn uitgedragen beleid in de praktijk werkt. 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 signalen te krijgen over de wijze waarop de organisatie omgaat met het onderwerp. Medewerkers kunnen er op vertrouwen dat besluiten op bestuurdersniveau genomen worden, wanneer de situatie daar om vraagt.

Bijlage B Baseline Informatiebeveiliging Overheid (BIO)

Informatiebeveiliging bij de overheid

Inleiding
Informatiebeveiliging is het proces van vaststellen van de vereiste beveiliging van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.

De BIO beoogt de beveiliging van informatie(systemen) bij alle bedrijfsonderdelen van de overheid te bevorderen, zodat deze bedrijfsonderdelen erop kunnen vertrouwen dat gegevens die worden verstuurd naar of worden ontvangen van andere onderdelen van de overheid, in lijn met wet- en regelgeving, passend beveiligd zijn.

De BIO beoogt zo de beveiliging van informatie(systemen) bij alle bestuurslagen en bestuursorganen van de overheid te bevorderen, zodat alle onderdelen erop kunnen vertrouwen dat onderling uitgewisselde gegevens, in lijn met wet- en regelgeving, passend beveiligd zijn. Het doel is continuïteit in de bedrijfsprocessen door waarborgen van juiste en tijdige informatie. Daarmee is de BIO ook van toepassing op besturings- en meetprocessen voor zover deze binnen een bestuursorgaan gebruikt worden.

De BIO is van toepassing op de overheid. In verband hiermee is de BIO van toepassing op de volgende bestuursorganen:
- Rijksdienst
- Provincies
- Waterschappen
- Gemeentes

Daarnaast wordt aanbevolen de BIO te verankeren in de taakomschrijving van de overige overheidsorganisaties en organisaties waarmee de overheid publiek privaat samenwerkt en private samenwerkingen waarbij de overheid de enige aandeelhouder is.

Informatiebeveiligingskaders en uitgangspunten overheid
De overheid past risicomanagement toe om tot de juiste beveiliging van informatie en informatiesystemen te komen binnen de context van de bedrijfsdoelstellingen. Risicomanagement is het inzichtelijk en systematisch inventariseren, beoordelen en – door het treffen van maatregelen – beheersbaar maken van risico's en kansen, die het bereiken van de doelstellingen van de organisatie bedreigen dan wel bevorderen, op een zodanige wijze dat verantwoording kan worden afgelegd over de gemaakte keuzes.

De insteek van risicomanagement in het kader van de BIO is dat er cyclisch en methodisch vanuit een PDCA-cyclus wordt omgegaan met informatiebeveiliging. De overheidslagen kiezen als basis voor deze procesmatige inrichting van risicomanagement en het inrichten van de PDCA-cyclus voor de NEN/ISO 27001:2017. Voor de rijksoverheid vindt nadere specificatie plaats in de algemene voorschriften voor de beveiliging van informatiesystemen: het Beveiligingsvoorschrift Rijksdienst (BVR), het Voorschrift Informatiebeveiliging Rijksdienst (VIR) en het Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIR-BI).

Voor de BIO geldt (op basis van deze documenten van NEN/ISO 27001 en BVR, VIR en VIR-BI) kort samengevat het volgende.
- Een ruime definitie voor een informatiesysteem, namelijk "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;
- Het lijnmanagement is verantwoordelijk voor de beveiliging van informatie(systemen);
- Informatiebeveiliging is een cyclisch proces is, volgens de Plan-Do-Check-Act cyclus;
- Deze Plan-Do-Check-Act cyclus maakt het lijnmanagement verantwoordelijk voor het treffen van maatregelen op basis van risicomanagement;
- De Secretaris/algemeen directeur van een organisatie is eindverantwoordelijk voor deze beveiliging en voor de inrichting en werking van de beveiligingsorganisatie;
- Het lijnmanagement stelt op basis van een expliciete risicoafweging de betrouwbaarheidseisen voor zijn informatiesystemen vast;
- Op basis van de betrouwbaarheidseisen kiest, implementeert en draagt het lijnmanagement de maatregelen uit.

De BIO is allereerst een gemeenschappelijk normenkader voor de beveiliging van de informatie(systemen) van de overheid. Daarnaast concretiseert de BIO een aantal normen tot verplichte overheidsmaatregelen:
- op grond van wet- en regelgeving;

- vanwege de gemeenschappelijk veiligheid van informatieketens;
- omdat deze fundamenteel zijn voor een betrouwbare c.q. professionele informatievoorziening.

De Baseline Informatiebeveiliging Overheid BIO is gebaseerd op de ISO 27002 standaard.

ISO 27002
De ISO 27002 'Code voor informatiebeveiliging' geeft richtlijnen en principes voor het initiëren, het implementeren, het onderhouden en het verbeteren van informatiebeveiliging binnen een organisatie. Deze standaard is een "best practice" om informatiebeveiligingsrisico's aan te pakken met betrekking tot vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening. De standaard kan gezien worden als een nadere specificatie van de ISO 27001 standaard. De ISO 27002 kan dienen als een praktische richtlijn voor het ontwerpen van veiligheidsstandaarden binnen een organisatie en als effectieve methode voor het bereiken van deze veiligheid.

De ISO bestaat uit 114 controls; de term 'control' wordt in de ISO vertaald als een beheersmaatregel. De BIO volgt de opbouw van de ISO 27002 en haar controls. De controls zijn in de BIO letterlijk overgenomen. Dit vergemakkelijkt afstemming met externe partners of leveranciers. Daarnaast vult de BIO enkele bepalingen uit het VIR inzake PDCA-cyclus en verantwoordelijkheden op een generieke wijze in.

Evaluatie en bijstelling
Door de snelle ontwikkelingen van de techniek verouderen maatregelensets voor informatiebeveiliging snel. De BIO is daarom zoveel als mogelijk op een abstractieniveau geschreven waarbij dergelijke wijzigingen en ontwikkelingen een zo klein mogelijke impact hebben op de maatregelen. De BIO beschrijft het wat en niet het hoe. Desondanks kunnen wijzigingen noodzakelijk zijn bij bijvoorbeeld aanpassingen van onderliggende wet- en regelgeving, nieuwe of juist verouderde handreikingen of nieuwe dreigingen en kwetsbaarheden.
Dit document wordt daarom regelmatig in zijn geheel geëvalueerd en indien nodig bijgesteld. Daarnaast wordt specifiek bezien of er wijzigingen en aanvullingen in de maatregelen en de (operationele) handreikingen nodig of gewenst zijn om hiermee de praktische toepasbaarheid te vergroten. Besluiten hierover worden via de bestaande informatiebeveiligingsgremia genomen en door de beheerder van de BIO verwerkt.

Forum Standaardisatie
De overheid volgt de standaarden die op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie (hierna Forum) staan. De BIO is gebaseerd op de NEN-ISO/IEC 27002:2017 en vanuit de BIO wordt verwezen naar de NEN-ISO/IEC 27001:2017, beide standaarden staan op de 'pas toe of leg uit'-lijst van het Forum. Ook een aantal technische maatregelen uit de BIO staan op de 'pas toe of leg uit'-lijst of op de 'open standaarden'-lijst van het Forum. Deze technische invullingen zijn niet allemaal uitgewerkt in deze BIO. Er is voor gekozen alleen aan te geven of de maatregel ingevuld wordt door een verplichte of open standaard van het Forum. Hierdoor wordt de BIO minder onderhoudsgevoelig.

Zie verder
https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/