1 Inleiding

Dit beleidsdocument beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2023 t/m 2025 en vervangt het in 2020 vastgestelde 'Strategisch informatiebeveiligingsbeleid 2020-2022'.
Dit beleid is richtinggevend en kader stellend en wordt aangevuld met onderwerp specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.

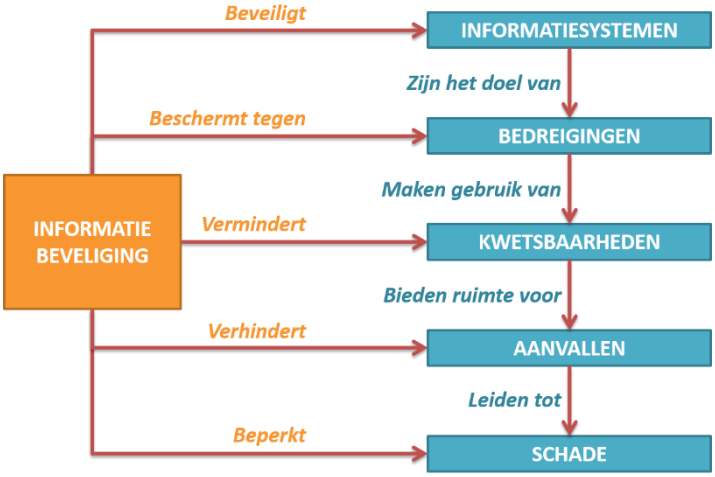
Met dit 'Strategisch Informatiebeveiligingsbeleid 2023-2025' zet het Inlichtingenbureau een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen het Inlichtingenbureau te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit strategisch beleid is de NEN-ISO/IEC 27001:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO).

1.1 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.

1.2 Ambitie en visie van het Inlichtingenbureau op het gebied van informatieveiligheid

Informatiebeveiliging heeft tot doel het beveiligen van informatiesystemen en de schade door mogelijke aanvallen zo veel mogelijk te beperken en ultiem te voorkomen. Dit wordt gerealiseerd door de kwetsbaarheden in en om informatiesystemen in kaart te brengen en te verminderen waardoor deze systemen zo goed mogelijk zijn beschermd tegen bedreigingen. Hierdoor verminderd de kans op geslaagde aanvallen en kan de mogelijke schade beperkt (en hopelijk voorkomen) worden.



Het Inlichtingenbureau doet haar risico analyse op basis van de volgende categorieën: **M**ens, **A**pparatuur, **P**rogrammatuur, **G**egevens, **O**rganisatie, **O**mgeving en **D**iensten. Dit zijn de zogenaamde MAPGOOD[1] categorieën uit de gelijknamige risicoanalyse methode[2]. Niet alleen dreigingen, maar ook risico's, kwetsbaarheden en aanvallen zijn 1 op 1 aan deze categorieën te koppelen. Alle controls en maatregelen in het BIO normenkader zijn er op gericht om risico's volgend uit de MAPGOOD categorieën te mitigeren en tot een acceptabel niveau terug te brengen. Indien nodig treft het Inlichtingenbureau aanvullende maatregelen om het acceptabel niveau te bereiken.

Jaarlijks zal de Directeur een risicoanalyse laten uitvoeren om een actueel inzicht te verkrijgen in de risico's voor het Inlichtingenbureau. Tevens zal op basis van de risico's jaarlijks een GAP-analyse plaatsvinden op de implementatie van de BIO. Door de implementatie en conformering aan de BIO wil het Inlichtingenbureau een kader scheppen met voldoende maatregelen om haar informatie afdoende te beveiligen. Het Inlichtingenbureau gaat hierbij uit van een basisbeveiligingsniveau conform BBN2 van de BIO.

Het Inlichtingenbureau scherpt jaarlijks, in samenspraak met de EDP-auditor, de informatiebeveiliging verder aan. Zie hiervoor paragraaf 2.4.

[1] MAPGOOD is een algemeen geaccepteerde risico analyse methode die ook door IBD gemeenten gebruikt en aanbevolen wordt.
[2] MAPGOOD wordt vaak ook "dreigingen analyse" genoemd, voor de eenduidigheid wordt in dit document de overal de term "risicoanalyse" gebruikt.

2 Strategisch beleid

2.1 Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligingsbeleid zijn de volgende:

2.1.1 De ISO27001

Het Inlichtingenbureau heeft haar Information Security Management System (ISMS) gebaseerd op de ISO27001. Het Inlichtingenbureau geeft invulling aan hoofdstuk 5 t/m 10 van deze norm, waaronder de directiebeoordeling en interne audit.

2.1.2 De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is het normenkader voor de gehele overheid. De werkwijze van deze BIO is gebaseerd op risicomanagement en een managementsysteem volgens de aanpak van de ISO 27001. 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 is in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

2.1.3 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

2.1.4 Informatie uit incidenten en inbreuken op de beveiliging

Het Inlichtingenbureau kent naast het hierboven genoemde dreigingsbeeld natuurlijk ook een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

2.1.5 EDP-audit

Het Inlichtingenbureau verantwoordt zich over informatiebeveiliging middels een EDP-audit. Het doel van de EDP-audit is als volgt: Het laten toetsen op opzet, bestaan en werking door een onafhankelijke auditor dat het Inlichtingenbureau beschikt over een afdoende informatiebeveiligingsmanagementsysteem (ISMS) ten aanzien van de informatieproducten die het Inlichtingenbureau voert in opdracht van haar opdrachtgevers en ten behoeve van haar afnemers. Deze toetsing vindt plaats op implementatie van de BIO gebaseerd op het volgende uitgangspunt:

- Jaarlijks selecteert het Inlichtingenbureau de set aan controls en maatregelen gebaseerd op door het Inlichtingenbureau noodzakelijk geachte onderwerpen of actuele thema's. Deze set wordt jaarlijks vastgesteld en geëvalueerd.

De resultaten van de jaarlijkse EDP-audit worden per wettelijk stelsel gepresenteerd aan de verschillende opdrachtgevers c.q. stelselverantwoordelijken. Over de werking van de informatiebeveiliging wordt, conform het bepaalde in artikel 5.22 Regeling SUWI, jaarlijks aan de minister van SZW gerapporteerd op basis van een NOREA EDP-audit voor wat betreft de informatiediensten die zijn opgenomen in het IB-Gegevensregister SUWI/Participatiewet. De VNG ontvangt een EDP-auditrapport over de informatiediensten die zijn opgenomen in het IB-Gegevensregister Jeugdwet en Wmo.

De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking in de verklaring Informatiebeveiliging. Met deze verklaring geeft de Directeur aan in hoeverre het Inlichtingenbureau voldoet aan de afspraken die gemaakt zijn voor de EDP-audit Informatiebeveiliging. Ook worden de eventuele verbetermaatregelen vermeld die het Inlichtingenbureau gaat treffen.

Middels deze verantwoording wordt het bestuur van het Inlichtingenbureau geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat het Inlichtingenbureau informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie adequaat te beschermen.

2.2 Scope informatiebeveiliging

De scope van dit beleid omvat alle Inlichtingenbureau processen, onderliggende informatiesystemen, informatie en gegevens van het Inlichtingenbureau, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur. Dit strategisch Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving (bijvoorbeeld SUWI) af. Bewust wordt in het strategisch beleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

2.3 Uitgangspunten

De Directeur speelt een cruciale rol bij het uitvoeren van dit strategisch informatiebeveiligingsbeleid. De Directeur maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor het Inlichtingenbureau heeft, de risico's die het Inlichtingenbureau hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het management dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

De Directeur geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor het gehele Inlichtingenbureau. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van het Inlichtingenbureau en de relevante landelijke en Europese wet- en regelgeving.

2.3.1 Strategische doelen

De strategische doelen van het informatiebeveiligingsbeleid zijn:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Het waarborgen van de naleving van dit beleid.

2.3.2 Uitgangspunten

De uitgangspunten van het beleid zijn:

- Alle informatie en informatiesystemen zijn van belang voor het Inlichtingenbureau, bepaalde informatie is van vitaal en kritiek belang. De Directeur is eindverantwoordelijke voor de informatiebeveiliging.
- Alle vitale informatiebronnen en informatiesystemen die gebruikt worden door het Inlichtingenbureau hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de vitale informatie.
- Door periodieke controle, organisatiebrede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
- Informatiebeveiliging is een continu verbeterproces. ‘Plan, do, check en act’ vormen samen het managementsysteem van informatiebeveiliging.
- Het Inlichtingenbureau stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
- 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.
- Informatiebeveiliging is onderdeel van het ontwerpen, ontwikkelen en beheren van software, ook als die door derden wordt ontwikkeld. Voor Secure Software Development (SSD) worden gebruik de:
  - SSD Beveiligingseisen voor (web)applicaties van het Centrum Informatiebeveiliging en Privacy (CIP);
  - OWASP top 10 (ASVS);
  - NCSC richtlijnen

  Deze zullen omgezet worden in een Security Impact Assessment document (SIA), welke verplicht is in te vullen voor wijzigingen met impact op Security.
- Productie omgevingen zijn gescheiden van andere omgevingen en hierin kunnen specifiek toegangsrechten worden verleend en is monitoring van de toegang mogelijk.
- Het beheer en de opslag van gegevens in productie omgevingen zijn zodanig, dat geen informatie verloren kan gaan tenzij er sprake is van overmacht.
- Er zijn functiescheidingen aangebracht tussen de ontwikkel-, beheer- en gebruikersorganisatie. Voorts wordt functiescheiding toegepast waar dat mogelijk en wenselijk is.
- Het Inlichtingenbureau en haar medewerkers realiseren zich de privacy gevoeligheid van de (bijzondere) persoonsgegevens die zij verwerken en waarborgen te allen tijde de afscherming, corrigeerbaarheid en transparantie van deze gegevens ter bescherming van de persoonlijke levenssfeer van de betrokkenen.
- De informatiebeveiliging maakt deel uit van afspraken met (keten)partners.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- De (gemandateerde) procesverantwoordelijken zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.

- Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van het Inlichtingenbureau en het behalen van de doelen die gesteld zijn.
- Alle medewerkers van het Inlichtingenbureau worden getraind in het gebruik van beveiligingsprocedures.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.

2.4 Controle en verantwoording

Dit Strategisch Beleid is een verantwoordelijkheid de Directeur van het Inlichtingenbureau. De Directeur van het Inlichtingenbureau zal richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie. De Directeur is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan het bestuur. De 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.

De Directeur zal minimaal 2 x per jaar een directiebeoordeling van het ISMS organiseren (conform hoofdstuk 9 van de ISO 27001).