Strategisch Informatiebeveiligingsbeleid GBLT 2022-2025

Strategisch Informatiebeveiligingsbeleid GBLT
Versie 1.02
Status: Definitief
Datum: September 2022
Auteur: Arjan de Wit en Gertjan Post

Versiebeheer

Versie	Datum	Door	Wijzigingen
0.9	25-04-2022	G. Post A.S. de Wit	Verwerken opmerkingen CISO
0.95	24-05-2022	G. Post A.S. de Wit	Verwerken opmerkingen en feedback ABC&P
1.0	30-5-2022	J. Blankvoort	Definitief gemaakt
1.01	08-09-2022	A.S. de Wit G. Post	Wijzigingen n.a.v. 1e MT voorstel
1.02	14-09-2022	J. Blankvoort	Wijzigingen n.a.v. 2e MT voorstel

Inhoudsopgave

1 Begrippenlijst

Afkorting	Toelichting
ACIB	Algemeen contactpersoon informatiebeveiliging
BIO	Baseline Informatiebeveiliging Overheid
BRP	Basisregistratie Personen
CSBN	Cybersecuritybeeld Nederland
CISO	Chief Information Security Officer
ENSIA	Europees Agentschap voor netwerk- en informatiebeveiliging
FG	Functionaris voor de Gegevensbescherming
IBD	Informatiebeveiligingsdienst
ICT	Informatie- en communicatietechnologie
IEC	International Electrotechnical Commission
ISMS	Informatie Security Management System
ISO	Internationale Organisatie voor Standaardisatie
MT	Management Team
NEN	NEderlandse Norm
NCSC	National Cyber Security Center
P&C	Planning & Control
SO	Security Officer
VCIB	Vertrouwde contactpersoon informatiebeveiliging
VNG	Vereniging van Nederlandse Gemeenten
VVT	Verklaring Van Toepasselijkheid

2 Bestuurssamenvatting

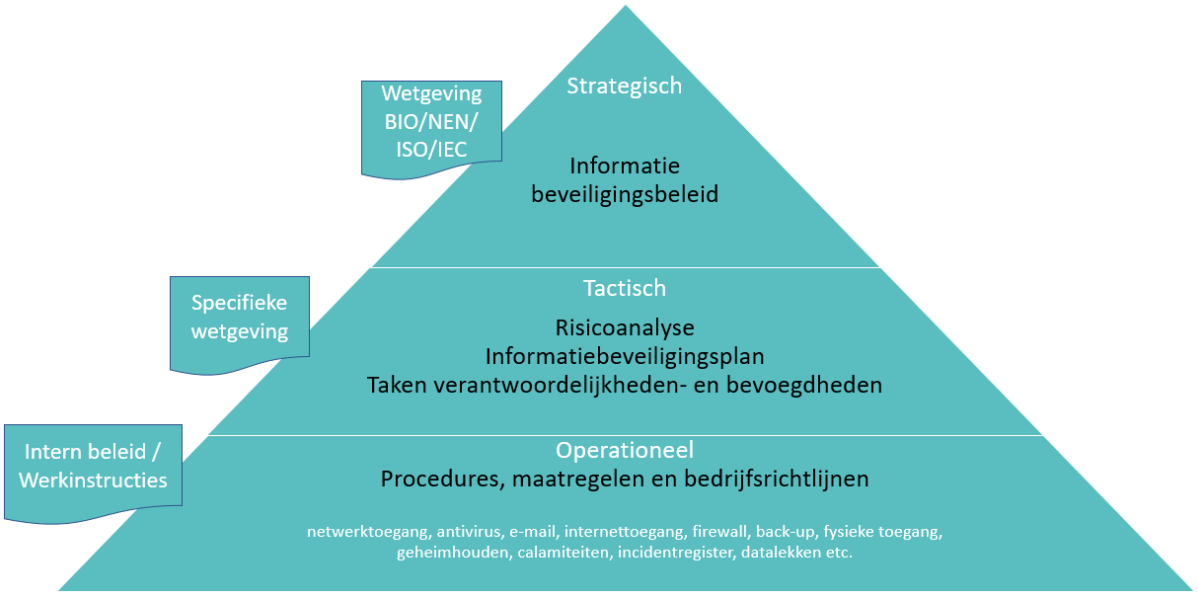
Voor u ligt het strategisch informatiebeveiligingsbeleid van GBLT voor de jaren 2022-2025. Dit strategisch informatiebeveiligingsbeleid wordt gebruikt als basis voor de verdere invulling van het tactische informatiebeveiligingsplan en daarmee geeft het richting aan de verdere invulling van het informatiebeveiligingsbeleid op operationeel niveau.

Beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening zijn van groot belang. Hoe we deze aspecten bij GBLT borgen wordt vastgesteld in dit strategisch informatiebeveiligingsbeleid.

GBLT houdt zich aan de wet. Informatie over klanten, deelnemers en medewerkers wordt zo zorgvuldig als mogelijk behandeld. Aandacht hiervoor hoort bij de proactieve houding van iedere medewerker, tegelijkertijd worden er niet meer maatregelen genomen dan noodzakelijk om het ondernemende en creatieve karakter van GBLT niet te frustreren.

Informatiebeveiliging is ieders verantwoordelijkheid en een lijnverantwoordelijkheid. Proceseigenaren dragen de primaire verantwoordelijkheid voor een goede informatiebeveiliging binnen hun proces. Alle informatiesystemen worden geclassificeerd op de aspecten beschikbaarheid, integriteit en vertrouwelijkheid; deze classificatie bepaalt het niveau van de beveiligingsmaatregelen.

De verantwoordelijkheid van de betrokken functionarissen wordt beschreven in hoofdstuk 5. In het bijzonder de verantwoordelijkheid van de Chief Information Security Officer (CISO), Security Officer (SO), adviseur risicomanagement, interne auditor, recordmanager, Functionaris Gegevensbescherming (FG) en de Privacy Officer (PO). Bovenstaande rollen vormen binnen GBLT het ABC&P. Wat staat voor Adviesgroep Beveiliging, Continuïteit & Privacy. Dit is een adviesgroep die maandelijks bijeenkomt in het kader van informatiebeveiliging/security en privacyvraagstukken.



3 Inleiding

Dit document beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2022 tot 2025 van GBLT. Dit beleid is richtinggevend en kaderstellend en wordt aangevuld met onderwerp specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.

Met dit 'Strategische informatiebeveiligingsbeleid 2022-2025' zet GBLT een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen GBLT 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 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO). Toepassen van de BIO is sinds 1 januari 2019 verplicht voor GBLT (Staatscourant 2019, 26526, 2018). Vóór deze periode conformeerde GBLT zich aan het normenkader van de BIG (Baseline Informatiebeveiliging Gemeenten).

3.1 Leeswijzer

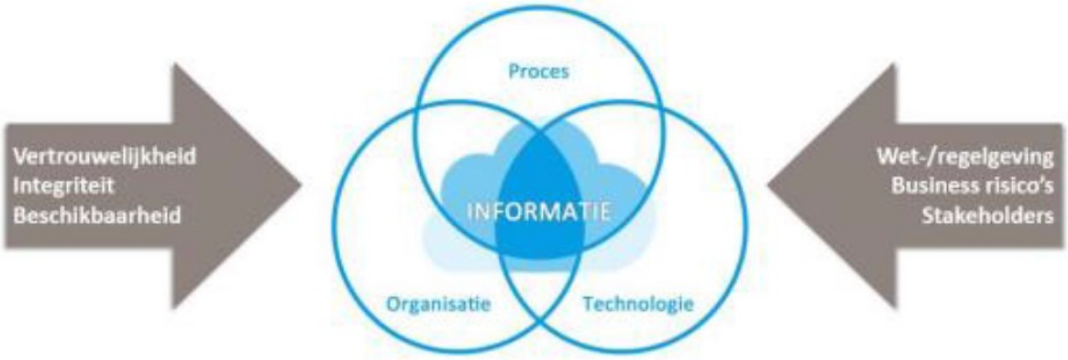
In hoofdstuk 4 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het Informatiebeveiligingsplan (vastgesteld door het MT) worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de proceseigenaren, de CISO en het dreigingsbeeld van de IBD. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Hoofdstuk 5 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

3.2 Wat is informatiebeveiliging?

Onder informatiebeveiliging wordt verstaan: het treffen en onderhouden van een samenhangend pakket van maatregelen om de continuïteit en de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere informatie.
Het strategisch informatiebeveiligingsbeleid geldt voor alle processen van GBLT 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 bestuur, alle GBLT medewerkers, klanten, gasten, bezoekers en externe relaties.

We kunnen informatiebeveiliging definiëren als:
"*Het geheel van preventieve, detective, repressieve en correctieve maatregelen, procedures en processen. Deze moeten de juistheid, volledigheid, vertrouwelijkheid en continuïteit van alle vormen van informatie binnen GBLT en naar haar opdrachtgevers en klanten toe garanderen*".
(Wikipedia Informatiebeveiliging, 2022)

Doel ervan is de continuïteit van de informatie en de informatievoorziening te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau te beperken.



Aspecten van informatiebeveiliging

3.3 Het belang van informatiebeveiliging en continuïteit

Informatie is één van de voornaamste bedrijfsmiddelen van GBLT. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de bedrijfsvoering van GBLT. Ernstige incidenten hebben mogelijk negatieve gevolgen voor klanten, deelnemers en de eigen organisatie met mogelijk ook politieke consequenties. Informatieveiligheid is daarom van groot belang. Informatiebeveiliging is het proces dat dit belang dient.

Continuïteit is de voortgang en de permanente beschikbaarheid van informatie en ongestoorde voortgang van de informatieverwerking en alle bedrijfsprocessen van GBLT die nodig zijn voor de dienstverlening en de uitvoering van haar taken.

Het strategisch informatiebeveiligingsbeleid is een verzameling van strategische uitgangspunten waarin het bestuur van GBLT eensgezind duidelijk maakt aan de organisatie welke gedragslijn GBLT dient te volgen om te komen tot een adequate informatiebeveiliging. Het strategisch informatiebeveiligingsbeleid vormt daarmee de basis voor de verderop uitgewerkte normen en maatregelen.

Het maken en vaststellen van het strategisch informatiebeveiligingsbeleid is nog geen garantie voor de goede werking. Hiervoor is het nodig dat de uitgangspunten in een strategisch informatiebeveiligingsbeleid concreet worden geformuleerd. Door middel van controles op de uitvoering dient het management vast te stellen of de maatregelen werken. Evaluatie van het beleid dient vervolgens plaats te vinden om na te gaan of het beleid nog steeds aansluit op de organisatie en of de juiste maatregelen zijn getroffen. Informatiebeveiliging is een continu proces gebaseerd op de Plan Do Check Act (PDCA) cyclus.

3.4 Ambitie en visie van GBLT op het gebied van informatiebeveiliging en continuïteit

De komende jaren zet GBLT in op het verhogen van informatieveiligheid en continuïteit en verdere professionalisering van de informatiebeveiligingsfunctie in de organisatie. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van het belastingkantoor en de basis voor het beschermen van rechten van klanten. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

4 Strategisch beleid

4.1 Doel

Het doel van dit document is het presenteren van het 'Strategisch informatiebeveiligingsbeleid voor de jaren 2022 tot 2025'. De uitwerking van dit beleid in concrete maatregelen staat beschreven in het tactische informatiebeveiligingsplan en wordt bijgehouden in het Information Security Management System (ISMS).

4.1.1 Doelstelling

Het continu beschermen van bedrijfsinformatie tegen een variëteit aan bedreigingen, op een effectieve en efficiënte wijze, om bedrijfsdoelstellingen te borgen en bedrijfsrisico's te minimaliseren, investeringen te optimaliseren en kansen te maximaliseren.

4.1.2 Doelgroepen

Doelgroep	Rol informatieveiligheid
Algemeen bestuur	Controlerende taak
Dagelijks bestuur	Integrale verantwoordelijkheid
Directeur	Bestuurlijk verantwoordelijk
Directie	Kaderstelling en implementatie
Chief Information Security Officer	Dagelijkse coördinatie
Security Officer	Dagelijkse uitvoering
Proceseigenaren	Sturing en controle op de naleving
Medewerkers	Gedrag en naleving
Gegevenseigenaren/bronhouders (BRP/BAG etc.)	Classificatie: beschermingseisen
Functionaris voor de Gegevensbescherming	Toetsen en toezicht houden op AVG-compliance
Informatiearchitect	Informatiesystemen toetsen / ontwerpen
HRM	Arbeidsvoorwaardelijke zaken
Facilitaire zaken	Fysieke toegangsbeveiliging
ICT-diensten	Technische beveiliging
Interne Auditor	Onafhankelijke toetsing
Leveranciers en ketenpartners	Compliance

4.2 Ontwikkelingen

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

- De Baseline Informatieveiligheid Overheid;
- De 10 principes voor informatiebeveiliging;
- Het dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten;
- De informatie uit incidenten en inbreuken op de beveiliging;
- De actuele bedreigingen.

4.2.1 De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is sinds 2019 het verplichte normenkader voor de gehele overheid. De werkwijze van deze BIO is meer gericht op risicomanagement dan het voormalige normenkader de Baseline Informatiebeveiliging Gemeenten (BIG). Dat wil zeggen dat de proceseigenaren nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Voor het management betekent dit dat men op voorhand continu keuzes en afwegingen maakt. Deze keuzes en afwegingen hebben betrekking op de vraag of informatie in bestaande en nieuwe processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

4.2.2 De 10 principes voor informatiebeveiliging

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO[1] en gaan over de waarden die het bestuur, directie en management zichzelf oplegt. De principes zijn als volgt: (Informatiebeveiligingsdienst, 2019)

1. Bestuurders, directie en management 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, directie en management controleert en evalueert.

De principes gaan vooral over de rol van het bestuur, directie en management bij het borgen van informatiebeveiliging. Deze principes ondersteunen bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen GBLT, dan kan dit directe gevolgen hebben voor klanten, deelnemers en medewerkers van GBLT.

4.2.3 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.

4.2.4 Informatie uit incidenten en inbreuken op de beveiliging

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

---

[1] Deze principes worden gelijk met de BIO van kracht, zie besluitvorming Informatiebeveiligingsdienst (IBD) en Vereniging van Nederlandse Gemeenten (VNG)

4.2.5 De actuele bedreigingen

Er zijn verschillende overheidsinstellingen die (jaarlijks) overzichten publiceren van de actuele bedreigingen. Dit zijn o.a.:

- National Cyber Security Center (NCSC), dreigingsmatrix (CSBN-x);
- IBD-gemeenten, maandmonitor en als algemeen contactpersoon informatiebeveiliging (ACIB) (IBD, 2022) en als vertrouwde contactpersoon informatiebeveiliging (VCIB) ontvangen we wekelijks een mailingslijst van acute bedreigingen specifiek voor de GBLT ICT omgeving.
- Europees Agentschap voor netwerk- en informatiebeveiliging (ENSIA).

4.3 Standaarden informatiebeveiliging

De basis voor de inrichting van het informatiebeveiligingsbeleid is NEN-ISO/IEC 27001. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002 genomen.
Voor de ondersteuning van gemeenten en belastingsamenwerkingen bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[2] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen. Ook zullen praktische operationele handreikingen worden uitgebracht, zoals een handleiding voor het uitvoeren van een risicoanalyse voor het opstellen van een beveiligingsplan. De inhoud en structuur van dit beleid zijn afgestemd op die van de ISO en de BIO. Ook het Informatiebeveiligingsplan zal deze structuur volgen.

4.4 Plaats van het strategisch beleid

Het strategisch informatiebeveiligingsbeleid wordt gebruikt om de basis te leggen voor het tactische informatiebeveiligingsplan en geeft daarmee richting voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau.
De daaruit voortkomende werkzaamheden worden uitgewerkt en continu bijgehouden in het ISMS en jaarlijks behandeld door een GAP- en Impactanalyse.

4.5 Scope informatiebeveiliging

De scope van dit strategische informatiebeveiligingsbeleid omvat alle GBLT processen, onderliggende informatiesystemen, informatie en gegevens van GBLT 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.

4.6 Uitgangspunten strategisch informatiebeveiligingsbeleid

Het bestuur en MT van GBLT spelen een cruciale rol bij het uitvoeren van dit strategisch informatiebeveiligingsbeleid. Het Dagelijks Bestuur (DB) stelt dit strategische informatiebeveiligingsbeleid vast en dit wordt ter informatie aangeboden aan het Algemeen Bestuur (AB). De directie van GBLT zorgt er voor dat de belangen en risico's van de informatievoorziening van GBLT duidelijk zijn, welke risico's GBLT hiermee loopt en welke van deze risico's onacceptabel hoog zijn.

---

[2] *De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.*

Op basis hiervan stelt de CISO het informatiebeveiligingsbeleid op, ondersteunt en bewaakt de uitvoering ervan.

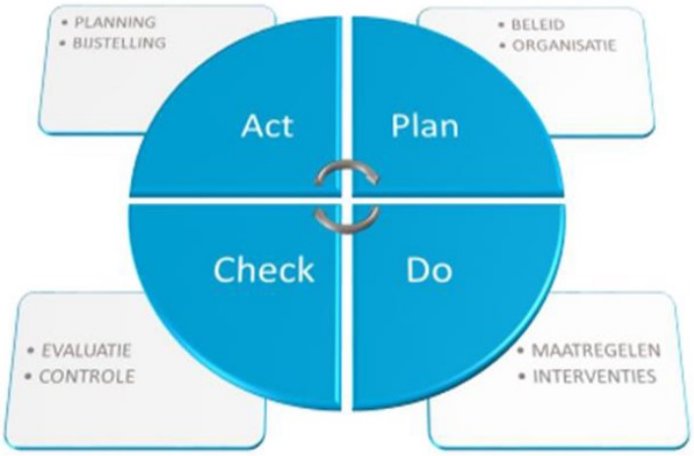
Het MT draagt uit dat informatiebeveiliging een belangrijk aspect is voor GBLT. Dit doet zij door het informatiebeveiligingsbeleid te onderschrijven en haar betrokkenheid te tonen. Het MT draagt dit actief uit en handhaaft dit richting de organisatie.

Dit strategische informatiebeveiligingsbeleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het strategische informatiebeveiligingsbeleid is in lijn met het algemene beleid van GBLT en de relevante landelijke en Europese wet- en regelgeving.

4.7 GBLT heeft de volgende uitgangspunten:

- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Overheid (BIO). Dit normenkader geldt dus expliciet ook voor de bedrijfsprocessen waar de audits zich op richten.
- GBLT conformeert zich aan dit normenkader, waarbij er ruimte is voor afweging en prioritering op basis van het “pas toe of leg uit” principe.
- Alle informatie en informatiesystemen zijn van belang voor GBLT, bepaalde informatie is van vitaal en kritiek belang.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van de directie, met het Dagelijks Bestuur als eindverantwoordelijke. De verantwoordelijkheden voor de bescherming van gegevens en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd.
  Alle informatiebronnen en -systemen die gebruikt worden door GBLT hebben een interne (proces)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 deze eigenaar van de informatie.
- Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen GBLT.
- Het strategisch informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatie breed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
- GBLT stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit strategische informatiebeveiligingsbeleid.
- Regels en verantwoordelijkheden voor het strategisch informatiebeveiligingsbeleid dienen te worden vastgelegd en vastgesteld. Alle gebruikers van informatiesystemen beschikken over voldoende kennis ten aanzien van informatiebeveiliging.
- 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 een continu verbeterproces. ‘Plan, do, check and act’. Dit wordt bijgehouden en vastgelegd in het ISMS evenals de implementatie van de BIO (zie afb. ISMS).

- In de Verklaring Van Toepasselijkheid (VVT) is vastgelegd welke beveiligingsrichtlijnen uit de BIO door GBLT van toepassing zijn verklaard, wanneer ze zijn of worden gerealiseerd en in welk document de maatregelen in opzet staan beschreven.



Informatie Security Management System

(afb. ISMS)

4.7.1 Strategische doelen

De strategische doelen van het strategische 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 klanten en medewerkers.
- Het waarborgen van de naleving van dit beleid.

4.7.2 Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- De directie is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- De directie is verantwoordelijk voor het vragen om informatie bij de proceseigenaren en ziet erop toe dat de proceseigenaren adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie.
- Tijdens P&C-gesprekken is er aandacht voor informatiebeveiliging.

- De onderwerpen, die als risicovol worden gezien, worden opgenomen in het controlejaarplan.
- De proceseigenaren zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- Hoewel de basisregistraties en kernregistraties belangrijk zijn in het kader van informatiebeveiliging, krijgen zij niet meer of minder voorrang dan andere (primaire) processen binnen GBLT. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van GBLT en het behalen van de doelen die zijn gesteld.
- Alle medewerkers van GBLT worden getraind in het gebruik van beveiligingsprocedures in bewustzijnstrajecten (zoals workshops en informatievoorziening op intranet).
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- Proceseigenaren dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen de juiste persoonsgegevens worden ingezien en verwerkt worden.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement.

4.7.3 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- Informatiebeveiliging wordt door het bestuur erkend als structurele randvoorwaarde voor het optimaal functioneren van GBLT.
- De informatiebeveiliging maakt deel uit van afspraken met opdrachtgevers en partners.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Het ISMS wordt continu bijgehouden, gebaseerd op:
  - Het normenkader BIO;
  - Het dreigingsbeeld gemeenten van de IBD;
  - De door de proceseigenaren ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.
  - Wettelijke bepalingen zoals bijvoorbeeld de actuele normenkaders van het Digid assessment.

5 Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie.

5.1 Aansturing: Directie

De directie zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een proceseigenaar. De directie zorgt dat de proceseigenaren zich verantwoorden over de beveiliging van de informatie die onder hen berust.

De directie stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De directie draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO van GBLT. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging en continuïteit wordt bij GBLT gezien als een integraal onderdeel van risicomanagement. GBLT beschouwt daarbij de BIO als normenkader.

5.2 Uitvoering: Proceseigenaren

Informatiebeveiliging valt onder de verantwoordelijkheden van alle proceseigenaren. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de organisatie. De proceseigenaren worden daarbij ondersteund en gefaciliteerd door de Security Officer en de CISO.

Taken van de proceseigenaren in het kader van informatiebeveiliging zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het binnen de eigen afdeling 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 overleg ligt bij de CISO.

5.3 Controle en verantwoording

Dit Strategisch informatiebeveiligingsbeleid is een verantwoordelijkheid van het dagelijks bestuur van GBLT. De bestuurders en directie van GBLT zullen volgens de 10 principes (hoofdstuk 4.2.2) voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.
De directie rapporteert daarnaast periodiek over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische informatiebeveiligingsbeleid.

5.4 Verantwoordelijkheden

1. Met betrekking tot het informatiebeveiliging worden de volgende functionarissen onderkend:
   - Het dagelijks bestuur
   - Directie
   - Systeem-, gegevens-, en proceseigenaren
   - Chief Information Security Officer (CISO)
   - Security Officer (SO)
   - Interne controle & audit
   - Adviseur risicomanagement
2. Het dagelijks bestuur keurt het beleid formeel goed en draagt zorg voor de naleving van het beleid van GBLT (Beleidsbepaling).
3. De directie is verantwoordelijk voor de uitvoering van het beleid en draagt zorgt voor de afstemming met het dagelijks bestuur.
4. De proceseigenaren zijn verantwoordelijk voor een correcte naleving van het beleid door hun medewerkers (Beleidsuitvoering).
5. De Chief Information Security Officer (CISO) ondersteunt vanuit zijn onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan het MT. De CISO is primair verantwoordelijk voor het informatiebeveiligingsbeleid. Dit betreft zowel het implementeren van beleid als het toezicht houden op de uitvoering ervan. De CISO wordt hierbij ondersteunt door de Security Officer (SO).
6. Het eigenaarschap van systemen, gegevens en processen is belegd bij de MT leden van GBLT. De eigenaren zijn verantwoordelijk voor het treffen en in stand houden van de autorisatiemaatregelen (Beleidsinrichting). De gegevenseigenaren zijn verantwoordelijk voor de beveiliging van de onder hun ressorterende gegevens. De gegevens-, systeem- of proceseigenaren verlenen de toestemming aan gebruikers tot gebruik van de onder de verantwoordelijkheid van de eigenaar ressorterende gegevens, systemen en processen (toewijzen van de autorisaties). Deze verleende rechten worden vastgelegd.
7. Interne controle & audit
   De interne auditor kan op verzoek een audit uitvoeren op informatiebeveiliging uitvoeren.
8. Adviseur risicomanagement
   De adviseur risicomanagement ondersteund bij het opstellen van risicoprofielen en geeft advies over de impact van risico's en het nemen van maatregelen om deze risico's te beheersen.

6 Bibliografie

IBD. (2022, 03 29). *Over de IDD*. Opgehaald van IBD: https://www.informatiebeveiligingsdienst.nl/over-de-ibd/

Informatiebeveiligingsdienst. (2019, 01 09). *De 10 bestuurlijke principes voor informatiebeveiliging*. Opgehaald van https://www.informatiebeveiligingsdienst.nl/: https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/01/De-10-bestuurlijke-principes-voor-Informatiebeveiliging_20190109.pdf

Staatscourant 2019, 26526. (2018, 12 14). Opgehaald van Staatscourant van het Koninkrijk der Nederlanden: https://zoek.officielebekendmakingen.nl/stcrt-2019-26526.html

Wikipedia Informatiebeveiliging. (2022, 03 29). Opgehaald van Wikipedia: https://nl.wikipedia.org/wiki/Informatiebeveiliging

gemeente- en
waterschapsbelastingen