IB BELEID

[OPDRACHTGEVER]

Auteur:	**Audittrail**
Opdrachtgever:	**[opdrachtgever]**
Versie:	**3.0**
Versiedatum:	**[datum oplevering]**

NHOUDSOPGAVE

REVISIEHISTORIE

Versie	Datum	Naam auteur	Wijzigingen
0.1	28-2-2019	Audittrail	Initiële versie
1.0	20-04-2019	Audittrail	Definitieve versie
1.1	06-02-2023	Audittrail	Review 2023
1.2	20-06-2024	Audittrail	Update BIC 4.0

1. ALGEMEEN

De directie en management spelen een cruciale rol bij het uitvoeren van dit informatiebeveiligingsbeleid. Zo maakt het management een inschatting van het belang dat de verschillende delen van de informatievoorziening voor [organisatie] hebben, de risico's die [organisatie] 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.

Het gehele management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitbrengen en handhaven van een informatiebeveiligingsbeleid van en voor heel [organisatie]. 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 de corporatie en de relevante landelijke en Europese wet- en regelgeving. Wetgeving richt zich sterk op het beschermen van privacy. Regelgeving is gericht op corporate governance en best practices voor bedrijfscultuur en -bestuur. Dit beleid bevat een bijlage met nadere aanwijzingen.

[Organisatie] is zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van het beleid.

Hierbij geldt:

- Er is wetgeving waar altijd aan voldaan moet worden, zoals Algemene Verordening Gegevens-bescherming (AVG), archiefwet, Wet computercriminaliteit (Wcc), Algemeen Burgerlijk Wetboek en de Telecommunicatiewet.
- [Organisatie] stelt dit normenkader vast, waarbij er ruimte is voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.

De volgende uitgangspunten zijn ontleend aan de Code voor Informatiebeveiliging (NEN/ISO 27002:2022)/Baseline informatiebeveiliging corporaties 4.0 (BIC 4.0):

1. Alle informatie en informatiesystemen zijn van kritiek en vitaal belang voor [organisatie]. De verantwoordelijkheid voor informatiebeveiliging ligt bij het (lijn)management, met de **directie als eindverantwoordelijke**. De verantwoordelijkheden voor de bescherming van gegevens en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd.

2. Door **periodieke controle, organisatie brede 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 organisatie breed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.

3. Informatiebeveiliging is een **continu verbeterproces**. 'Plan, do, check en act' vormen samen het **managementsysteem** van informatiebeveiliging.

4. De **informatiebeveiliging coördinator/security officer en/of- functionaris** ondersteunen vanuit een **onafhankelijke positie** de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover.

5. [Organisatie] stelt de benodigde **mensen en middelen beschikbaar** om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid.

6. **Regels en verantwoordelijkheden** voor het beveiligingsbeleid dienen te worden **vastgelegd** en **vastgesteld**. Alle medewerkers van [organisatie] worden getraind in het gebruik van beveiligingsprocedures.

7. 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.

Aldus vastgesteld door directeur-bestuurder van [organisatie] op *[datum].*

De informatiebeveiligingsterminologie die in dit document wordt gebruikt komt overeen met die van de Nederlandse vertaling van de ISO27002:2022/ BIC 4.0 in bijlage 2 zijn definities en verklaringen opgenomen.

1.1 DOELSTELLING BELEID

Het doel van dit beleid voor informatiebeveiliging (IB-beleid) is het bieden van een beleidskader waarmee [organisatie] kan zorgen voor een consistente en uitgebalanceerde set aan beveiligingsmaatregelen, zodanig dat:

- Van toepassing zijnde wet- en regelgeving wordt nageleefd;
- Gewaarborgd is dat [organisatie] aan haar primaire doelstellingen kan voldoen;
- (Toekomstige) maatregelen en investeringen in beveiliging getoetst kunnen worden;
- Bedrijfsschade en persoonlijk letsel zoveel als mogelijk wordt voorkomen en een veilige (werk)omgeving wordt geboden aan medewerkers, klanten, inleenkrachten en bezoekers.

1.2 KOPPELING BELEID AAN PRIMAIRE DOELSTELLINGEN [ORGANISATIE]

[Organisatie] ondersteunt mensen met betaalbare woningen. Dat is het belangrijkste uitgangspunt. Vanuit deze achtergrond zijn de aanvullende uitgangspunten op het gebied van informatiebeveiliging:

1. Veilig en betrouwbaar omgaan met informatie in het dagelijkse werk is ieders professionele verantwoordelijkheid.
2. Informatiebeveiliging en privacy zijn een continu proces.
3. [Organisatie] is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert [organisatie] informatie, waarvan het eigendom (auteursrecht) toebehoord aan derden.
4. In opdracht van de eigenaar, houdt en beheert de houder de informatie met behulp van een informatiesysteem (applicatie) en ziet toe op juiste classificatie, middels risicoanalyse, van het informatiesysteem op gebieden van BIV.

1.3 UITGANGSPUNTEN BELEID

De volgende uitgangspunten zijn gehanteerd bij het opstellen van dit beleid.

- Leidraad voor het IB-beleid [organisatie] is de Nederlandse vertaling van de internationale
- beveiligingsnorm ISO/IEC 27002:2022 of BIC 4.0.
- Certificering op basis van de ISO27001 norm is voor [organisatie] niet aan de orde.
- Het IB-beleid en plan moet toetsbaar zijn.
- Het IB-beleid en plan moeten door de directie erkend en goedgekeurd zijn
- Het IB-beleid beïnvloedt de dienstverlening slechts minimaal.
- Het IB-beleid sluit aan op andere bedrijfsbeleidsstukken. Wanneer het IB-beleid vervangend is voor ander beleid, dan zal dit expliciet in de tekst worden aangeven.
- Het IB-beleid en de maatregelen zijn risico gebaseerd. In het geval dat er maatregelen geselecteerd worden dient dit te gebeuren op basis van een risicoanalyse.
- Er behoort aandacht te zijn voor overlappende activiteiten met fysieke (gebouw)beveiliging en personele veiligheid.
- De beveiligingsorganisatie maakt voor zover mogelijk een integraal onderdeel uit van de bestaande organisatie.
- Het IB-beleid wordt zoveel mogelijk in de organisatie ingebed; toetsing en bewaking van dit beleid behoort onafhankelijk te worden belegd, intern dan wel extern.

1.4 REIKWIJDTE EN POSITIONERING BELEID

Het informatiebeveiligingsbeleid beschrijft de beveiligingssituatie die [organisatie] nastreeft voor al haar activiteiten. Veranderingen die van invloed zijn op informatiebeveiliging dienen in het licht van dit beleid beoordeeld te worden.

Dit beleid heeft niet alleen betrekking op de interne organisatie en technische infrastructuur van [organisatie], maar ook op de relatie met derden, zoals leveranciers, instanties waarmee gegevens worden uitgewisseld.

De in dit beleid beschreven beveiligingsnormen bestaan uit twee onderdelen, het strategische en tactische normenkader.

Het strategische normenkader is zodanig abstract dat de normen zoveel mogelijk onafhankelijk zijn (en daarmee toekomst bestendig) van de daadwerkelijke organisatorische en technische inrichting van [organisatie]. Een wijziging in de organisatie van [organisatie] hoeft niet direct te leiden tot aanpassing van dit normenkader.

De volledige versie van dit Informatiebeveiligingsbeleid vind u in de PRISM Kennisbank.

Dit informatiebeveiligingsbeleid legt de basis voor het beschermen van informatie binnen uw organisatie. Het document behandelt het doel van informatiebeveiliging en de essentiële principes, zoals betrouwbaarheid en risicomanagement, die de organisatie volgt om haar data en systemen veilig te houden. Daarnaast beschrijft het beleid de reikwijdte, het gebruik en voor wie het bedoeld is, zodat elke medewerker weet wat zijn of haar rol is in het beschermen van informatie.

Dit template is exclusief beschikbaar voor PRISM Members en dient als basis voor de vormgeving van een eigen, organisatie-specifiek cookiestatement.

Contactgegevens
Audittrail
Sisalbaan 5a
2352 AZ Leiderdorp

071 - 747 71 71
bijpraten@audittrail.n