Informatiebeveiligingsbeleid Stichting Inlichtingenbureau 2018-2020

Dit document beschrijft het strategisch informatiebeveiligingsbeleid van Stichting Inlichtingenbureau (IB) in de periode van 2018 tot en met 2020. Bij het uitvoeren van dit informatiebeveiligingsbeleid speelt het management een cruciale rol doordat het een inschatting maakt van het belang dat de verschillende onderdelen van de informatievoorziening voor het Inlichtingenbureau hebben, de risico's die de organisatie hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis daarvan maakt het management keuzes die worden vertaald in tactisch-operationeel beleid en de bijbehorende acties die worden opgenomen in jaarplannen informatiebeveiliging. Die jaarplannen worden als onderdeel van de PDCA-cyclus intern en extern gecommuniceerd. Het management bewaakt de uitvoering ervan. Op deze wijze geeft het gehele management een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt.

Strategisch informatiebeveiligingsbeleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen) daarnaast alle afspraken met externe leveranciers en ketenpartijen. Het informatiebeveiligingsbeleid past binnen het algemene beleid van de organisatie en de geldende en relevante landelijke en Europese wet- en regelgeving. Het Inlichtingenbureau is zelf verantwoordelijk voor het opstellen, uitvoeren en handhaven van het beleid. Hierbij geldt:

- De organisatie moet voldoen aan wet- en regelgeving, zoals (niet-uitputtend): de AVG en sectorspecifieke regelgeving zoals de wet, besluit en regeling SUWI.
- Het informatiebeveiligingsbeleid van IB is vanaf medio 2017 gebaseerd op de BIR. Een groeiende subset van BIR-normen vormt het toetsingskader voor de jaarlijkse externe EDP-audit. Met deze subset worden ook de normen afgedekt uit specifieke normenkaders zoals het GGK normenkader en het GeVS-normenkader.
- Jaarlijks wordt een IB-toetsingskader informatiebeveiliging vastgesteld op basis van een zo recent mogelijke versie van de BIR.

Het informatiebeveiligingsbeleid is gebaseerd op de volgende uitgangspunten:

1. Informatie en informatiesystemen zijn van kritiek en vitaal belang voor de organisatie. De verantwoordelijkheid voor informatiebeveiliging ligt bij het (lijn-) management, met het bestuur 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 en 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 beleid en het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
3. Informatiebeveiliging is een continue verbeterproces. 'Plan, do, check en act' (PDCA) vormen samen het managementsysteem van informatiebeveiliging.

4. De Chief Information Security Officer (CISO), de Technisch Informatie Security Specialist (TISS), en de architect – tezamen ondersteunen de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening. De CISO overziet security processen en beleid vanuit een onafhankelijke positie en rapporteert hierover aan de directeur.
5. De organisatie stelt de benodigde mensen en middelen beschikbaar om eigendommen en werkprocessen te kunnen beveiligen conform beleid.
6. Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld. Alle medewerkers van de organisatie worden getraind in het gebruik en de opvolging van beveiligingsprocedures.
7. Iedere medewerker, zowel vast als tijdelijk, intern of extern is verplicht gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

Dit informatiebeveiligingsbeleid treedt in werking na vaststelling. Het beleid wordt periodiek geëvalueerd (minstens eens in drie jaar) door de CISO in opdracht van de directeur.

Aldus vastgesteld door de directeur van het Stichting Inlichtingenbureau op 26 juni 2018.