BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 1616

13 september 2024

Officiële uitgave van de gemeenschappelijke regeling WerkSaam Westfriesland

Strategisch Informatie Beveiligingsbeleid (SIB) WerkSaam WF 2024 tot 2028

Managementsamenvatting

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid (SIB) voor de jaren 2024 tot 2028. Deze nota is richtinggevend en kaderstellend en beschrijft op strategisch niveau het informatiebeveiligingsbeleid, dat vervolgens wordt vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks op te stellen 'Informatiebeveiligingsplan'. De basis voor dit strategisch beleid vormen de NEN-ISO/IEC 27002 normen en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO).
Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen met als doel om de beschikbaarheid, integriteit en vertrouwelijkheid van persoonsgegevens en andere gevoelige informatie te waarborgen binnen WerkSaam. Dit is essentieel voor de naleving van de Algemene Verordening Gegevensbescherming (AVG), aangezien de borging van privacy afhankelijk is van adequate informatiebeveiliging. Het is de primaire verantwoordelijkheid van de procesverantwoordelijken en proceseigenaren om de eigen processen, systemen en gegevens te beveiligen en hier voldoende middelen voor beschikbaar te stellen. De Chief Information Security Officer (CISO) adviseert, coördineert en ondersteunt hierbij. Advies omtrent privacy en gegevensbescherming wordt gegeven door de Privacy Officer (PO) en Functionaris Gegevensbescherming (FG).
Het informatiebeveiligingsbeleid geldt voor alle processen binnen WerkSaam en zorgt ervoor dat informatie en de bijbehorende systemen gedurende hun hele levenscyclus goed beschermd worden.
Voor een veilige omgeving is het van belang informatiebeveiliging optimaal te professionaliseren. De Baseline Informatiebeveiliging Overheid (BIO) is het normenkader voor de gehele overheid, gebaseerd op de ISO-standaarden. Het helpt WerkSaam bij het nemen van haar verantwoordelijkheid ten aanzien van informatiebeveiliging. Risicomanagement is hierin een noodzakelijke randvoorwaarde. Het zorgt dat informatie en informatiesystemen niet te licht of te zwaar worden beveiligd. Er wordt een inschatting gemaakt van mogelijke gevolgen als informatiesystemen (tijdelijk) niet beschikbaar zijn, de informatie niet integer is en/of in verkeerde handen valt. Op basis van deze inschatting wordt gekeken of maatregelen passend zijn, aanvullende maatregelen nodig zijn en of het (rest)risico kan worden geaccepteerd.
Het huidige volwassenheidsniveau van informatiebeveiliging bij WerkSaam ligt op niveau 2.2. De ambitie is om eind 2024 volwassenheidsniveau 3 (figuur 1) en eind 2025 volwassenheidsniveau 4 te bereiken. Zodra dat niveau bereikt is, heeft WerkSaam informatieveiligheid geborgd binnen de processen, voldoet WerkSaam aan wet- en regelgeving én is er voldoende kennis om proactief op ontwikkelingen te anticiperen. Dan zijn de risico's verkleint tot een acceptabel niveau en in lijn met de ambities uit de strategische agenda. Het volwassenheidsniveau wordt periodiek geëvalueerd.

Figuur 1: BIO volwassenheidsmodel

1. Strategisch beleid 1.1 Doelstelling

Het informatiebeveiligingsbeleid bestaat uit de volgende lagen:

A. *St r ategisch informatiebeveiligingsbeleid (SIB)*
B. *Tactisch informatiebeveiligingsbeleid (TIB)*
C. *Op operationeel niveau:*
   a. *Een jaarlijks informatiebeveiligingsplan met concrete maatregelen*
   b. *Werkinstructies*

Elke laag legt de basis voor de onderliggende laag.

1.2 De 10 principes voor informatiebeveiliging

Als de informatiebeveiliging niet op orde is, kan dit gevolgen hebben voor cliënten, leveranciers en medewerkers van WerkSaam. Informatiebeveiliging is daarmee ook een zaak van de gehele organisatie en vereist een top-down benadering waarin het bestuur en management het voortouw neemt door duidelijke richtlijnen en beleid vast te stellen. Deze benadering zorgt ervoor dat alle medewerkers, ongeacht hun functie, het belang van informatiebeveiliging begrijpen en hun verantwoordelijkheid hierin erkennen. Door een cultuur van beveiligingsbewustzijn te bevorderen en passende middelen en training te bieden, wordt een veilige en betrouwbare werkomgeving gewaarborgd.
De 10 bestuurlijke principes voor informatiebeveiliging zijn een 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
9. Verbetering komt voort uit leren en ervaring
10. Het bestuur controleert en evalueert

Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

1.3 Scope Informatiebeveiliging

Het informatiebeveiligingsbeleid is van toepassing op alle:

- Processen
- Informatiesystemen
- Locaties, ruimten en bedrijfsmiddelen die worden gebruikt
- Medewerkers, zowel vast als tijdelijk, in- of extern
- Opdrachten, contracten of samenwerkingen met (keten)partners.

Het heeft betrekking op het Algemeen Bestuur, Dagelijks Bestuur, directie, Strategisch Management Team (SMT), Tactisch Overleg (TO), middenkader, staf, OR, alle medewerkers, stagelopers, cliënten, gasten, bezoekers en externe relaties.

1.4 Randvoorwaarden en uitgangspunten

Iedere medewerker werkzaam voor WerkSaam is verantwoordelijk voor informatiebeveiliging. De beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens en daarmee onze dienstverlening staat hierbij centraal. Het bestuur en het management spelen hierbij een cruciale rol.

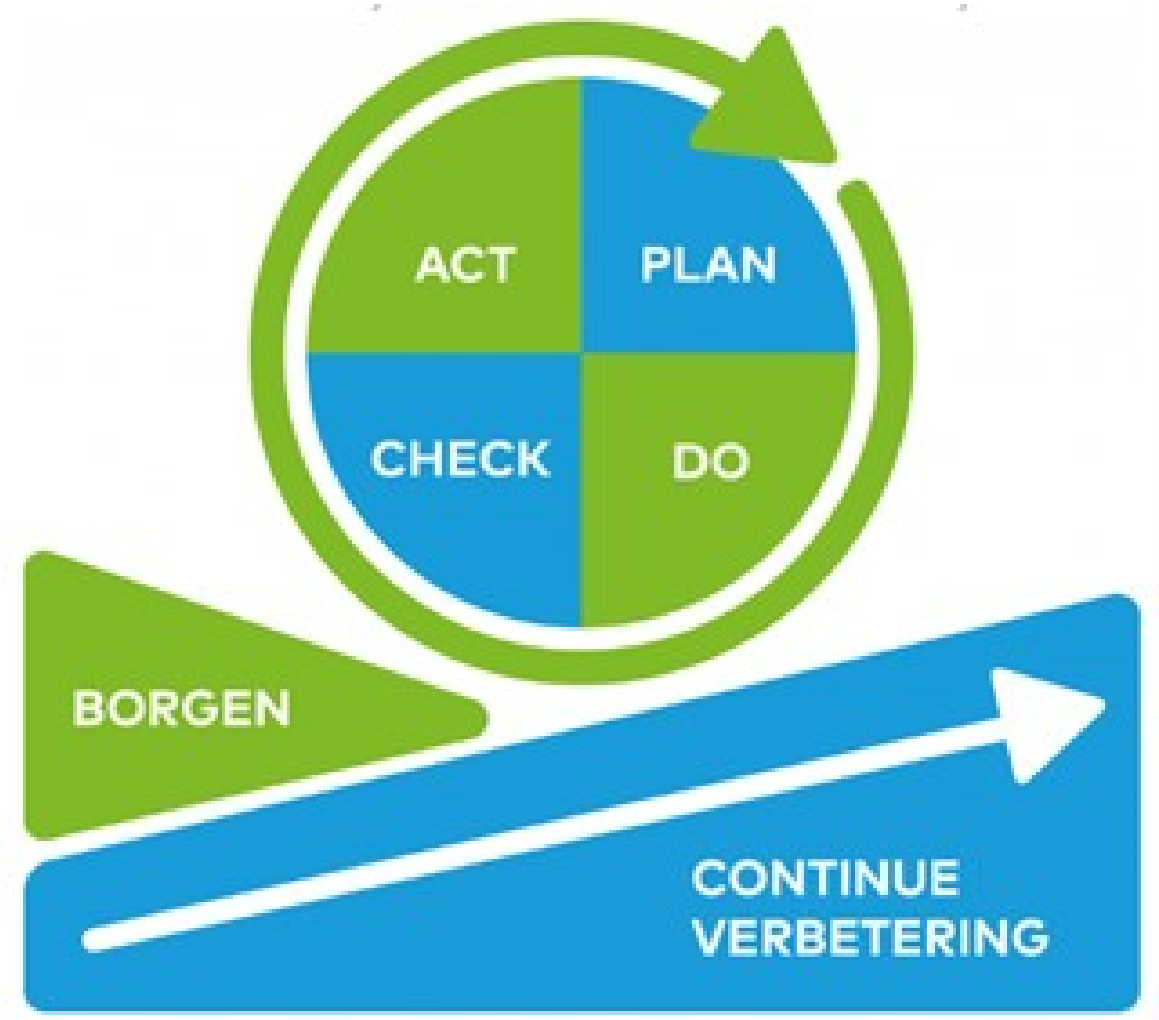
1.4.1 Belangrijkste randvoorwaarden

- Informatiebeveiliging is een verantwoordelijkheid van alle medewerkers.
- Informatiebeveiliging is gebaseerd op risicomanagement.
- Informatiebeveiliging maakt deel uit van afspraken met (keten)partners.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met gegevens wordt actief bevorderd en geborgd.

- Er zijn mensen en middelen beschikbaar gesteld om de juiste beschikbaarheid, integriteit en vertrouwelijkheid van gegevens te garanderen.

1.4.2 Belangrijkste uitgangspunten

- De informatiebeveiliging is in lijn met relevante wet- en regelgeving en normenkaders;
- De uitvoering van informatiebeveiliging is de verantwoordelijkheid van directie en MT;
- Alle processen en informatiesystemen hebben een proceseigenaar die zorgt voor de juiste mate van beschikbaarheid, integriteit en vertrouwelijkheid;
- Informatiebeveiliging is een continu verbeterproces. De PDCA-cyclus (zie figuur 2) vormt het managementsysteem van informatiebeveiliging. Door periodieke controle, organisatie brede planning en coördinatie is de beveiliging van de informatievoorziening verankert binnen WerkSaam;
- Er is een informatiebeveiligingsplan. Dit plan wordt periodiek, jaarlijks, bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses;
- Procedures, afspraken en verantwoordelijkheden voor Informatiebeveiliging zijn vastgelegd en worden waar nodig bijgesteld;
- Alle medewerkers van WerkSaam zijn op de hoogte van de beveiligingsprocedures en passen deze toe;
- Iedere medewerker 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.

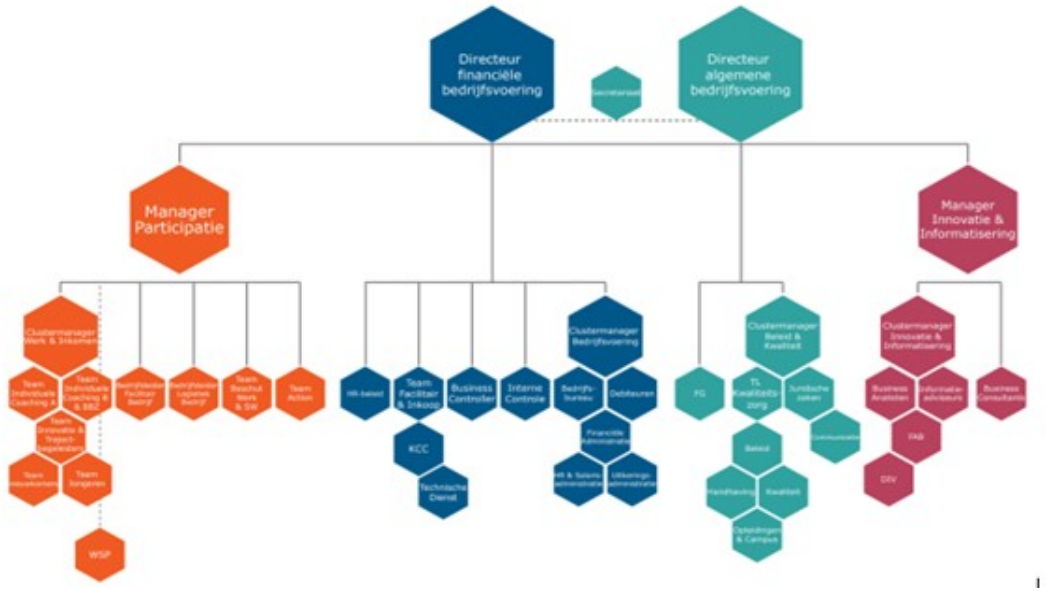


Figuur 2: PDCA-cyclus

2. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk zijn de taken en verantwoordelijkheden met betrekking tot informatiebeveiliging beschreven.

2.1 Organigram WerkSaam



2.2 Bestuur (algemeen en dagelijks)

Het dagelijks bestuur is eindverantwoordelijk voor de informatiebeveiliging binnen WerkSaam. Het bestuur stelt, als eindverantwoordelijke, het strategisch en tactisch informatiebeveiligingsbeleid vast.

2.3 Procesverantwoordelijke (Directie en SMT)

De directie en het SMT zijn betrokken en ondersteunen bij, geven duidelijke richting aan en dragen het belang van informatiebeveiliging uit. Zij borgen dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een clustermanager, bedrijfs- of teamleider. De procesverantwoordelijke:

- Zorgt dat proceseigenaren zich verantwoorden over de informatieveiligheid van de informatie in processen en systemen waar zij verantwoordelijk voor zijn.
- Beoordeelt periodiek het informatiebeveiligingsbeleid op basis van de evaluatie van de CISO en laat eventueel waar nodig bijstellen.
- Zorgt dat de CISO naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met informatiebeveiliging.
- Ziet erop toe dat de medewerkers geïnformeerd worden over informatiebeveiliging.

2.4 Proceseigenaren (Clustermanagement, team- en bedrijfsleiders)

De proceseigenaar is verantwoordelijk voor de beveiliging van een proces/informatiesysteem. Alle processen, systemen, data en applicaties hebben een proceseigenaar. De proceseigenaren:

- Zijn primair verantwoordelijk voor de bescherming van informatie in het proces.
- Stellen jaarlijks het informatiebeveiligingsplan vast in het tactisch overleg.
- Zijn verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels.
- Zien erop toe dat het gewenste niveau van beschikbaarheid, integriteit en vertrouwelijkheid is vastgesteld en geborgd per proces/ informatiesysteem.
- Sturen op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn). Het bespreken van beveiligingsincidenten en de consequenties hiervan voor beleid en maatregelen is hier onderdeel van.

- Maken een inschatting van de risico's en dreigingen die WerkSaam loopt op het gebeid van informatieveiligheid en treft maatregelen waar de risico's hoog zijn.
- Maken afspraken met andere organisatieonderdelen over het borgen van de informatieveiligheid als informatie stroomt tussen verschillende organisatieonderdelen.
- Zorgen voor de juiste beveiliging door derden als (delen van) de ontwikkeling, exploitatie of het onderhoud van systemen wordt uitbesteed.
- Zien erop toe dat controles op informatieveiligheid regelmatig worden uitgevoerd, zodat vastgesteld kan worden dat alleen rechthebbenden gegevens/informatie kunnen inzien en/of gebruiken.
- Rapporteren over compliance aan wet- en regelgeving en het beleid.
- Zorgen voor de aanlevering aan de ENSIA-coördinator van de informatie die nodig is voor de ENSIA-verantwoording.
- Leveren input voor wijzigingen op maatregelen en procedures.
- Het uitdragen binnen de eigen afdeling van het beveiligingsbeleid en de daaraan gerelateerde procedures.
- Signaleren vroegtijdig de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Bespreken beveiligingsincidenten en de consequenties die deze moeten hebben voor beleid en maatregelen.

2.5 Controle en verantwoording

De directeur Bedrijfsvoering informeert het bestuur periodiek over de stand van zaken met betrekking tot informatiebeveiliging.

2.5.1 Verantwoordingstraject ENSIA (m.b.t. de Suwinet diensten)

De gemeenten voor wie WerkSaam de Participatiewet verzorgt, moeten zich verantwoorden middels de ENSIA-systematiek. WerkSaam is verantwoordelijk om te voldoen aan de normen en eisen van het gebruik van Suwinet en DigiD op onze website. Wij dragen ervoor zorg dat we voldoen aan de DigiD audit én leveren TPM's (Third Party Mededeling) aan de ENSIA-coördinatoren van de verschillende gemeenten.

Vastgesteld in de vergadering van het dagelijks bestuur van 12 september 2024.
De voorzitter,
Y.W. Nijsingh

De directeur algemene bedrijfsvoering,
D.G.H. Gelinck