FERM WERK
brengt mens en werk samen

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 600
21 juni
2023

Officiële uitgave van de gemeenschappelijke regeling Ferm Werk

Informatiebeveiligingsbeleid Ferm Werk 2023-2027

1. Vertrekpunt informatiebeveiligingsbeleid Ferm Werk

Deze beleidsnota beschrijft het informatiebeveiligingsbeleid van Ferm Werk voor de jaren 2023 tot 2027. Het in 2019 vastgestelde *'Strategisch Informatiebeveiligingsbeleid 2019-2022'* is hiermee vervangen. Dit herziene beleid borduurt voort op de reeds ingeslagen richting gebaseerd op het normenkader BIO (Baseline Informatie Overheid) dat Ferm Werk noodzaakte nieuw en passend informatiebeveiligingsbeleid te formuleren. Daarnaast zijn er aanscherpingen, gebaseerd op de resultaten van de BIO-metingen van de afgelopen jaren.
Met dit *'Informatiebeveiligingsbeleid 2023-2027'* zet Ferm Werk een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te waarborgen. Daarbij houden we rekening met het feit dat informatiebeveiliging een proces is waar de komende jaren continue aandacht voor nodig is.

1.1 Wat informatiebeveiliging is

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 alle informatiestromen.
Het informatiebeveiligingsbeleid geldt voor alle processen binnen Ferm Werk. Het omvat dus de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie of het karakter van de informatie. Het beperkt zich niet alleen tot de ICT maar heeft ook betrekking op het (politiek) bestuur, alle processen en op personen; alle medewerkers, inwoners en externe partijen.

1.2 Ambitie/doelstelling

De NOREA heeft een model ontwikkeld om de volwassenheid op het vlak van informatie-beveiliging te kunnen duiden op een schaal van 1 tot 5 (laag tot hoog).

Figuur 1 Volwassenheidsniveau informatiebeveiliging
Om aantoonbaar een informatieveilige organisatie te zijn en te (kunnen) voldoen aan de AVG, dient de gemeente op alle aspecten minimaal een 3,0 te scoren. Het streven is stapsgewijs deze score te behalen op alle aspecten. De verantwoordelijkheid voor het behalen van deze doelstelling ligt breed binnen de gehele organisatie.
Naar verwachting worden de normen aangescherpt externe en interne dreigingen het hoofd te kunnen bieden.

2. Inleiding

2.1 Doel van dit beleid
Het informatiebeleid is gebaseerd op het normenkader voor de gehele overheid, de Baseline Informatiebeveiliging Overheid (BIO). Het doel van dit beleidsstuk is het bieden van kaders en beschrijven van rollen en verantwoordelijkheden ten aanzien van de informatiebeveiliging voor Ferm Werk voor een periode van vier jaar. De concrete uitwerking van dit beleid vindt plaats in een nog op te stellen Informatiebeveiligingsplan.

2.2 Scope informatiebeveiliging
De scope van dit beleid omvat alle processen, onderliggende informatiesystemen, informatie en gegevens van Ferm Werk en haar externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.
Het informatiebeveiligingsbeleid is een algemene basis. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen (bijvoorbeeld ENSIA). Deze worden in aanvullende documenten geformuleerd.
Het beleid bevat geen limitatief overzicht van onderliggende documenten. Wel dienen beleidsdocumenten voor de bedrijfsvoering zich te conformeren aan de bepalingen van het informatiebeveiligingsbeleid, waardoor wordt voldaan aan de BIO normen.

3. Aandachtspunten voor informatiebeveiliging

3.1 Plaats van het informatiebeveiligingsbeleid
Deze nota beschrijft op hoofdlijnen het informatiebeveiligingsbeleid van Ferm Werk. Dit beleid wordt vertaald naar tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in een twee jaar geldend nog te schrijven Informatiebeveiligingsplan.

3.2 Dreigingsbeeld Nederlandse Gemeenten
Het Dreigingsbeeld Nederlandse Gemeenten[1] 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 voor Ferm Werk een informatiebron voor het identificeren van nieuwe risico's en dreigingen. De CISO is namens Ferm Werk aangemeld bij de Informatiebeveiligingsdienst (IBD, VNG) en ontvangt periodiek berichten en rapportages hierover. Deze worden meegenomen in verschillende rapportages. Aansluitend hierop worden passende maatregelen genomen.

3.3 Informatie uit incidenten en inbreuken op de beveiliging
Ferm Werk kent naast het hierboven genoemde dreigingsbeeld ook een incidentenprocedure waarin wordt aangegeven hoe incidenten worden vastgelegd en gemonitord. Het bewaken van de oplossing van de beveiligingsincident wordt uitgevoerd door het team privacy en informatiebeveiliging (PIV) en de ICT manager binnen Ferm Werk..
Het functioneren en behoud van deze procedure zijn de verantwoordelijkheid van de controller met portefeuille bedrijfsvoering en wordt gewaarborgd door (integrale/) informatieveiligheid.

3.4 Randvoorwaarden
Belangrijke randvoorwaarden om dit beleid te implementeren zijn:
- *De informatiebeveiligingstaken zijn integraal onderdeel van de bedrijfsprocessen. Waar nodig worden de juiste veiligheidsmaatregelen getroffen om kwetsbaarheden in de processen te verkleinen.*
- *Alle medewerkers binnen Ferm Werk worden getraind in het gebruik en toepassen van de juiste beveiligingsprocedures.*
- *Medewerkers gaan verantwoord om met (persoons)gegevens en andere informatie(systemen). Ze spreken elkaar aan op onveilig gedrag en melden mogelijke hiaten direct aan de leidinggevenden.*
- *De informatiebeveiliging maakt deel uit van afspraken met ketenpartners en dienstenleveranciers.*
- *Kennis en bewustzijn van informatiebeveiliging wordt actief bevorderd en geborgd bij alle lagen binnen de organisatie, ketenpartners en externe partijen.*

1) Het dreigingsbeeld NL/IBD: https://www.informatiebeveiligingsdienst.nl/product/dreigingsbeeld-informatiebeveiliging-nederlandse-gemeenten-2021-2022/

- *Periodiek worden onafhankelijke audits uitgevoerd om vast te stellen of de vereiste maatregelen uit het beleid in voldoende mate zijn geborgd.*
- *Security en privacy by design principes worden toegepast bij innovaties. Denk hierbij aan common ground , internet of things (IoT) en datagedreven werken.*

3.5 Doelen Informatiebeveiliging

Ferm Werk kent de volgende doelen voor het informatiebeveiligingsbeleid:

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

De vertaling van deze doelen komt verder tot uiting in het op te stellen Informatiebeveiligingsplan.

4. Principes van informatiebeveiliging

De BIO (Baseline Informatiebeveiliging Overheid) is sinds 1-1-2019 het nieuwe normenkader voor de gehele overheid. De werkwijze van deze BIO is meer gericht op risicomanagement, in tegenstelling tot de voormalige Baseline Informatiebeveiliging Gemeente (BIG)-richtlijnen. Dat wil zeggen dat proceseigenaren nu meer dan voorheen dienen te werken volgens de aanpak van de ISO-27001, waarbij risicomanagement centraal staat. Dit houdt voor het MT in dat zij op voorhand keuzes en continu afwegingen dienen te maken of informatie in bestaande en nieuwe processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

4.2 Handvaten voor de rol van de bestuurder

De 10 principes voor de informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader[2] BIO. Ze gaan over de waarden die het bestuur aan de organisatie en zichzelf oplegt. De principes zijn als volgt:

1. Bestuurders bevorderen een veilige cultuur;
   Menselijk gedrag en cultuur beïnvloeden op significante wijze alle aspecten van risicomanagement op elk niveau en in elk stadium. Informatiebeveiliging is van iedereen.
2. Informatiebeveiliging is risicomanagement;
   Passende en tijdige betrokkenheid van belanghebbenden maakt het mogelijk dat hun kennis, opvattingen en percepties worden meegenomen in het informatiebeleid en de te nemen maatregelen. Dit resulteert in een verbeterd bewustzijn en goed geïnformeerd risicomanagement.
3. Risicomanagement is onderdeel van de besluitvorming;
   Risicomanagement wordt bewust toegepast bij alle organisatie-activiteiten en in het bijzonder bij de besluitvorming.
4. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking;
   Risicomanagement is onderdeel van alle besluiten en onderdeel van integraal management..
5. Informatiebeveiliging is een proces;
   Het risicomanagementproces wordt aangepast op basis van nieuwe ontwikkelingen en staat in verhouding tot doelstellingen en de context van de organisatie.
6. Onzekerheid dient te worden ingecalculeerd[3];
7. Risico's kunnen ontstaan, veranderen of verdwijnen als de externe en interne context van een organisatie verandert. Risicomanagement detecteert en anticipeert op die veranderingen en gebeurtenissen op een gepaste en tijdige manier.
8. Informatiebeveiliging kost geld;

2) Deze principes worden gelijk met de BIO van kracht, zie besluitvorming Informatiebeveiligingsdienst (IBD) en de Verenigde Nederlandse Gemeenten (VNG).

3) Het incalculeren van onzekerheden; besluiten worden gebaseerd op historische en actuele informatie, evenals op toekomstige verwachtingen. Risicomanagement houdt expliciet rekening met eventuele beperkingen en onzekerheden die aan dergelijke informatie en verwachtingen zijn verbonden. Informatie moet tijdig, duidelijk en beschikbaar zijn voor relevante belanghebbenden.

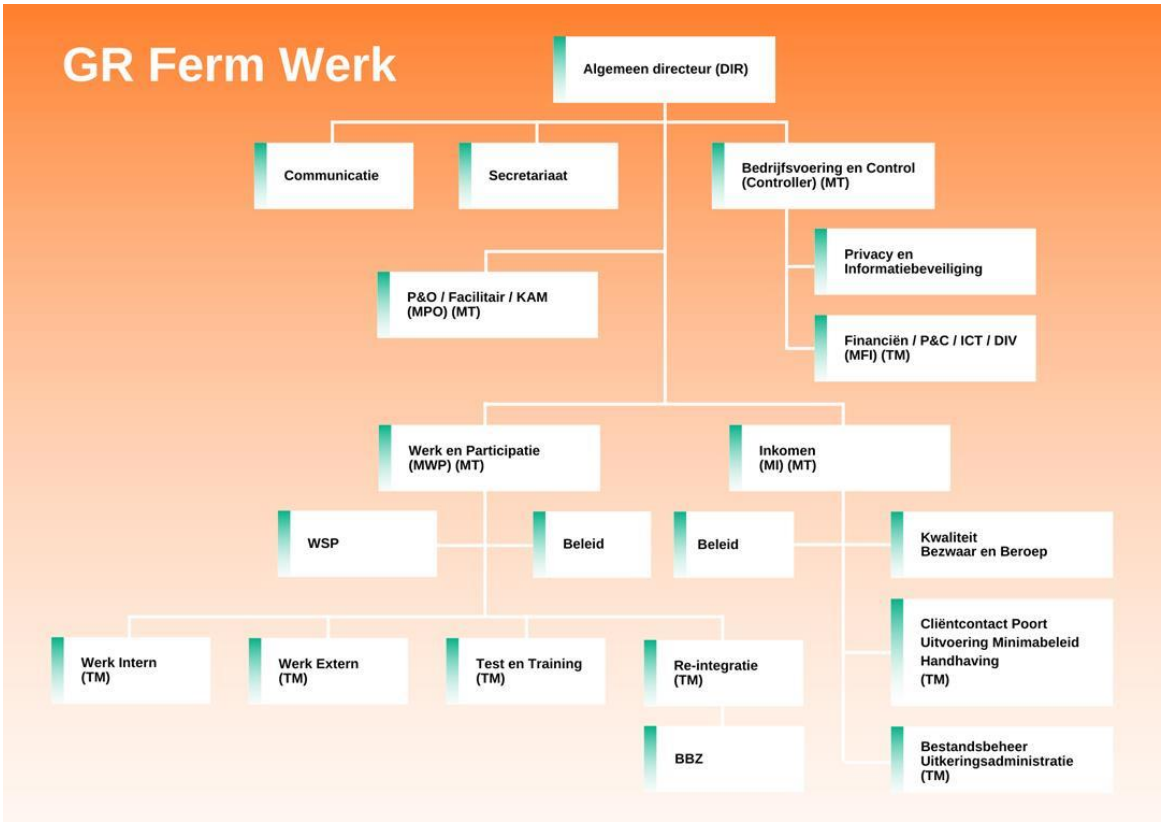
Risico's moeten behandeld worden en er zijn vele manieren om veiligheid te realiseren, maar aan alle zijn kosten verbonden.

9. Onzekerheid dient te worden ingecalculeerd;
   De input voor risicomanagement is gebaseerd op historische en actuele informatie, evenals op toekomstige verwachtingen. Risicomanagement houdt expliciet rekening met eventuele beperkingen en onzekerheden die aan dergelijke informatie en verwachtingen zijn verbonden. Informatie moet tijdig, duidelijk en beschikbaar zijn voor relevante belanghebbenden.
10. Verbetering komt voort uit leren en ervaring;
    Risicobeheer wordt voortdurend verbeterd door leren en ervaring.
11. Het bestuur controleert en evalueert;
    Risicomanagement is het controleren en evalueren van resultaten, evenals het nemen van eindverantwoordelijkheid en het doorhakken van lastige knopen.

Deze principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeenschappelijke regeling. Ze ondersteunen de bestuurder bij het waarborgen van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van Ferm Werk. Daarmee hoort het onderwerp informatiebeveiliging thuis op de bestuurstafel.

5. Governance van informatiebeveiliging

Voor een gedegen organisatie van informatiebeveiliging binnen Ferm Werk staat risicomanagement centraal. Het Dagelijks Bestuur (DB), managementteam (MT) en teammanagers spelen een cruciale rol binnen Ferm Werk bij het waarborgen van dit informatiebeveiligingsbeleid. Hieronder zijn hun rol en verantwoordelijkheden benoemd.



Figuur SEQ Figuur * ARABIC 2: Organigram Ferm Werk

5.1 Het Dagelijks Bestuur (DB)

- Het DB stelt het informatiebeveiligingsbeleid vast, gebaseerd op het ambitieniveau, actuele ontwikkelingen en de stand van zaken bij Ferm Werk;
- Het DB is verantwoordelijk voor het behalen van de doelstelling rondom de volwassenheid van informatiebeveiliging, te weten minimaal niveau 3,0 voor alle aspecten;

- De directeur is verantwoordelijk voor het toezien op de gemaakte afspraken rondom informatiebeveiliging.

5.2 Het Management Team (MT)

- Het MT is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit informatiebeveiligingsbeleid.
- Het MT is verantwoordelijk voor het vragen om informatie bij de teammanagers en ziet erop toe dat de managers adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoording valt.
- Het MT is verantwoordelijk voor het inrichten en uitvoeren van een bewustzijnsprogramma ten aanzien van informatiebeveiliging en privacy.
- Het MT-lid met de portefeuille Bedrijfsvoering is bovendien verantwoordelijk voor het waarborgen van de incidentmanagementprocedure.

5.3 Teammanagers (proceseigenaren)

- De teammanagers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij zorgdragen.
- De teammanagers zijn verantwoordelijk voor opzet en onderhoud van de dataclassificatie van de datasets die zij onder hun hoede hebben. Er worden adequate maatregelen genomen om de risico's die op basis van deze dataclassificatie duidelijk worden, te verkleinen.
- Teammanagers zien er aantoonbaar op toe dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd. Zo kunnen zij vaststellen dat alleen rechthebbende medewerkers de juiste persoonsgegevens ingezien en verwerkt hebben.

5.4 Alle medewerkers

- Alle medewerkers van Ferm Werk worden getraind in het gebruik van beveiligingsprocedures.
- Medewerkers gaan verantwoord om met persoonsgegevens en andere informatie.
- Medewerkers doen een melding bij afwijkingen, incidenten of vragen.

5.5 Specifieke rollen en taken 5.5.1 Controller & CISO

- 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 het MT.
- De Concerncontroller bewaakt het algemeen belang van Ferm werk ten aanzien van informatiebeveiliging.
- Tijdens P&C cyclus is er aandacht voor de informatiebeveiliging n.a.v. de rapportage van de CISO. Onderwerpen, die als risicovol worden gezien, moeten worden opgenomen in de auditplannen.

5.5.2 Interne en externe controleurs

- FG Privacy
- CISO Informatiebeveiliging/ IT-audits
- Controllers Financiën/ Bedrijfsvoering

5.5 Het belang van betrokkenheid

Het Dagelijks Bestuur, managementteam en de teammanagers spelen een cruciale rol binnen Ferm Werk bij het waarborgen van dit informatiebeveiligingsbeleid.
Teammanagers maken een inschatting van het belang dat de verschillende delen van de informatievoorziening voor Ferm Werk hebben, van de risico's die Ferm Werk hiermee loopt op basis van de opgestelde richtlijnen[4]. Ook dragen zij verantwoordelijkheid voor het uitdragen, ondersteunen en bewaken van dit informatiebeveiligingsbeleid. Zij rapporteren hierover middels BIO-metingen. De CISO gebruikt deze rapportages om het informatiebeveiligingsniveau periodiek te toetsen en Ferm Werk te adviseren vanuit het perspectief van de veiligheid.
Het MT bepaalt uiteindelijk welke van bedrijfsmatige risico's acceptabel of onacceptabel zijn. Verder geeft het 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 heel Ferm Werk.

4) Deze richtlijnen komen voort uit het Informatiebeveiligingsbeleid en het informatiebeveiligingsplan.

Het DB is verantwoordelijk voor het goedkeuren en waarborgen van de inhoud van het informatiebeveiligingsbeleid.

6. Rapportagemomenten voor informatiebeveiliging

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

De gemeenten voor wie Ferm Werk sociale zaken verzorgt, moeten zich verantwoorden middels de ENSIA-systematiek. Hierbij ligt een verantwoordelijkheid omtrent kwaliteitsgarantie voor Ferm Werk, door het leveren van TPM's (Third Party Mededeling). Jaarlijks worden deze TPM's geleverd aan de ENSIA-coördinatoren van de verschillende gemeenten. Ook wordt het MT ingelicht over de resultaten.

6.2 Periodieke toetsing

De CISO stelt jaarlijks van een stand ten opzichte van de BIO normeringen op. Deze rapportage dient als sturingsmiddel voor de bedrijfsvoering en wordt hiertoe verstrekt aan het MT. Op basis van deze input en de overige activiteiten en vorderingen op dit gebied wordt gerapporteerd aan het bestuur via de planning en control cyclus.