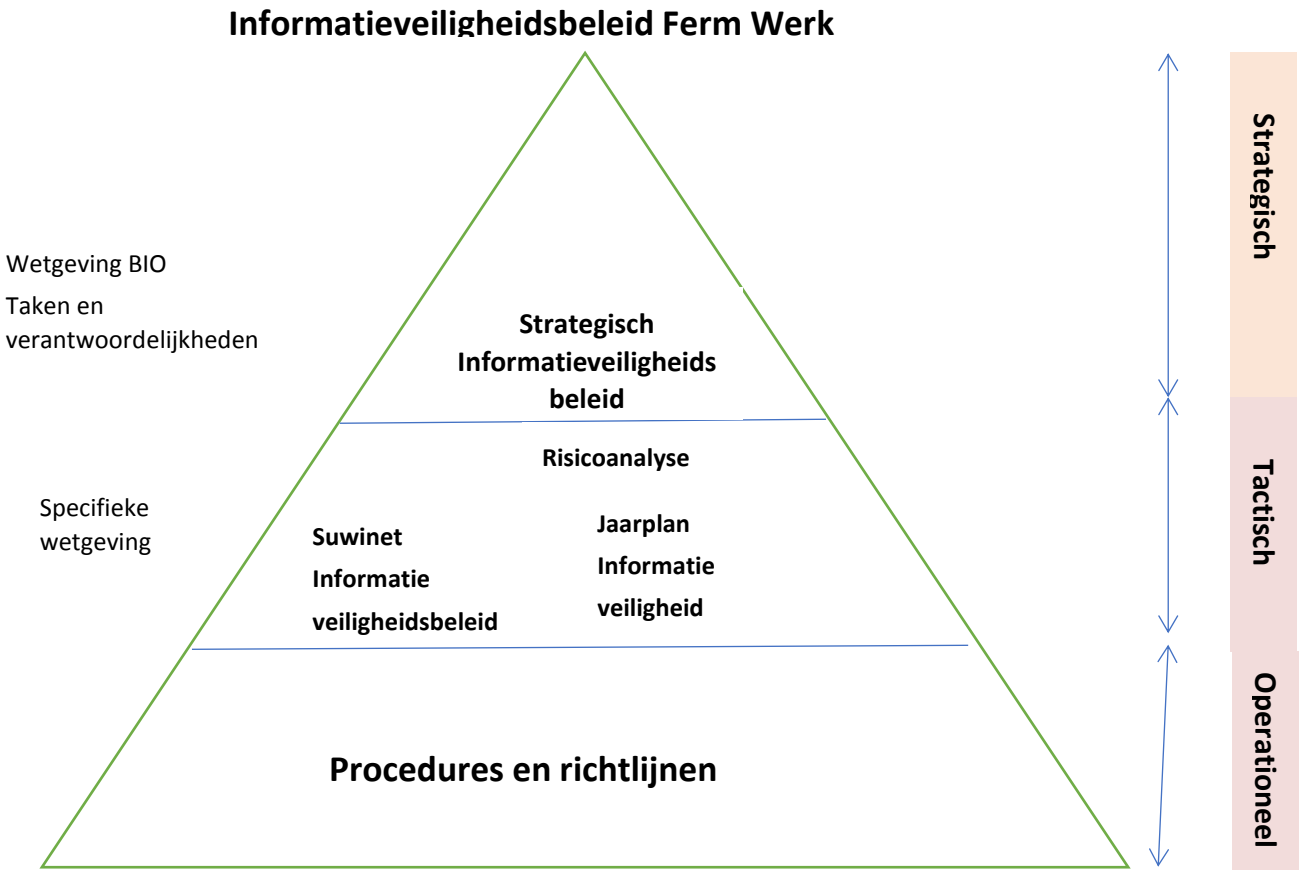
Strategisch Informatiebeveiligingsbeleid 2019 - 2022

Ferm Werk

Inhoud

Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2019 tot 2022.



Het beleid wordt vastgesteld door het Dagelijks bestuur[1] van de GR Ferm Werk en ter info gestuurd aan het Algemeen Bestuur en de raad van de commissarissen van Ferm Werk N.V.

Deze beleidsnota is richtinggevend en kaderstellend en wordt aangevuld met onderwerp-specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau. De specifieke beleidsdocumenten en werkinstructies worden vastgesteld door het management.

[1] Bevoegdheid en verantwoordelijkheid t.a.v. Informatieveiligheid
Op grond van artikel 4 en 5 van de Gemeenschappelijke Regeling Ferm Werk verricht de uitvoeringsorganisatie Ferm Werk als basisdienstverlening de uitvoering van de aan de deelnemers opgedragen of in de toekomst op te dragen taken in het kader van de Wet sociale werkvoorziening, de Participatiewet, de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers, de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen, het Besluit bijstandsverlening zelfstandigen en de Wet inburgering. Bij de uitvoering van de genoemde wetten worden op grote schaal persoonsgegevens verwerkt. Het verwerken van persoonsgegevens wordt beheerst door de Algemene Verordening Gegevensbescherming. Het bestuur van Ferm Werk is verwerkingsverantwoordelijke (art. 4, 7e lid AVG) aangezien Ferm Werk op grond van een specifieke juridische bevoegdheid het doel en de middelen voor de verwerking vaststelt. Op grond van artikel 24, 1e lid AVG bestaat de verplichting technische en organisatorische maatregelen te treffen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de Algemene Verordening Gegevensbescherming wordt uitgevoerd. De technische en organisatorische maatregelen moeten voldoen aan het normenkader van de Baseline Informatieveiligheid Overheid, die per 1 januari 2020 geldt voor de gehele overheid.
Op grond van voorgaande overweging is het dagelijks bestuur van Ferm Werk bevoegd en verantwoordelijk voor het vaststellen van het Informatiebeveiligingsbeleid.

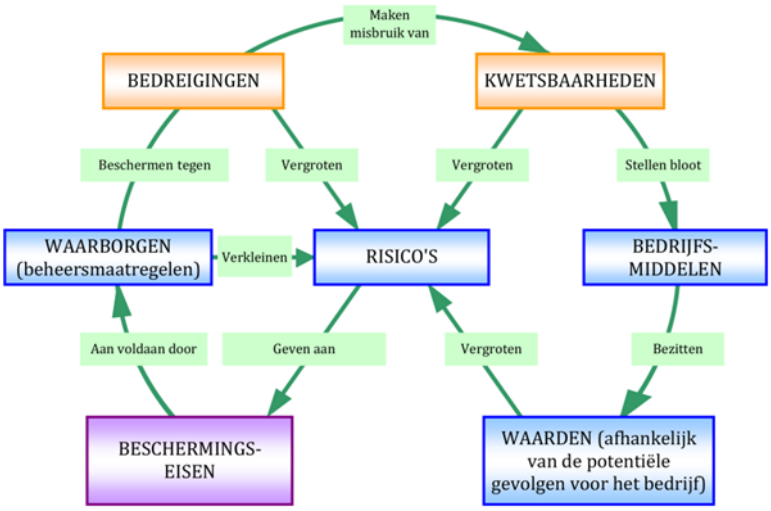
Met dit 'Strategisch Informatiebeveiligingsbeleid 2019-2022' zet Ferm Werk een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen Ferm Werk te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit strategisch beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO).

Leeswijzer

In hoofdstuk 2 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 jaarlijks uit te brengen gemeentelijk Informatiebeveiligingsplan (vastgesteld door het hoogste management) worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van het management, de CISO's van Ferm Werk en de deelnemende gemeenten , het dreigingsbeeld van de IBD[2] en de uitkomsten van ENSIA[3]. 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 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie zijn belegd.

Informatiebeveiliging

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 andere informatie.



Het informatiebeveiligingsbeleid geldt voor alle processen van Ferm Werk 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 politieke bestuur, alle medewerkers, cliënten, gasten, bezoekers en externe relaties.

[2] IBD: Informatie Beveiligingsdienst, onderdeel van VNG Realisatie.
[3] ENSIA: de Eenduidige Normatiek Single Information Audit, volgens welke systematiek het bestuur van de gemeenten verantwoording afleggen over de Informatieveiligheid aan de gemeenteraad en externe toezichthouders.

Ambitie en visie van Ferm Werk op het gebied van informatieveiligheid

Beschikbare, integere en vertrouwelijke informatie is een belangrijke voorwaarde. Informatie is één van de voornaamste bedrijfsmiddelen van onze organisatie; we zijn als overheidsinstelling immers een informatie verwerkende en leverende organisatie. Het goed organiseren van de informatievoorziening draagt bij aan het efficiënt inrichten van de bedrijfsvoering.

Strategisch beleid

2.1 Doel

Het doel van deze beleidsnota is het presenteren van het 'Strategisch Informatieveiligheidsbeleid voor de jaren 2019 tot 2022'. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen informatieveiligheidsbeleidsplan.

2.2 Uitgangspunten

De uitgangspunten die van belang zijn voor de actualisering van het informatieveiligheidsbeleidsplan zijn de volgende:

2.2.1 De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is het nieuwe normenkader voor de gehele overheid. De werkwijze van deze BIO is meer gericht op risicomanagement dan de oude Baseline Informatie Veiligheid Gemeenten. Dat wil zeggen dat het management nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

2.2.2 De 10 principes voor informatieveiligheid

De 10 principes voor informatiebeveiliging zijn een bestuurlijke 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.

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen processen, dan kan dit directe gevolgen hebben voor cliënten, ondernemers, bestuurders en partners van Ferm Werk. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel. Voor een nadere uitwerking van deze regels zie Bijlage 2.

2.2.3 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. Het dreigingsbeeld wordt actief gevolgd door de CISO en afhankelijk van de risicoanalyse worden er maatregelen genomen.

2.2.4 Informatie uit incidenten en inbreuken op de beveiliging

Ferm Werk heeft het systeembeheer uitbesteed aan de Gemeente Woerden. De gemeente kent naast het hierboven genoemde dreigingsbeeld natuurlijk een eigen systeem waarin incidenten worden vastgelegd. Dit systeem (TOPdesk©) geeft ook waardevolle informatie om van te leren en daarmee zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

2.2.5 Actuele bedreigingen

1		Malware in de vorm van virussen, cryptolockers en spyware.
2		Aanvallen op de ICT infrastructuur en de webapplicaties door hackers. Zeker door de toename van nation state hacks is dit een grote bedreiging.
3		Spam en Phishingmails worden in grote hoeveelheid verspreid.
4		Verlies van data. Het naar een verkeerde persoon versturen van mail is de meest voorkomende vorm van een datalek.
5		De oorzaak van veel incidenten komen voort uit het menselijk gedrag.

Er zijn verschillende instituten die jaarlijks overzichten publiceren van de actuele bedreigingen, zoals het National Cyber Security Center (NCSC) en het Europees Agentschap voor netwerk- en informatieveiligheid (ENISA). In het hiernaast opgenomen overzicht staan de bedreigingen waarvoor men momenteel waarschuwt.

2.3 Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2017. De maatregelen worden op basis van best practicus bij (lokale) overheden en NEN-ISO/IEC 27002:2017 genomen.

Voor het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek 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 worden praktische operationele handreikingen uitgebracht, zoals een handleiding voor het uitvoeren van een risicoanalyse voor het opstellen van een beveiligingsplan.

De inhoud en structuur van deze beleidsnota zijn afgestemd op die van de ISO en de BIO. Ook het Informatiebeveiligingsplan zal deze structuur volgen.

2.4 Plaats van het strategisch beleid

Het strategisch beleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau.

Deze nota beschrijft op strategisch niveau het informatiebeveiligingsbeleid. Dit beleid zal worden vertaald in tactische en operationele beleidsplannen, richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijkse Informatiebeveiligingsplan.

2.5 Scope informatiebeveiliging

De scope van dit beleid omvat alle processen, onderliggende informatiesystemen, informatie en gegevens van de GR Ferm Werk (uitvoeringsorganisatie voor de Participatiewet en Sociale Werkvoorziening), Ferm Werk N.V. en verbonden organisaties , het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Dit strategisch Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit specifieke wetgeving af, zoals voor Suwinet. Deze worden in aanvullende documenten geformuleerd.

Er wordt in het strategisch beleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

2.6 Uitgangspunten

Het bestuur en het management[4] spelen een cruciale rol bij het uitvoeren van dit strategische informatiebeveiligingsbeleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor Ferm Werk heeft, de risico's die de organisatie hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Het management wordt hierbij geadviseerd door de CISO

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 management geeft 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 de hele 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 Ferm Werk en deelnemende gemeenten en de relevante landelijke en Europese wet- en regelgeving.

2.6.1 Strategische doelen

De strategische doelen van het 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 cliënten en medewerkers.

2.6.2 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

- Alle informatie en informatiesystemen zijn van belang voor de organisatie, bepaalde informatie is van vitaal en kritiek belang.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het management. Alle informatiebronnen en -systemen die gebruikt worden door de organisatie hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De

[4] In dit beleidsplan wordt in algemene termen de verschillende verantwoordlijkheden weergegeven, in bijlage 1 wordt verder uitgewerkt hoe het management georganiseerd is.

primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie. De verantwoordelijkheden worden belegd door middel van het verwerkingsregister.

- 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.
- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging.
- De organisatie stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
- 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.

2.6.3 Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het dagelijks bestuur van Ferm Werk stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
- Het management stelt jaarlijks het informatiebeveiligingsplan vast.
- Het management is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. Zij worden hierbij ondersteunt door de Chief Information Security Officer(C ISO).
- Het management is verantwoordelijk voor het vragen om informatie omtrent informatieveiligheid bij het lijnmanagement en ziet erop toe dat het lijnmanagement adequate maatregelen heeft genomen voor de bescherming van de informatie die onder diens verantwoordelijkheid valt.
- De 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 controller, voorafgaand aan de Planning & Control (P&C) -gesprekken. Tijdens P&C-gesprekken wordt de informatiebeveiliging besproken op basis van de desbetreffende rapportage van de CISO. De onderwerpen, die als risicovol worden gezien, worden opgenomen in de auditplannen.
- Het management is verantwoordelijk dat elke proces een proceseigenaar heeft die verantwoordelijk is voor de uitvoering van de informatiebeveiliging van de processen
- Medewerkers krijgen afhankelijk van hun functie periodiek trainingen teneinde conform de beveiligingsprocedures te werken uitgewerkt in het Suwinet beveiligingsbeleid en het jaarplan.
- Medewerkers gaan verantwoordelijk om met persoonsgegevens en andere informatie.
- Het management ziet erop toe dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd en stelt vast dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben. Dit vindt plaats door logging en controles op de loggings.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Het management voert quickscans informatiebeveiliging uit op basis van de BIO en maakt op grond daarvan risico-afwegingen.
- Medewerkers krijgen zover mogelijk vanuit een efficiënte bedrijfsvoering alleen toegang tot noodzakelijke gegevens. Het inzien van de gegevens wordt zover mogelijk gelogd en op periodieke basis gemonitord.

2.6.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- De informatiebeveiliging maakt deel uit van afspraken met ketenpartners.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een informatiebeveiligingsplan opgesteld onder leiding van de CISO, gebaseerd op:

1. de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
2. het dreigingsbeeld gemeenten van de Informatiebeveilingsdienst (onderdeel VNG);
3. overleg van CISO's van deelnemende gemeenten.
4. onderwerpen om de informatievoorziening te verbeteren ingebracht door de organisatie en geprioriteerd door het management.

Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats zijn belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence. In dit model is het management verantwoordelijk voor de eigen processen. De tweede lijn (CISO/security officers) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

3.1 Aansturing: management

Het management zorgt dat alle processen en systemen en de daarbij behorende middelen altijd zijn toegewezen aan een verantwoordelijke manager[5]. Het management zorgt dat de managers zich verantwoorden over de beveiliging van de informatie die onder hen berust. Het managementteam zorgt dat het Dagelijks bestuur gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kunnen de besturen zich ook verantwoorden naar de gemeenteraden.

Het management stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. Het management draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO van Ferm Werk. Het management autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de werkorganisatie gezien als een integraal onderdeel van risicomanagement.

3.2 Uitvoering: management

Informatiebeveiliging valt onder de verantwoordelijkheden van alle leidinggevenden. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Lijn-en stafmanagers rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de teams over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging te bespreken in het bedrijfsvoeringsoverleg.

[5] Voor uitwerking managementstructuur zie Bijlage 1

Taken van de lijn- en stafmanagers 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.

3.3 Controle en verantwoording

Dit Strategisch Beleid is een verantwoordelijkheid van het Dagelijks Bestuur van Ferm Werk. Het bestuur en de directie van Ferm Werk zullen volgens de 10 bestuurlijke principes voor informatiebeveiliging (zie Bijlage 2) richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.

Het management is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan verantwoordelijke bestuurders. Het management rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

1.1.1 ENSIA

De deelnemende gemeenten verantwoorden zich over informatiebeveiliging middels de ENSIA-systematiek. Dat betekent dat jaarlijks contact wordt opgenomen met de ENSIA coördinatoren van de deelnemende gemeenten.

In augustus-september worden afspraken gemaakt hoe de benodigde verantwoording over de informatiebeveiliging van Ferm Werk wordt aangeleverd aan de deelnemende gemeenten.

Aldus vastgesteld door het dagelijks bestuur van Ferm Werk op 19 september 2019.

Bijlage 1 Bestuur en Management Ferm Werk

Ferm Werk zit momenteel in een organisch ontwikkelproces wat betreft structuur en organisatie.

Daarom wordt de managementstructuur in deze bijlage beschreven zodat deze makkelijk aangepast kan worden.

Bestuur

Ferm Werk is een gemeenschappelijke regeling van 4 gemeenten. De 4 deelnemende gemeenten: Woerden, Montfoort, Bodegraven-Reeuwijk en Oudewater.

De vier deelnemende gemeenten leveren elk een collegelid voor het Dagelijks Bestuur. Dit Dagelijks Bestuur vormt samen met een raadslid per gemeente het Algemeen Bestuur.

Ferm werk heeft onder de gemeenschappelijke regeling 3 andere organen hangen:

De Ferm Werk NV wordt bestuurd door de algemeen directeur van Ferm Werk en heeft een onafhankelijke raad van commissarissen. Deze raad is het tevens de Raad van Advies voor de Gemeenschappelijke Regeling Ferm Werk.

De stichting de Wissel, is een payrolbedrijf met de algemeen directeur als bestuurder en een raad van commissarissen gelijk aan Dagelijks Bestuur.

Stichting Facilitaire Dienstverlening, waar het meeste stafpersoneel wordt ingehuurd heeft als bestuurders de algemeen directeur en de algemeen manager.

Management

Directie: Algemeen Directeur

Management: Managementteam bestaande uit algemeen directeur en manager Inkomen, manager WP&PD, manager personeelszaken en controller

Lijnmanagers: Team bestaande uit alle managers Lijnmanagement; alle lijn-en stafmanagers waaronder leden managementteam, manager financiën en ICT, teammanagers/-leiders.

Binnen het management team is de controller eerste aanspreekpunt voor Informatieveiligheid en Privacy.

Bedrijfsvoeringsoverleg: manager WP&PD, manager inkomen, manager personeelszaken manager financiën ICT, controller, FG en CISO

Bijlage 2 10 bestuurlijke principes voor informatiebeveiliging.

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.

Ik ben mij bewust van de voorbeeldfunctie van een bestuurder en ik draag uit dat risicomanagement van iedereen is. Ik zorg daarom voor een cultuur waarin iedereen vrij is om dreigingen waar te nemen en te melden. In eerste instantie bij de verantwoordelijke, maar indien nodig ook bij mij als bestuurder. Ik spoor managers aan om voorwaarden te scheppen zodat iedereen binnen de organisatie deelgenoot wordt van het proces van risicomanagement. Ik zorg ervoor dat fouten besproken kunnen worden en dat daarmee een lerende organisatie ontstaat. Ten slotte geef ik in mijn eigen doen en laten het goede voorbeeld van hoe je verantwoordelijk omgaat met informatie..

Toelichting

Zonder open cultuur waar iedereen vrij is om te spreken is het niet goed mogelijk om risico's te identificeren en als de risico's niet bekend zijn, kunt u ze ook niet adresseren. Als u in uw organisatie een cultuur bevordert waarin mensen zich vrij voelen om risico's te melden en maatregelen voor te stellen, dan kunt u adequaat reageren op dreigingen en samenhangende risico's.

2 Informatiebeveiliging is van iedereen

Passende en tijdige betrokkenheid van belanghebbenden maakt het mogelijk dat hun kennis, opvattingen en percepties in aanmerking worden genomen. Dit resulteert in een verbeterd bewustzijn en goed geïnformeerd risicomanagement.

Ik maak medewerkers bewust van de risico's van het werken met informatie en ik maak risicomanagement onderdeel van het MT-overleg en laat het anderen in vergaderingen agenderen. Ik zorg ervoor dat iedereen risicomanagement toepast en dat het gezien wordt als vanzelfsprekend en nuttig. Ik ben transparant naar de raad en zorg ervoor dat hij ook zijn rol kan pakken op dit onderwerp.

Toelichting

Iedereen moet betrokken worden bij risicomanagement, in alle lagen van de organisatie. Maak gebruik van de kennis en verantwoordelijkheid van proces- en systeem eigenaren. Gebruik uw Chief Information Security Officer (CISO), Functionaris Gegevensbescherming (FG) en Controller als onafhankelijke adviseur en laat ze samenwerken in een risicoteam, waar u vanzelfsprekend ook zitting in heeft. Laat uw interne communicatie aandacht besteden aan het verspreiden van de boodschap, het belang en het voordeel van risicomanagement binnen uw organisatie. Goed uitgevoerd risicomanagement creëert waarde voor de organisatie omdat de kwaliteit
van besluiten toeneemt en de kans op falen afneemt.

3 Informatiebeveiliging is risicomanagement

Risicomanagement wordt bewust toegepast bij alle organisatie activiteiten.

Ik zorg ervoor dat risicomanagement integraal onderdeel uitmaakt van uitbestedingen en samenwerkingen. Ik zorg ervoor dat risicomanagement geformaliseerd wordt binnen de hele organisatie met een duidelijke verdeling van verantwoordelijkheden en heldere besluitvorming.

Toelichting

Risicomanagement werkt alleen als het geïntegreerd is in alle werkprocessen van de organisatie. Dat kan alleen bereikt worden als risico's regelmatig op de agenda staan en als risico's een plek/paragraaf krijgen in alle bestuurlijke documenten. Maak lijnmanagers verantwoordelijk voor risicomanagement door afspraken met ze te maken over uw risicobereidheid. Lijnmanagers zijn verantwoordelijk voor de maatregelen en rapportage daarover.

4 Risicomanagement is onderdeel van de besluitvorming

Risicomanagement is onderdeel van alle besluiten.

Ik maak medewerkers mede-eigenaar van het risicoproces op het vlak van informatieveiligheid en ik maak informatiebeveiliging onderwerp van alle overlegstructuren. Ik draag er zorg voor dat besluiten ten aanzien van de omgang met risico's expliciet genomen en vastgelegd worden. Ik laat risicomanagement naadloos aansluiten op de strategische en beleidsmatige doelstellingen van de organisatie. Op deze wijze bied ik een duidelijk kader waarbinnen de medewerkers kunnen opereren.

Toelichting

U kunt als bestuurder alleen de juiste richting aangeven als informatie u bereikt. Door dreigingen en risico's mee te nemen in de vragen die u stelt aan uw managers kunt u er in uw beslissingen ook rekening mee houden Zo kunt u bijsturen voordat risico's manifest worden en escalatie voorkomen.

5 Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking

Het risicomanagementproces is aangepast en staat in verhouding tot de externe en interne context van de organisatie die verband houdt met haar doelstellingen.

Ik zorg dat ik de risico's ken die een gevaar vormen voor de informatievoorziening van de bedrijfsvoering van de gemeente en ik anticipeer op risico's die voortkomen uit het werken in ketens en ik houd rekening met de complexiteit, de onzekerheid en ambiguïteit in de samenwerking met anderen. Bij samenwerken of uitbesteden van (delen) van de organisatie of processen zorg ik ervoor dat de risico's in kaart gebracht zijn, verantwoordelijkheden verdeeld en dat de juiste maatregelen getroffen worden.

Toelichting

Het risicomanagementproces moet passen bij de organisatie en ondersteunen aan de organisatiedoelstellingen. De keten is zo sterk als de zwakste schakel. De gemeente dient met ketenpartners en leveranciers regelmatig het gesprek te voeren over risico's en de maatregelen die ervoor zorgen dat de risico's tot een acceptabelniveau worden teruggebracht.

6 Informatiebeveiliging is een proces

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.

Ik zorg ervoor dat risicomanagement cyclisch is en daarmee kan ik reageren op veranderingen en toekomstgericht sturen. Het staat daarom regelmatig op de agenda.

Toelichting

Risicomanagement moet een cyclisch, iteratief en terugkerend proces zijn, want dreigingen veranderen, doelstellingen veranderen, de omgeving verandert en wetgeving verandert

Indien je in je risicomanagement geen rekening houdt met een veranderde omgeving, dan zijn uw maatregelen op termijn wellicht niet doeltreffend of doelmatig.

7 Informatiebeveiliging kost geld

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

k zorg ervoor dat er voldoende middelen beschikbaar zijn om de onderkende risico's op een adequate manier te behandelen. Als gebleken is dat een risico een bedreiging is voor de organisatiedoelstellingen en er maatregelengenomen moeten worden, dan zorg ik er ook voor dat de middelen beschikbaar zijn om deze maatregelen uit te voeren.

Toelichting

Risico's kunt u ontwijken, mitigeren, overdragen of wegnemen door het nemen van preventieve-, repressieveen/of correctieve maatregelen. Welke strategie u ook kiest, ze kosten allemaal middelen in termen van tijd en ld. Voor maatregelen kan derhalve een kosten-batenanalyse worden gemaakt.

8 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.

Risicomanagement is gebaseerd op de best beschikbare informatie vanuit mijn organisatie en vanuit mijn samenwerkingen. Ik zorg ervoor dat alle belanghebbenden op een gestructureerde en voorspelbare wijze informatie delen die bijdraagt aan risicomanagement.

Toelichting

Zonder goede informatie kunt u geen goede risico-inschattingen en besluiten nemen. Zonder goede en tijdige informatie bent u niet bekend met de risico's die uw organisatie loopt.

9 Verbetering komt voort uit leren en ervaring

Risicobeheer wordt voortdurend verbeterd door leren en ervaring.

Door mijn inzet zorg ik ervoor dat risicogestuurd werken doorontwikkeld wordt. Ik reflecteer op ervaringen en ik nodig medewerkers uit tot het delen van ervaringen met betrekking tot de risico's die de informatievoorziening bedreigen. Ik zorg ervoor dat de organisatie kan leren van incidenten en dat de organisatie leert te ontdekken wat wel en wat niet werkt.

Toelichting

Risicomanagement gedijt het beste in een organisatie die leert van ervaringen en op basis hiervan verbeteringen
doorvoert. Hoe goed u uw informatiehuishouding ook beveiligt, incidenten zullen altijd voorkomen. Door te zoeken naar verbeterpunten en de wil om te leren bouwt u doorlopend aan het verhogen van uw digitale weerbaarheid.

10 Het bestuur controleert en evalueert

Risicomanagement is het controleren en evalueren van resultaten, evenals het nemen van eindverantwoordelijkheid in het doorhakken van lastige knopen.

Ik geef opdracht om de werking van risicomanagement binnen mijn organisatie op effectiviteit en efficiency te (laten) controleren. Naast managementrapportages zijn (externe) controles de manier om te weten te komen of en hoe het beleid in de praktijk uitwerkt. Als bestuurder weeg ik goed geïnformeerd risico's en belangen af en neem ik mijn verantwoordelijkheid om knopen door te hakken.

Toelichting

Controle is belangrijk om goed inzicht te krijgen in de mate waarin het informatiebeveiligingsbeleid en risicomanagement ingebed zijn in de organisatie. Naast verslagen en managementrapportages zijn incidenten, en dan vooral de manier waarop ze afgewikkeld worden, een goede graadmeter om te zien hoe de organisatie omgaat met het onderwerp. Medewerkers kunnen erop vertrouwen dat besluiten op bestuursniveau genomen worden, wanneer de situatie daar om vraagt.