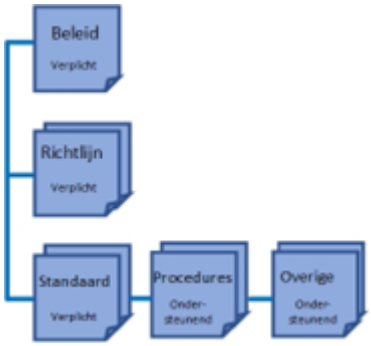
DE FORENSISCHE ZORGSPECIALISTEN

Informatiebeveiliging

Informatiebeveiligingsbeleid

Datum:	29-09-2023
Versie:	1.1
Doelgroep:	Medewerkers
Auteur:	Information Security Officer
Eigenaar:	Raad van Bestuur
Status:	Vastgesteld
Type:	Beleid



DE FORENSISCHE ZORGSPECIALISTEN

Versiebeheer

Versie	Datum	Omschrijving reden nieuwe versie
0.4	25-05-2022	Verwerken opmerkingen en tekstuele wijzigingen
0.9	07-06-2023	Finale controle
1.0	11-07-2023	Definitieve versie
1.1	29-09-2023	Tekstuele wijzigingen n.a.v. interne audit

Verspreiding

Versie	Datum	Verspreiding
0.4	25-05-2022	Strict, De Forensische Zorgspecialisten
0.9	07-06-2023	Strict, De Forensische Zorgspecialisten
1.0	11-07-2023	Strict, De Forensische Zorgspecialisten
1.1	29-09-2023	Strict, De Forensische Zorgspecialisten

Acceptatie

Acceptatie en goedkeuring	Datum
Raad van Bestuur	29-09-2023

Inhoudsopgave

1. Informatiebeveiliging in de forensische zorg

De Forensische Zorgspecialisten (DFZS) is opgericht om mensen met grensoverschrijdend gedrag en mensen die een gevaar voor zichzelf of anderen zijn, te helpen. Het leveren van kwaliteit staat daarbij voorop. Om deze kwaliteit te kunnen bieden is een betrouwbare informatievoorziening essentieel. De betrouwbaarheid van de informatievoorziening moet zijn gewaarborgd ongeacht de vorm, dus zowel handmatig als geautomatiseerd. Denk bijvoorbeeld aan het gebruik van het elektronisch patiëntdossier (EPD), onderzoeksgegevens, internet en e-mail. Uitgebreide aandacht voor de beveiliging van de opslag, verwerking en uitwisseling van informatie is continu vereist. Dit informatiebeveiligingsbeleid geeft daar invulling aan.

De Raad van Bestuur en het management spelen een cruciale rol bij het waarborgen van informatiebeveiliging. DFZS geeft middels dit beleid een duidelijke richting aan informatiebeveiliging en laat zien dat zij zich bewust is van het steeds toenemende belang van informatiebeveiliging. Dit beleid wordt aangevuld met onderwerp specifieke beleidsdocumenten (richtlijnen) voor informatiebeveiliging op tactisch niveau en daar waar gewenst procedures en werkinstructies op operationeel niveau.

Medewerkers hebben een sleutelrol in de zorgvuldige omgang met informatie over cliënten en patiënten. Het is van belang om naast het toepassen van organisatorische en technische maatregelen ook voortdurend aandacht te geven aan bewustwording. Zo zullen bij alle veranderingen in de organisatie, verantwoordelijkheden en informatiesystemen, de consequenties daarvan m.b.t. informatiebeveiliging moeten worden meegewogen.

Dit informatiebeveiligingsbeleid treedt in werking na vaststelling door de Raad van Bestuur van DFZS. Het beleid wordt tenminste eenmaal per jaar beoordeeld en indien nodig herzien. De evaluatie van het beleid wordt ook uitgevoerd als er trends en ontwikkelingen zijn die daar aanleiding toe geven of als er zich een ernstig incident heeft voorgedaan. Aanpassingen van dit beleid worden aangekondigd via publicatie op intranet. De meest actuele versie van het beleid is te vinden op het intranet.

Informatiebeveiliging en privacy zijn termen die vaak door elkaar worden gebruikt. Zij hebben een gemeenschappelijk raakvlak, maar ook een eigen domein. Om die reden is er een apart privacybeleid.

Utrecht, 29-09-2023

I. de Boer,

Raad van Bestuur van De Forensische Zorgspecialisten

2. Algemeen

2.1. Inleiding

DFZS kan niet om informatiebeveiliging heen. De informatievoorziening is van essentieel belang voor de kwaliteit en continuïteit van de bedrijfsvoering. Bij ons dagelijks werk zijn wij afhankelijk van de beschikbaarheid van betrouwbare informatie.

Onze organisatie en onze informatievoorziening worden blootgesteld aan een groot aantal bedreigingen, al dan niet opzettelijk van aard. Deze bedreigingen vereisen gerichte maatregelen, zodat de risico's tot een aanvaardbaar niveau worden gereduceerd. Het proces van informatiebeveiliging begint met het definiëren van beleid op dit vlak. Dit beleid is vastgelegd in dit document.

2.2. Doelstelling van dit beleid

Dit beleid stelt vast hoe DFZS met de beveiliging van informatie omgaat. Daarbij gaat het om zowel de eigen informatie (zoals documentatie, rapportages, presentaties, financiële en personeelsgegevens), als om de informatie van cliënten, patiënten en onderzoeksgegevens.

Tevens faciliteert dit beleid aanknopingspunten om de huidige inrichting te evalueren en aanbevelingen ter verbetering of tot aanpassingen te maken. Het beleid geeft ook richting aan de afspraken waar medewerkers en leveranciers zich aan dienen te houden.

De operationele en tactische aspecten van dit beleid worden verder uitgewerkt en geconcretiseerd in het jaarlijks op te stellen jaarplan informatiebeveiliging en richtlijnen die door DFZS worden vastgesteld.

2.3. Scope van het beleid

Het informatiebeveiligingsbeleid is van toepassing op DFZS, bestaande uit de organisatieonderdelen de Waag en de Van der Hoeven Kliniek. Het beleid ziet op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van DFZS. Het beleid richt zich op eigen medewerkers en behandelaren, tijdelijk personeel en op personeel dat door derden wordt ingezet om diensten te verlenen. Daarnaast geldt het beleid voor ketenpartners, leveranciers en zakelijke relaties van DFZS die te maken hebben met het verwerken van informatie.

Het informatiebeveiligingsbeleid is locatie onafhankelijk. Indien een medewerker, zakelijke relatie, leverancier of derde zich buiten een locatie van DFZS bevindt, maar wel met informatie of informatievoorzieningen van DFZS werkt (denk aan gesprekken in het veld, thuiswerken en/of communicatie via webmail), dient men zich aan dit beleid te conformeren.

Deze informatie bestaat uit verschillende categorieën, namelijk:

- Patiëntinformatie in het kader van leveren van zorg;
- Informatie t.b.v. interne processen en documentatie;
- Personeelsgegevens die worden verwerkt in het kader van het uitvoeren van de taken van de organisatie;
- Onderzoeksgegevens.

De inrichting van beveiligingsmaatregelen wordt afgestemd op de strategie van de organisatie, samen met de prioriteitenbepaling van de huidige en gewenste beveiligingsmaatregelen.

2.4. Doel van informatiebeveiliging

Informatiebeveiliging wordt als volgt gedefinieerd: "het samenhangend stelsel van maatregelen dat zich richt op het blijvend realiseren van een optimaal niveau van

beschikbaarheid, **integriteit** en **vertrouwelijkheid** van informatie en informatiesystemen ter voorkoming en beperking van het optreden van bedreigingen van binnenuit en van buitenaf".

- **Beschikbaarheid:** de informatie moet op de gewenste momenten beschikbaar zijn. Hierdoor hebben medewerkers toegang tot relevante bedrijfsinformatie om hun werk en hun dienstverlening richting de burgers ongestoord voort te zetten.
- **Integriteit**: de informatie moet juist en volledig zijn en de informatiesystemen moeten juiste en volledige informatie opslaan en verwerken. Voor een efficiënte en effectieve dienstverlening is het voor DFZS van belang dat de correcte informatie aanwezig is in de systemen.
- **Vertrouwelijkheid:** de informatie moet alleen toegankelijk zijn voor degene die daartoe bevoegd is. Voor DFZS is het van belang dat vertrouwelijke informatie zoals de persoonsgegevens, medische gegevens, financiële gegevens en/of informatie met strategische waarde niet toegankelijk is voor onbevoegden.
- **Controleerbaarheid**: het moet ook duidelijk zijn wie wat met de informatie heeft gedaan of doet.

Het doel van informatiebeveiliging is om bedreigingen ten aanzien van bovenstaande aspecten te voorkomen en/of te beperken.

De bedreigingen waar de informatie en informatievoorziening van DFZS aan zijn blootgesteld, komen onder andere voort uit:

- Fysieke bedreigingen, zoals brand, waterschade, diefstal etc.
- Logische bedreigingen, zoals verkeerde autorisaties en schadelijke software
- Menselijk falen, zoals onderhouds- en gebruikersfouten
- Technische storingen, zoals storingen van de apparatuur of software
- Communicatieverstoringen, zoals verkeerde adressering of uitval

Vertaald naar DFZS: behalve waarborging van de beschikbaarheid, integriteit en vertrouwelijkheid, is eveneens controleerbaarheid van de (handmatige en geautomatiseerde) gegevens belangrijk. Dit is nodig om cliënten en patiënten verantwoorde zorg te kunnen bieden en om onderzoek op een verantwoorde manier te kunnen uitvoeren.

De verschillende maatregelen, die tezamen de informatiebeveiliging vormgeven, worden niet los van elkaar getroffen, maar in relatie met elkaar. Het stelsel van beveiligingsmaatregelen heeft tot doel een blijvend niveau van beveiliging te realiseren. Door een zorgvuldige borging wordt bereikt dat het gewenste niveau van beveiliging ook op langere termijn gehandhaafd blijft.

Informatiebeveiliging is gericht op het realiseren van een optimaal niveau van beveiliging. De maatregelen die in dit kader worden getroffen, leveren een bijdrage aan de bescherming van privacygevoelige gegevens. Dit optimum wordt bereikt door een zorgvuldige afweging van kosten en baten, rekening houdend met de geldende wet- en regelgeving.

2.5. Kritische succesfactoren

In de dagelijkse gang van zaken zijn maatregelen ter beveiliging van de informatie een noodzaak. Dit is geen eenmalige activiteit, maar een continu proces. Onderstaande kritische succesfactoren dragen ertoe bij dat dit proces succesvol blijft verlopen:

- *Betrokkenheid van het management*

  De implementatie van informatiebeveiliging is geen vakgebied van alleen specialisten. Het management is nadrukkelijk betrokken bij het uitdragen ervan.

- *Borgen in het beleid, de projectaanpak en de bedrijfsvoering*
  Informatiebeveiligingsmaatregelen dragen bij tot het beschermen van informatie en informatiesystemen. Het opnemen van deze regels in het beleid, projecten en bedrijfsvoering werkt succes verhogend.
- *Praktische en toepasbare maatregelen*
  Er dient steeds te worden gestreefd naar praktisch haalbare maatregelen, afgestemd op de specifieke situatie. Deze maatregelen zijn meestal het resultaat van een risicoanalyse als onderdeel van risicomanagement en beoordeelt de geïdentificeerde risico's ten aanzien van de doelstelling van informatiebeveiliging.
- *Informatiebeveiligingsbewustzijn van gebruikers*
  Als gebruikers in hun dagelijks handelen op een bewuste wijze omgaan met (de bescherming van) informatie draagt dit in hoge mate bij aan het niveau van informatiebeveiliging.

3. Strategisch beleid

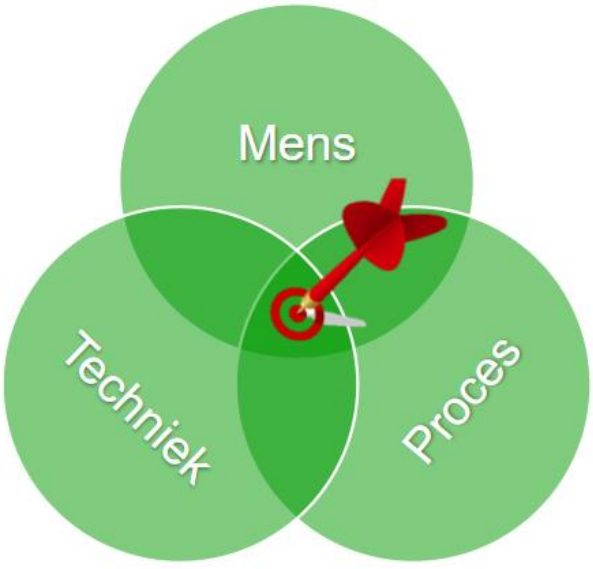
3.1. Beleidskeuzes

DFZS is zich bewust van de risico's ten aanzien van informatieverwerking en kiest ervoor om deze risico's zo goed mogelijk te beheersen.

DFZS kiest ervoor een passend niveau van beveiliging te realiseren in de relatie met cliënten, patiënten en leveranciers, ten aanzien van de betrokken medewerkers, processen en toegepaste techniek.

3.2. Beleidsuitgangspunten

Het creëren van een veilige omgeving is de eerste prioriteit van DFZS. Veiligheid van cliënten en patiënten, en kwaliteit van zorg en onderzoek, worden gediend door informatiebeveiliging en privacybescherming. De aspecten mens, proces en technologie vereisen daarbij alle drie aandacht om informatiebeveiliging adequaat in te richten. In de optimale situatie versterken deze drie aspecten elkaar.



Mens
Medewerkers van DFZS zijn zich bewust van de risico's ten aanzien van beveiliging en het omgaan met (vertrouwelijke) gegevens van cliënten, patiënten en medewerkers.

Medewerkers zijn opgeleid en getraind ten aanzien van informatiebeveiliging zodat ze risico's omtrent informatiebeveiliging herkennen en adequaat kunnen adresseren. Daar waar noodzakelijk zijn de medewerkers gecertificeerd en/of gescreend. Medewerkers van DFZS krijgen uitsluitend toegang tot gegevens waarvoor ze op grond van hun rol toegang toe moeten hebben.

Proces
De processen van DFZS zijn transparant ingericht. Daarbij bestaat met name aandacht voor informatiebeveiliging inzake de beheer-, advies- en detacheringsprocessen, waarbij voor beveiliging gerelateerde incidenten een expliciet escalatietraject is ingericht. In geval van incidenten of calamiteiten kan worden teruggevallen op een actueel business continuïteitsplan.

Techniek
De door en voor DFZS toegepaste technologieën voldoen aan de eisen op het gebied van security. Er wordt gebruik gemaakt van actuele industriestandaard security baselines en de beheerprocessen zijn zodanig dat informatie niet noemenswaardig in gevaar komt. Bij aanschaf en verwerving van oplossingen worden passende beveiligingsmaatregelen in het pakket van eisen opgenomen.

3.3. Belangrijkste uitgangspunten

Alle drie de aspecten komen aan bod in de beleidsuitgangspunten die de organisatie vaststelt:

- De organisatie voldoet aantoonbaar aan de Nederlandse normen NEN 7510 (Informatiebeveiliging in de zorg), NEN 7512 (Vertrouwensbasis voor gegevensuitwisseling) en NEN 7513 (Vastleggen van acties op elektronische patiëntdossiers). Voldoen aan deze normen is een wettelijke verplichting (zie het Besluit Elektronische Gegevensverwerking Zorgaanbieders). Voor NEN 7510 wil de organisatie gecertificeerd zijn om richting andere Nederlandse samenwerkingspartners, zorginstellingen en toezichthouders aan te tonen dat informatiebeveiliging op een adequate manier is ingericht. Jaarlijks wordt hiervoor een verplichte externe audit uitgevoerd.
- De organisatie voldoet aantoonbaar aan de Nederlandse norm NTA 7516 (Eisen voor veilige e-mail en chatapplicaties). Naar verwachting wordt deze norm op korte termijn eveneens wettelijk verplicht gesteld.
- De organisatie voldoet aan de Algemene Verordening Gegevensbescherming (AVG) en andere wet- en regelgeving op het gebied van informatiebeveiliging en privacybescherming.
- De organisatie hanteert een pragmatische benadering van informatiebeveiliging. Daarmee erkent de organisatie dat beveiligingsmaatregelen praktisch en aanpasbaar moeten zijn, en bovendien afgestemd moeten zijn op de doelstellingen en behoeften van de organisatie. De organisatie streeft naar een evenwicht tussen veiligheid en operationele efficiëntie, terwijl de risico's tot een aanvaardbaar niveau worden geminimaliseerd.
- Beveiliging van informatie is een onderdeel van de lijnverantwoordelijkheid. Alle afdelingen van de organisatie hebben hiertoe verantwoordelijkheden voor informatiebeveiliging toegewezen en vastgelegd. Ook toezicht in de vorm van interne audits is belegd.
- Wanneer de organisatie samenwerkingsverbanden aangaat met externe partijen, hetzij inhoudelijk, hetzij voor de ontwikkeling of het beheer van de informatievoorziening, wordt nadrukkelijk aandacht besteed aan informatiebeveiliging in de vorm van schriftelijke afspraken en controle op naleving daarvan.
- De binnen de organisatie aanwezige informatie wordt op een gestructureerde methode geclassificeerd naar de aspecten beschikbaarheid, integriteit en vertrouwelijkheid. De informatie-eigenaar is hiervoor verantwoordelijk. Op basis van de classificatie worden passende beveiligingsmaatregelen getroffen.

- Bij de aanname, tijdens het dienstverband en in geval van ontslag van medewerkers, zowel vast als tijdelijk, wordt nadrukkelijk aandacht besteed aan de integriteit van medewerkers en aan de waarborging van de vertrouwelijkheid van informatie. Dit is een verantwoordelijkheid van de Afdeling HR.
- De organisatie voert een actief beleid om het beveiligingsbewustzijn van management en medewerkers te stimuleren. Dit is een verantwoordelijkheid van de Manager I&A en Communicatie en Marketing.
- Er zijn voorschriften (zoals een personeelsreglement en een gedragscode) voor het gebruik van (algemene) informatievoorzieningen. Er is toezicht op naleving hiervan, waarbij zo nodig de Functionaris Gegevensbescherming en interne auditors ondersteuning bieden.
- In de organisatie zijn maatregelen getroffen voor de fysieke beveiliging van mensen en middelen, waaronder vertrouwelijke informatie en apparatuur waarop deze informatie is opgeslagen.
- De organisatie treft maatregelen ter waarborging dat alleen daartoe geautoriseerde gebruikers toegang krijgen tot de informatie- en communicatievoorzieningen.
- Bij de aanschaf van informatiesystemen wordt in alle fasen van het proces nadrukkelijk aandacht besteed aan informatiebeveiliging. De afdeling die zo'n initiatief onderneemt is hiervoor verantwoordelijk.
- De organisatie treft adequate maatregelen om de correcte werking van de bedrijfsprocessen en de hierbij gebruikte informatie(systemen) te borgen, zowel onder gewone als onder buitengewone omstandigheden.
- De organisatie beschikt over middelen voor het melden, opvolgen en afhandelen van incidenten waarbij informatiebeveiliging en/of privacybescherming in het geding is. De evaluatie van de afhandeling van zulke incidenten wordt benut voor de verbetering van maatregelen met betrekking tot informatiebeveiliging en privacybescherming.

Deze uitgangspunten voor informatiebeveiliging worden verder geconcretiseerd in onder meer richtlijnen, procesbeschrijvingen, procedures en standaards.

3.4. De 10 principes voor informatiebeveiliging

De 10 principes voor informatiebeveiliging gaan over de waarden die de organisatie zichzelf oplegt. De principes zijn als volgt:

1. De Raad van Bestuur bevordert een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is gebaseerd op risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in 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. De Raad van Bestuur controleert en evalueert.

De bovenstaande principes gaan met name over de rol van de Raad van Bestuur bij het borgen van informatiebeveiliging binnen DFZS. De principes ondersteunen de Raad van Bestuur bij het inrichten en uitvoeren van goed risicomanagement. Immers als er iets verkeerd gaat met betrekking tot het beveiligen van informatie binnen de processen van DFZS, kan dit directe gevolgen hebben voor onder andere patiënten, cliënten, medewerkers, relaties en bezoekers van DFZS.

3.5. Informatiebeveiligingsdoelstelling

Om de veiligheid en het welzijn van onze patiënten in de forensische geestelijke gezondheidszorg te beschermen, wil DFZS aantoonbaar voldoen aan de NEN 7510 norm en hiervoor gecertificeerd worden.

Onze toewijding aan het voldoen aan de NEN 7510 dient als een pijler in onze strategie, waarbij we de hoogste normen op het gebied van patiëntenzorg en informatiebeveiliging garanderen. Onze focus ligt op het aanbieden van behandelingen voor mensen met strafbaar gedrag en mensen die een gevaar voor zichzelf of anderen zijn, en dit alles met inachtneming van strenge veiligheids- en gegevensbeveiligingsmaatregelen om de waardigheid, rechten en privacy van onze patiënten te beschermen.

Het stellen van de naleving van de NEN 7510 als informatiebeveiligingsdoelstelling betekent dat DFZS zich inzet voor het implementeren van de noodzakelijke beveiligingsmaatregelen en controles om aan de eisen van de norm te voldoen. Dit bevat:

1. Beleid en procedures: Ontwikkelen en implementeren van informatiebeveiligingsbeleid, -procedures en -richtlijnen in lijn met NEN 7510.
2. Toegangscontrole: Beperking van de toegang tot patiëntgegevens tot geautoriseerd personeel via toegangscontrolemechanismen.
3. Risicomanagement: Het identificeren en beheersen van beveiligingsrisico's voor patiëntinformatie volgens de NEN 7510 richtlijnen.
4. Training en bewustzijn: ervoor zorgen dat personeelsleden getraind zijn en zich bewust zijn van hun rol bij het handhaven van de beveiliging volgens de norm.
5. Incidentrespons: Vaststellen van procedures voor het detecteren, rapporteren en reageren op beveiligingsincidenten, zoals beschreven in NEN 7510.
6. Documentatie en registratie: het bijhouden van de juiste documentatie en registratie van beveiligingsgerelateerde activiteiten, zoals vereist door de standaard.
7. Regelmatige audits en beoordelingen: Het uitvoeren van regelmatige audits en beoordelingen om de naleving van NEN 7510 te beoordelen en verbeterpunten te identificeren.
8. Continue verbetering: Het voortdurend verbeteren van beveiligingsmaatregelen om zich aan te passen aan veranderende bedreigingen en kwetsbaarheden.

De Raad van Bestuur steunt deze doelstelling door:

- dit beleid op advies van de Information Security Officer te herijken;
- het borgen dat informatiebeveiligingseisen zijn geïntegreerd in de bedrijfsprocessen;
- het beschikbaar stellen van de benodigde middelen;
- met regelmaat het belang van informatiebeveiliging onder de aandacht te brengen in de organisatie;
- toe te zien op realisatie van de doelstelling op basis van rapportages en auditresultaten (intern en extern) die door onder andere de auditor, de Information Security Officer en de Functionaris Gegevensbescherming worden aangeleverd.

4. Rollen en verantwoordelijkheden

4.1. Uitgangspunten

Informatiebeveiliging is primair een verantwoordelijkheid van het lijnmanagement. Medewerkers in verschillende rollen ondersteunen het management daarbij.

Met betrekking tot het toekennen van taken en bevoegdheden bij informatiebeveiliging gaat de organisatie uit van de volgende taak- en functiescheiding:

- scheiden van beleidsvoorbereiding (planning en normering c.q. regelgeving) en uitvoering (inclusief dagelijks monitoren) van maatregelen.
- kader stellende functies scheiden van ontwerpfuncties binnen de architectuur.

- beslissen over maatregelen scheiden van advies, toezicht of controle van die maatregelen.
- het primair adviseren en houden van toezicht scheiden van primair controleren.
- functionele taken scheiden van technische taken.

Deze uitgangspunten leiden tot de volgende indeling op strategisch, tactisch en operationeel niveau.

Strategisch
Op strategisch niveau worden de kaders vastgesteld met betrekking tot informatiebeveiliging. De Raad van Bestuur is eindverantwoordelijk voor de beleidsvorming en heeft de voorbereiding hiervan belegd bij de Information Security Officer. De centrale kaders worden vastgelegd in het informatiebeveiligingsbeleid en nader uitgewerkt in richtlijnen, procedures, standaarden en dergelijke die op het intranet worden gepubliceerd. Op basis van een integrale risicoanalyse wordt een jaarplan en een meerjarenplan voor informatiebeveiliging vastgesteld.

Tactisch
De planning van specifieke activiteiten met betrekking tot informatiebeveiliging vormt het tactische niveau. Van de management teams van de Waag, de Kliniek en de Ondersteunende Diensten wordt verwacht dat een verbeterplan wordt opgesteld op basis van de centrale kaders en een meer specifieke risicoanalyse.

Operationeel
De uitvoering van activiteiten met betrekking tot informatiebeveiliging vindt plaats op operationeel niveau. Eerstverantwoordelijke voor deze activiteit is het lijnmanagement. Ten behoeve van het structureren van de uitvoering van taken met betrekking tot informatiebeveiliging zijn procedures opgesteld.

Toezicht op de naleving van het informatiebeveiligingsbeleid en van geldende wet- en regelgeving vindt plaats op verschillende niveaus:

- interne auditoren – deze auditoren voeren periodiek controles uit op de naleving van processen en procedures op het gebied van kwaliteit en veiligheid.
- externe accountant – jaarlijks legt de organisatie met betrekking tot een aantal thema's verantwoording af aan de externe accountant. Een van de thema's betreft de implementatie van het informatiebeveiligingsbeleid;
- externe auditor – jaarlijks dient een onafhankelijke externe auditor na te gaan hoe goed de organisatie voldoet aan de informatiebeveiligingsnorm NEN 7510;
- security audits & ethische hacks – jaarlijks of bij grote veranderingen in de ICT-omgeving dient een security audit uitgevoerd te worden op (onderdelen van) de technische omgeving van de organisatie.

DFZS heeft een Information Security Officer, Technical Security Officer en Functionaris Gegevensbescherming die toezien op het voldoen aan wet- en regelgeving, en die zich bezighouden met kwesties rondom integriteit en misstanden rondom de naleving van wet- en regelgeving.

4.2. Specifieke rollen en functies voor informatiebeveiliging

De Richtlijn "Informatiebeveiliging Rollen en Verantwoordelijkheden" geeft een overzicht van de functies of rollen die nodig zijn om informatiebeveiliging te bevorderen in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.

4.3. Overlegvormen voor informatiebeveiliging

Voor overleg, coördinatie en afstemming op het gebied van informatiebeveiliging worden de volgende overlegvormen onderscheiden:

- Managementteam IB (driemaandelijks)
- ICT en Functioneel beheeroverleg (maandelijks)
- Systeembeheeroverleg (wekelijks) bestaande uit systeembeheerders + Manager I&A + Technical Security Officer
- Werkgroep Informatiebeveiliging (IBMF) bestaande uit Raad van Bestuur + Information Security Officer + Technical Security Officer + Functionaris Gegevensbescherming + Manager I&A (maandelijks en ad hoc)
- Overleg tussen Technical Security Officer en Functionaris Gegevensbescherming (wekelijks)
- Incidenteel management, Manager I&A en MT (ad hoc)

4.4. Controle en verantwoording

Dit informatiebeveiligingsbeleid is een verantwoordelijkheid van de Raad van Bestuur van DFZS. De Raad van Bestuur zal op basis van de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging. De Information Security Officer is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan de Raad van Bestuur, en rapporteert daarnaast over de mate waarin invulling is gegeven aan het uitwerken van tactische beleidsonderwerpen die aanvullend zijn op dit strategische beleid.