# INFORMATIEVEILIGHEID & PRIVACY

En hoe Amstelring hiermee omgaat

Definitieve versie, oktober 2019

Auteurs: Leden stuurgroep informatieveiligheid

Vastgesteld door: Raad van Bestuur Amstelring op 14 oktober 2019

# Inleiding

De visie van Amstelring is: samen zorg dragen voor kwaliteit van leven, op basis van gelijkwaardigheid en met respect voor ieders rol. De kaders waarbinnen wij werken zijn: goede zorg, leuk werk en een financieel gezond beleid. Hiervan afgeleid is de koers voor de inzet van digitale middelen:

- Iedere medewerker van Amstelring is digitaal vaardig en wordt ondersteund door technische middelen die op elkaar zijn afgestemd. Deze zijn 24/7 beschikbaar, snel en begrijpelijk.
- De medewerker wordt dicht bij de cliënt ondersteund met digitale middelen.
- Het gebruik van digitale middelen heeft geen handleidingen nodig.
- Printen, faxen en scannen is niet nodig.
- De informatie in de systemen is betrouwbaar en beschikbaar voor wie en wanneer dat nodig is.

Ons **privacystatement**: Privacy vinden wij heel belangrijk. Zorgvuldig omgaan met persoonsgegevens is bij Amstelring onderdeel van goede zorg en goed werkgeverschap. Medewerkers van Amstelring zijn zich bewust van en handelen naar de actuele wetgeving rondom privacy. Jij gaat vertrouwelijk om met persoonsgegevens en krijgt alleen toegang tot data die nodig is voor je werk.

Informatiebeveiliging gaat om de zaken die Amstelring geregeld heeft zodat de medewerkers doorlopend betrouwbare informatie krijgen voor hun werkzaamheden en dat deze informatie wordt beschermd tegen onbedoeld verlies of misbruik. Privacy gaat specifiek over het beschermen van persoonsgegevens (van medewerkers en cliënten) zodat geen misbruik kan worden gemaakt van deze gegevens.

Dit organiseren we door middel van technische maatregelen, autorisaties en toegang en afspraken met onze leveranciers, controles door applicatiebeheer en controles die de medewerkers zelf doen in de werkprocessen (gebruikerscontroles). Amstelring volgt de NEN-normeringen en specifiek de NEN7510.

Het begint altijd met ons eigen gedrag. Hier kan je lezen wat de afspraken zijn waar we ons aan houden en wat te doen wanneer het toch een keer mis gaat.

# 1. Verantwoordelijkheden informatieveiligheid & privacy

We zijn allemaal verantwoordelijk voor informatieveiligheid & privacy. We willen continu verbeteren, ook op dit vlak. Dit betekent dat elk incident ook een leermoment is. Aangebrachte verbeteringen zijn input voor een goede en doorlopende verbetercyclus: plan, do, check, act.

Hier een overzicht van wie waarvoor verantwoordelijk is om informatieveiligheid te kunnen waarborgen.

Iedereen werkzaam bij Amstelring is verantwoordelijk voor het veilig omgaan met informatie en het bewaken van de persoonsgegevens waar hij/zij mee te maken heeft. Dit betekent dat iedereen werkzaam bij Amstelring zelf verantwoordelijk is om te handelen naar de afspraken die in dit document staan. In dit document gebruiken we de term 'medewerker', hieronder wordt ook verstaan de vrijwilliger, lid cliëntenraad, lid Raad van Toezicht, uitzendkracht/externe of stagiaire.

## Hieronder staan meer gespecialiseerde functies:

*Applicatiebeheerder*
De applicatiebeheerders zijn verantwoordelijk om de autorisatie en toegang van de applicaties waar hij /zij verantwoordelijk voor is, zo in te richten dat voldaan wordt aan de afspraken in dit document.

*Functionaris Gegevensbescherming (FG)*
Verantwoordelijk voor het toezicht op de inrichting van de processen rondom privacy. Daarnaast heeft de FG een adviserende en toezichthoudende functie voor privacy-gerelateerde onderwerpen. Ook heeft Amstelring een Privacy Officer. De Privacy Officer adviseert gevraagd en ongevraagd over onderwerpen rondom de privacy en coördineert de melding van datalekken.

*Stuurgroep Informatieveiligheid*
Opstellen, evalueren en bijstellen van de afspraken rondom informatieveiligheid en verantwoordelijk voor risico-afwegingen op dit vlak.

*Raad van Bestuur*
De Raad van Bestuur is verantwoordelijk voor het vaststellen van het beleid en neemt deel aan de stuurgroep informatieveiligheid.

Binnen de organisatie zijn er verantwoordelijkheden voor de technische maatregelen (IT-manager), organisatorische verantwoordelijkheden (RVE-managers en manager ISA) en specifieke verantwoordelijkheden.

# 2. Privacybeleid

## Privacyverklaring

De (externe) privacyverklaring die gepubliceerd is op www.amstelring.nl is onderdeel van het Privacybeleid.

Het Amstelring Privacybeleid is bestemd voor alle personen werkzaam binnen de Stichting Amstelring en is van toepassing op alle persoonsgegevens die binnen Amstelring worden verwerkt. Het beleid beschrijft de maatregelen op het gebied van privacybescherming.

Het Privacybeleid ondersteunt het principe van 'Privacy-by-design': al in de beginfase(s) van een project en bij het ontwikkelen van producten of diensten wordt rekening gehouden met de bescherming van persoonsgegevens.

De uitgangspunten in dit beleid zijn gebaseerd op wettelijke vereisten: de Algemene Verordening Gegevensbescherming (AVG), een Europese verordening voor bescherming van persoonsgegevens en andere specifieke nationale wet- en regelgeving.

De basis van het privacybeleid van Amstelring kenmerkt zich door het vastleggen van: zo min mogelijk gegevens, het doel van de vastlegging en de betrokkenen weten hiervan.

## Hier wordt dit nog verder uitgelegd:

**Dataminimalisatie**
De wet zegt dat persoonsgegevens - gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt - 'toereikend, terzake dienend en niet bovenmatig moeten zijn'. Dit betekent dat Amstelring bij het uitoefenen van haar werkzaamheden zo weinig mogelijk persoonsgegevens moet gebruiken. Daardoor is bij een eventueel datalek het risico voor betrokkenen kleiner, omdat er minder gegevens zijn die verloren kunnen gaan.

**Doelbinding**
Voor iedere verwerking van persoonsgegevens moet vooraf duidelijk worden vastgesteld waarvoor de persoonsgegevens worden gebruikt. Dit bepaalt welke persoonsgegevens Amstelring mag verwerken, hoe lang Amstelring gegevens mag gebruiken en waarvoor Amstelring de gegevens in de toekomst mag gebruiken.

**Informeren**
Betrokkenen moeten altijd goed en duidelijk worden geïnformeerd over de verwerking. Zij moeten weten wat voor persoonsgegevens worden verwerkt, door wie en wat er met de gegevens gebeurt. Zo houdt de betrokkene controle over de eigen persoonsgegevens.

## De privacy-afspraken

Het privacybeleid van Amstelring staat op de website van Amstelring. Amstelring verwacht dat iedereen werkzaam bij Amstelring op de hoogte is van de regels en wetgeving rondom privacy.

Je aan de spelregels houden betekent dat je je aan de volgende privacy-afspraken houdt:

1. Je deelt alleen persoonsgegevens met andere partijen wanneer dit nodig is voor de uitvoering van jouw dienstverlening of wanneer dit verplicht is vanwege (andere) wetgeving. Je zult nooit persoonsgegevens verkopen aan derden.

   *Alle medewerkers van Amstelring zijn wat betreft cliëntgegevens ook gebonden aan het (medisch) beroepsgeheim.*

2. Je deelt alleen persoonsgegevens met collega's wanneer dit nodig is voor de dienstverlening aan jouw cliënten. Alleen wanneer het nodig is voor de behandeling zullen medische gegevens gedeeld worden tussen medewerkers betrokken bij deze behandeling, en dan altijd zo min mogelijk gegevens en altijd per beveiligde e-mail naar individuen en niet naar groepsmailboxen of distributielijsten. Dit betekent dat je alleen in dossiers kijkt waar je vanuit je functie bij moet. Mocht je meer toegang hebben, dan wordt er van je verwacht dat je alleen in de dossiers kijkt waar je vanuit je functie bij moet. Tevens wordt van je verwacht dat wanneer je teveel ziet, je dit meldt bij applicatiebeheer en informatieveiligheid@amstelring.nl.

   *Er mag niet gekeken worden in een dossier van bijvoorbeeld de moeder van je buurvrouw die zorg of behandeling ontvangt van Amstelring waar jij niet bij betrokken bent.*

3. Amstelring stelt vooraf de doeleinden en grondslag voor de verwerking van persoonsgegevens vast, in lijn met de AVG. Je gebruikt persoonsgegevens niet voor andere doeleinden of grondslagen.

   *Medewerkers mogen een mailadres dat verzameld is om uitnodigingen voor een informatieavond te versturen niet gebruiken om bijvoorbeeld reclame te versturen.*

4. Je voldoet aan de juiste voorwaarden bij het gebruik van de grondslag ‘toestemming’.

   *Alle cliënten vullen een duidelijke toestemmingsverklaring in voordat foto’s van hen worden gepubliceerd. Ze kunnen hun toestemming altijd intrekken.*

5. Bij verwerking van alle persoonsgegevens volg je de instructies om te voldoen aan organisatorische en technische eisen. Alle systemen hebben goede toegangsautorisaties, Amstelring controleert deze regelmatig.

*Je gebruikt je telefoon (privé of van Amstelring) om op een tweede manier (naast inlognaam en wachtwoord) de applicatie te laten weten dat jij het bent.*

6. Als jij of je team besluit om nieuwe IT systemen of processen te implementeren, bestaande systemen of processen aan te passen (of te beëindigen), moeten de **privacy, beveiliging en IT risico's** eerst in kaart worden gebracht en eventueel risicoverlagende maatregelen getroffen moeten worden alvorens de wijzigingen gemaakt mogen worden. Wil je meer weten over wat je dan moet doen, klik dan hier.

   *Je wilt Sillo gebruiken om cliëntgegevens te delen met de specialist van het ziekenhuis en je wilt de app downloaden. Alvorens dit te doen start je een onderzoek naar de risico's (RIA) of neem je contact met het ISA.*

## De volgende afspraken zijn algemeen voor Amstelring - laag 3

7. Bij beleidsonderwerpen die van invloed zijn op de privacy van persoonsgegevens van medewerkers en/of cliënten vraag je eerst instemming aan de Ondernemingsraad (OR) en/of Cliëntenraad van Amstelring. Ook leg je dit voor aan de privacy officer en functionaris gegevensbescherming.

   *Wanneer er bij een locatie camera's worden ingezet in bijvoorbeeld de gangen en de huiskamer, dan moet dat in overleg met cliëntenraad en de medewerkers moeten geïnformeerd worden.*

8. Amstelring stelt voor alle persoonsgegevens die gebruikt worden bewaartermijnen vast en bewaart persoonsgegevens niet langer dan nodig. Amstelring neemt hierbij alle relevante wet- en regelgeving in acht.

   *Medisch dossiers worden 15 jaar bewaard, en financiële gegevens 7 jaar. Dit vanwege wettelijke verplichtingen. Als gegevens niet bewaard hoeven te worden, worden ze weggegooid.*

9. Amstelring communiceert begrijpelijk en transparant over het gebruik van persoonsgegevens en informeert betrokkenen over hun rechten bij het gebruik van hun gegevens.

   *Op de website van Amstelring is een duidelijke privacyverklaring in te zien.*

10. Waar Amstelring samenwerkt met andere partijen neemt Amstelring passende maatregelen om beveiliging en privacy bij deze partijen te waarborgen en legt deze vast in verwerkersovereenkomsten.

    *Amstelring tekent met alle leveranciers een verwerkersovereenkomst en controleert of deze voldoet aan de eisen van Amstelring. Met leveranciers, die niet aan deze eisen voldoen, zal niet mee worden samengewerkt.*

11. Amstelring verwacht van andere partijen dat zij minimaal hetzelfde privacyniveau handhaven als Amstelring.

    *Amstelring controleert in verwerkersovereenkomsten of partijen hetzelfde privacy- en beveiligingsniveau hanteren. Amstelring werkt niet samen met partijen die dat niet kunnen garanderen.*

## Grondslagen uit de AVG

Amstelring verwerkt alleen persoonsgegevens als er een geldige wettelijke grondslag voor bestaat. De grondslagen uit de AVG en die gebruikt worden bij Amstelring zijn:

- **Contract**: de meeste zorg bij Amstelring wordt geleverd op grond van een Zorgleveringsovereenkomst.
- **Toestemming**: Amstelring maakt, indien nodig, gebruik van geldige toestemming, die transparant wordt omschreven, die actief en ondubbelzinnig gegeven moet worden en welke altijd ingetrokken kan worden. Amstelring gebruikt dit bijvoorbeeld bij gebruik van beeldmateriaal.
- **Gerechtvaardigd belang**: in geval van een gerechtvaardigd belang maakt Amstelring een goede, zorgvuldig gedocumenteerde afweging tussen het eigen belang en de inbreuk op de privacy. Dit gebeurt bijvoorbeeld bij cameratoezicht.
- **Wettelijke plicht**: wanneer er een wettelijke plicht bestaat om gegevens te verwerken, zoals de wettelijke bewaartermijn voor medisch dossiers, dan zal Amstelring daaraan voldoen.
- **Vitaal belang**: in geval van een leven-of-dood situatie mag een arts van Amstelring altijd de persoonsgegevens van een betrokkene verwerken om hem/haar te helpen.
- **Algemeen belang**: Amstelring zal weinig gebruik maken van deze rechtsgrond.

## Inbreuk persoonsgegevens (datalek)

Een inbreuk in verband met persoonsgegevens, beter bekend als een datalek, is een incident dat leidt tot vernietiging, verlies, wijziging, ongeoorloofde verstrekking van of ongeoorloofde toegang tot verwerkte persoonsgegevens, of wanneer niet uitgesloten kan worden dat dit is gebeurd.

Een ‘hack’ van systemen, waarbij persoonsgegevens worden buitgemaakt, is typisch een voorbeeld van een datalek met kwade opzet.

Er is echter niet altijd sprake van kwade opzet. Een datalek kan per ongeluk optreden, zoals het verliezen van een medisch dossier van een cliënt. Ook wanneer dat dossier later wordt teruggevonden is niet uit te sluiten dat onbevoegden het hebben ingezien. Amstelring wil leren van datalekken en zal steeds zoeken naar manieren om het geleerde te bespreken en continu te verbeteren.

Datalekken moeten altijd gemeld worden. Meer informatie: Amstelring Datalek Protocol.

## Bescherming van privacy van medewerkers

Amstelring beschermt de privacy van de eigen medewerkers goed. Amstelring zal nooit persoonsgegevens van medewerkers delen met andere partijen, tenzij de medewerker daar toestemming voor heeft gegeven, of als er een wettelijke plicht voor bestaat. Amstelring zal nooit zomaar gegevens van de medewerkers delen met derden.

Als mantelzorgers/familie van cliënten gebruik maken van woonzorgtechnologie, zelf geïnstalleerd cameratoezicht, of andere middelen voor toezicht op het familielid bij Amstelring, dan dient dit doorgegeven te worden aan Amstelring. De familie dient er akkoord mee te dat de verzamelde gegevens uit dit soort technologie enkel gebruikt zullen worden voor de veiligheid van het eigen familielid en dat er geen toezicht gehouden mag worden op het gedrag of functioneren van de medewerkers van Amstelring.

Enkel in geval van ernstige calamiteiten mogen deze gegevens gebruikt worden. In dat geval mogen ze overgedragen worden aan politie/justitie.

## Cameratoezicht

Amstelring maakt in en rondom haar locaties gebruik van cameratoezicht en doet dat door gebruik te maken van de grondslag ‘gerechtvaardigd belang’. Cameratoezicht op openbare ruimtes wordt gebruikt om de veiligheid van betreffende ruimtes te waarborgen. Camera’s zijn op zo’n manier opgesteld dat zij alleen relevante gebieden voor bescherming van die veiligheid filmen.

Camera’s op afdelingen of kamers worden beschouwd als vrijheidsbeperkende maatregelen en zullen altijd in overeenstemming met de Wet Zorg & Dwang worden geïnstalleerd en geëvalueerd. Daar waar gebruik wordt gemaakt van cameratoezicht wordt men geïnformeerd door middel van zichtbare waarschuwingen (bijvoorbeeld een sticker).

Amstelring maakt, tenzij hiervoor zeer zwaarwegende redenen zijn, nooit gebruik van cameratoezicht zonder dat dit bekend is bij de medewerkers of de cliënt (ook wel genoemd heimelijk cameratoezicht). Heimelijk cameratoezicht is alleen kortdurend toegestaan, en de Raad van Bestuur dient hiervoor een akkoord te geven. Na afloop van heimelijk cameratoezicht zullen alle gefilmde medewerkers en de OR geïnformeerd worden over het cameragebruik.

Het cameratoezicht aangebracht door familie of cliënten zelf, moet uitgeschakeld worden als een medewerker van Amstelring bezwaar heeft tegen het cameratoezicht. Dit moet dus altijd in overleg, zie ook Algemene Voorwaarden Actiz en BTN 2018 algemene module pagina 4 punt 5 onder het kopje ‘Welke verplichtingen heeft u’?.

# 3. Gedragsregels ICT

De gedragsregels voor het gebruik van ICT-middelen, internet- en e-mailgebruik van Amstelring zijn aanvullend op de algemene gedragsrichtlijn voor medewerkers en vrijwilligers. De Gedragsregels ICT zijn:

- Het is niet toegestaan om ICT-voorzieningen voor onacceptabele persoonlijke doeleinden te gebruiken. Bij onacceptabel persoonlijk gebruik van internet moet onder andere worden gedacht aan: het bezoeken van sites of versturen van berichten die pornografisch, racistisch, discriminerend, dreigend, beledigend of anderszins aanstootgevend materiaal bevatten.
- Het is niet toegestaan om persoonlijke (beeld)informatie van en over cliënten, bezoekers of collega's te plaatsen op social media (Facebook, Linkedin, Twitter, Instagram, Snapchat, etc.) tenzij hiervoor schriftelijk toestemming is gegeven door betreffende perso(o)n(en).
- Beveiligingsincidenten, zoals verdachte of aanstootgevende e-mail moeten gemeld worden aan het ISA. Let ook op phishing-mails (mail die mensen naar een valse websites lokt).
- Het scherm van de computer wordt door de medewerker altijd vergrendeld als de medewerker wegloopt van de computer. Bij een Chromebook volstaat het om de Chromebook dicht te klappen.
- Na het printen van cliënteninformatie, wordt het papier altijd vernietigd. Na het scannen van documenten haalt de medewerker het document uit de scanner en vernietigt het na gebruik. Print alleen indien strikt noodzakelijk.
- Alle gegevens binnen het bedrijfsnetwerk en Google-omgeving zijn van Amstelring.
- Het is niet toegestaan om cliënt-, medewerkers- of bedrijfsinformatie te versturen naar of vanuit je eigen privé e-mailadres.
- Binnen Amstelring zijn ONS, AFAS en Ysis de systemen voor persoons- en medische gegevens en deze gegevens hoeven niet meer intern gemaild te worden. Mocht er toch noodzaak zijn tot mailen van persoonsgegevens, dan is het niet toegestaan om dit naar groepsmailboxen of distributielijsten (mailgroepen) te mailen (maar alleen naar individuele e-mailadressen van personen).

Verder is de gedragsrichtlijn medewerkers en vrijwilligers van kracht. Hierin staan ook enkele zaken opgenomen die te maken hebben met privacy.

# 4. Toegang tot systemen

## Autorisaties en toegang

*Autorisatie* gaat over wat iemand mag, en welke informatie iemand mag zien binnen een systeem. *Toegang* gaat over voor welke teams/locaties/medewerkers een autorisatie geldt. Voor iedere applicatie wordt een 'autorisatiematrix' opgesteld door de proceseigenaar en de

applicatiebeheerder. Indien wordt afgeweken van de uitgangspunten, documenteren we waarom en leggen we de afwijking voor aan de Raad van Bestuur (bijvoorbeeld 'niet mogelijk in de applicatie' of 'wens proceseigenaar'). Door deze werkwijze:

- kunnen autorisatie vraagstukken worden opgelost;
- is het mogelijk om medewerkers eenduidig te autoriseren;
- is de informatiebeveiliging van Amstelring -voor dit onderwerp- aantoonbaar;
- borgen we de kwaliteit van gegevens.

## Bij het opstellen van de uitgangspunten voor autorisatie en toegang hanteren we het onderstaande beleid:

- **Betrouwbare informatie** is alleen te verkrijgen door medewerkers die goed getraind zijn in de functionaliteiten van de applicaties, zodat ze deze goed en veilig gebruiken.
- **Alle informatie nodig om het werk te kunnen doen:** medewerkers moeten toegang hebben tot alle informatie die ze nodig hebben om hun werkzaamheden te kunnen verrichten, ook als die informatie slechts incidenteel nodig is, bijvoorbeeld in noodsituaties.
- **Functiescheiding:** stappen in een proces worden - daar waar het privacy-risico's kent - opgesplitst tussen medewerkers/functiegroepen/systemen.
- **Ontzorg de zorgmedewerkers** door te registreren bij de bron en te faciliteren met slimme ICT. Hierbij ligt de verantwoordelijkheid bij de medewerker, ondersteunt door het Integraal Servicepunt Amstelring (ISA).
- Waar **controles** onvoldoende de risico's afdekken wordt dit aangevuld met signaallijsten (datagedreven controle) of andere aanvullende maatregelen. De controles worden opgenomen in de AO/IC.

## Wie krijgt welke rechten?

- **Admin** rechten in een applicatie zijn altijd voorbehouden aan een beperkt aantal, zeer deskundige medewerkers: de applicatiebeheerders. Admin rechten gaan hoger dan wijzigingen op individueel cliënt/medewerker niveau, zoals bijvoorbeeld: wijzigingen in master data[1] in opdracht van bijvoorbeeld bedrijfsinformatie of zorginkoop, autorisaties aanpassen binnen de kaders van de opgestelde autorisatiematrices, configureren, koppelingen aanpassen, etc.
- De **functioneel applicatiebeheerder** en/of **ISA-adviseur** mag gegevens wijzigen in opdracht van de verantwoordelijke medewerker. Indien de applicatiebeheerder inschat dat er grote consequenties zijn, wordt er afgestemd met de relevante verantwoordelijke. De afhandeling hiervan wordt gelogd en steekproefsgewijs gecontroleerd. De ISA-specialist heeft in de applicatie van haar expertise extra bevoegdheden om te zorgen dat mensen die het ISA bellen zo snel mogelijk geholpen kunnen worden.
- **Ondersteuners** (bijvoorbeeld **ISA-medewerkers**) hebben leesrechten en soms

[1] Master data: kostenplaatsen, nieuwe producten, afdelingen, etc.

schrijfrechten in systemen, waarbij steeds gekeken wordt of de betrouwbaarheid van de gegevens gewaarborgd blijft. Bij het toekennen van deze rechten aan ondersteuners wordt er altijd een afweging gemaakt tussen 'het goed helpen van de teams' (doelbestemming) en de risico's van het geven van deze bevoegdheden. Wanneer dit risicovol is, wordt de bevoegdheden overgedragen aan de ISA-adviseur.
- Om te controleren of er niet een te ruime autorisatie wordt toegekend aan gebruikers, wordt per applicatie geïnventariseerd welke rapportagemogelijkheden er zijn om periodiek inzicht te krijgen in het autorisatieprofiel per gebruiker.

## Uitgangspunten rechten

- Als er naast de functioneel applicatiebeheerder nog andere gebruikers zijn die stamtabellen kunnen wijzigen, moet er een rapportage zijn die deze wijzigingen inzichtelijk maakt.
- Wanneer de rechtenstructuur binnen een applicatie niet fijnmazig genoeg is om een medewerker exact de juiste autorisatie te geven, kiest Amstelring voor het verstrekken van rechten die zo dicht mogelijk in de buurt komen van wat de medewerker nodig heeft. Tegelijk blijft Amstelring de leverancier aansporen om aanpassingen in de applicatie aan te brengen.
- Een medewerker die - door de beperkingen in de autorisatie-mogelijkheden van een applicatie - meer autorisaties krijgt dan nodig is voor de werkzaamheden, wordt uitvoerig getraind zodat helder is welke functies niet gebruikt mogen worden en welke gevolgen het heeft als de medewerker dit toch doet.
- De juiste autorisaties voor gebruik van persoonsgegevens zijn geregeld in de primaire applicaties, bijvoorbeeld Ons, Afas en Puur. Autorisaties binnen overige applicaties of reporting-tools die gebruik maken van de persoonsgegevens uit deze applicaties, inclusief het downloaden, gebruiken en delen van informatie uit deze applicaties naar bijvoorbeeld Spreadsheets of Excel, mogen nooit verder gaan qua inzage in persoonsgegevens dan geregeld in de primaire applicaties. Afwijkingen hierop kunnen aangevraagd worden via informatieveiligheid@amstelring.nl.
- Informatie over een cliënt is alleen zichtbaar voor een medewerker indien de medewerker een behandelrelatie heeft met de cliënt.
- Artsen hebben een bredere toegang. Een arts kan ook informatie zien van cliënten waar hij/zij geen directe behandelrelatie mee heeft. Artsen nemen diensten voor elkaar waar en hebben daarom een bredere toegang tot cliëntgegevens nodig.
- Gebruikers op ondersteunende afdelingen kunnen een bredere toegang krijgen als dat voor zijn of haar werkzaamheden nodig is.
- Informatie over een medewerker is zichtbaar voor een andere medewerker wanneer dit nodig is voor de werkzaamheden die bij zijn of haar rol horen. Zo kan bijvoorbeeld een roosteraar het deskundigheidsniveau van iemand inzien omdat dit nodig is bij het roosteren. Een salarisadministrateur kan de salarissen van iedereen inzien.
- Binnen een team zijn persoonlijke gegevens inzichtelijk als dat nodig is ten behoeve van zelfsturing.
- Bij het toekennen van rechten geldt het principe van ‘high trust, high penalty’. Er zal er

continu geïnvesteerd worden in deskundigheid en bewustwording.

## Overige aandachtspunten

- Amstelring maakt **geen groepsaccount** aan wanneer met het groepsaccount persoonsgegevens bewerkt of ingezien kunnen worden. Bestaande groepsaccounts, van waaruit meerdere medewerkers werken, worden zo snel mogelijk afgebouwd en verwijderd. Google heeft accounts waar meerdere medewerkers in kunnen, maar iedereen werkt daarin vanuit zijn of haar persoonlijke account.
- Groepsmailboxen zijn wel toegestaan. Persoonsgevoelige gegevens worden niet gemaild naar groepsmailboxen. Groepsmailboxen worden altijd vanuit een persoonlijk account benaderd.
- Voor het vervangen van een collega, bijvoorbeeld tijdens verzuim of verlof, worden tijdelijk extra rechten toegekend volgens een vaste afspraak (die is vastgelegd bij de autorisatiematrix). Hierbij wordt rekening gehouden met bijvoorbeeld avond- en weekenddiensten.

## Een medewerkersaccount

- Wanneer een medewerker in dienst komt, krijgen relevante functioneel applicatiebeheerders of ISA de benodigde informatie om een account te verstrekken.
- Wanneer de functie (of afdeling/locatie) van een medewerker wijzigt, en hierdoor wijzigingen moeten worden doorgevoerd in de autorisatie, ontvangt de functioneel applicatiebeheerder of ISA de informatie die nodig is om het account aan te passen.
- Wanneer een medewerker uit dienst gaat wordt indien mogelijk automatisch het verstrekte account afgesloten, anders wordt het account zo snel mogelijk handmatig afgesloten.
- Accounts voor externen worden altijd in opdracht van de proceseigenaar aangemaakt door de functioneel applicatiebeheerder of ISA, inclusief een omschrijving van de activiteiten waaruit de functioneel applicatiebeheerder kan opmaken welke autorisatie en toegang precies nodig is. Wat er aan rechten is verstrekt wordt meegenomen in de terugkoppeling. Hiervoor wordt ook een geheimhoudingsverklaring getekend door de betrokkene.
- Externen krijgen een persoonlijk account voor de applicaties die nodig zijn voor de werkzaamheden; hierbij zijn de reguliere uitgangspunten voor autorisatie van toepassing.
- Accounts voor externen/uitzendkrachten worden altijd voorzien van een einddatum zodat deze op het opgegeven moment vanzelf worden afgesloten.

Van bovenstaande procedures afwijken kan alleen binnen de kaders van de opgestelde autorisatiematrices, overige autorisatie en toegang wordt alleen verstrekt in opdracht van de proceseigenaar en indien het niet in tegenspraak is met de privacy-afspraken van Amstelring.

## Autorisatie Integraal Servicepunt Amstelring

Wanneer medewerkers van de teams problemen ervaren met een account (of applicatie), zoals onvoldoende autorisatie of toegang, nemen ze contact op met het ISA.

- Prioriteit is de medewerkers in teams direct te helpen, een te strakke autorisatie van het ISA moet het zorgproces niet vertragen;
- Per applicatie wordt bekeken welk type (persoons)gegevens er toegankelijk wordt door 'te breed' te autoriseren en besluiten. Hieruit volgt een risicoafweging of het risico op continuïteitsproblemen en datalekken acceptabel is;
- Als te breed autoriseren niet gewenst of mogelijk is, wordt de vraag doorgezet naar een medewerker van applicatiebeheer en/of ISA-adviseur voor de relevante applicatie.

## Functiescheiding en rollen

Functiescheiding is erop gericht om juistheid en volledigheid van de administratie van Amstelring te garanderen. Naast de kwaliteit van data dient functiescheiding als intern controlemechanisme, het helpt fraude te voorkomen. Het doorvoeren van een fijnmazige rechtenstructuur met ver doorgevoerde functiescheidingen is niet werkbaar voor zelfsturende teams en voor allround ondersteunende administratief medewerkers.

De volgende functiescheidingen zijn cruciaal en hebben een plaats in de rechtenstructuur en autorisaties. Deze opsomming is nog niet limitatief maar geeft wel de minimale functiescheiding aan.

Inkoop tot betalen-proces (AFAS/Proquro/Internetbankieren):

- Scheiding tussen muteren van crediteurenstamgegevens en de financiële administratie;
- Scheiding tussen het fiatteren van inkoopfacturen en de financiële administratie;
- Scheiding tussen het aanmaken van de betaaladvieslijst en de controle daarop;
- Scheiding tussen 1e en 2e handtekening in de bankapplicatie.

Zorgproces (ONS/NEDAP):

- De scheiding tussen indicatie stellen (niveau 5 verpleegkundige) en het plannen enerzijds en uitvoeren anderzijds;
- de scheiding tussen uitvoeren en fiatteren;
- de scheiding tussen registreren en controleren.

Medewerkerproces: (Afas)

- Scheiding tussen aanmaken mutatie in HRSS, autoriseren daarvan en de verwerking;
- Scheiding tussen aanmaken mutatie en de controle daarvan.

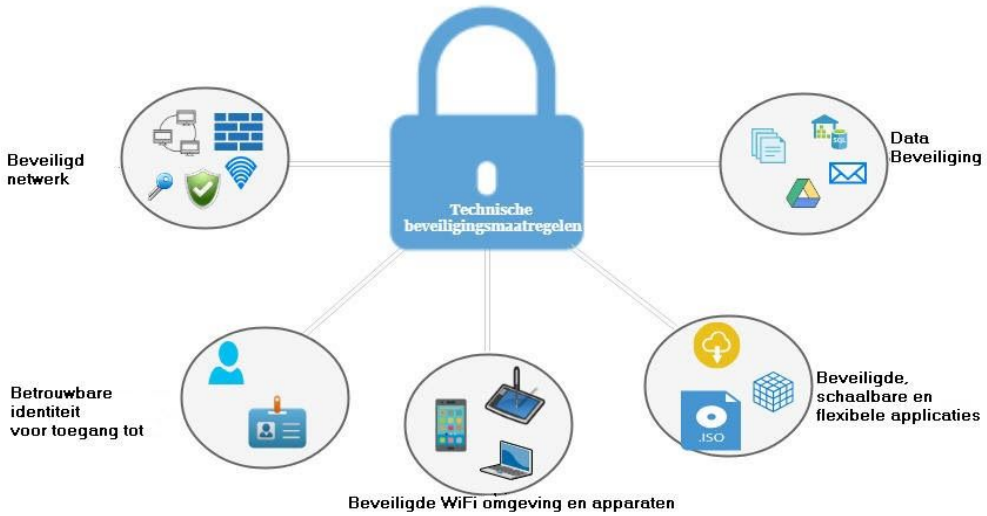
Binnen Amstelring hanteren we de volgende rollen met de daarbij behorende rechten (kort beschreven) aan de rechterkant. Leveranciers vallen logischerwijs niet binnen Amstelring maar worden wel genoemd omdat de functioneel applicatiebeheerders daar direct contact mee onderhouden en zij vaak rechten hebben binnen ons netwerk.

| Rol | Uitwerking |
|---|---|
| Leverancier | Tijdelijk op afspraak, wat nodig is voor uitoefening van de taken |
| Applicatiebeheerder | Admin rechten |
| ISA/Helpdesk | + Gebruikers beheerrechten voor zorgverleners<br>- Admin rechten |
| Supergebruikers | + Extra kennis<br>+ Betrokkenheid bij testen<br>+ Aanspreekpunt voor collega's<br>- Geen extra rechten |
| Gebruikers | Rechten voor het werken volgens dagelijks proces |

# 5. Hoe zorgen we dat alles blijft werken

## Technische maatregelen

Technische maatregelen worden ingezet om op een veilige wijze data te verwerken. Een netwerk zonder beveiliging is immers als een huis zonder slot op de voordeur. De beveiliging van het netwerk begint bij de ingang die toegang verschaft tot alle systemen, waarbij rekening gehouden wordt met het soort apparaten dat tegenwoordig op de werkvloer worden gebruikt.




Binnen Amstelring zijn de systemen berekend op **één ramp tegelijk.** Zo kan er omgegaan worden met stroomuitval, waterschade, brand of zombies, maar niet alle 'rampen' tegelijk. Onderstaand een aantal technische maatregelen die ingezet worden:

- **Beveiligd netwerk:** Er zijn diverse maatregelen genomen om het Amstelring computernetwerk te beveiligen tegen ongeautoriseerde toegang. Antivirus, spamfilters, Firewalls, wachtwoordbeleid, twee stappen authenticatie, data encryptie, LAN scheiding (gescheiden netwerken) en radius authenticatie zijn hier onderdeel van.

- **Gecontroleerde identiteit geeft toegang tot:** Het gaat hier primair om de authenticatie en de toegangsrechten die een gebruiker heeft in het netwerk, de zogenoemde autorisatie. Er wordt op toegezien dat de juiste personen de juiste rechten hebben en dat hier geen misbruik van gemaakt wordt.

- **Beveiligde WiFi omgeving en apparaten**: Het WiFi netwerk is een gescheiden omgeving welke is opgedeeld in een aantal netwerken waarbij, met uitzondering van het gastennetwerk, beveiligingsmethodes zijn ingesteld. De bedrijfsapparaten (smartphones, ipads, en chromebooks) worden middels een Mobile Device Management systeem beheerd.

- **Beveiligde, schaalbare en flexibele applicaties:** SaaS (Software as a Service) applicaties en SSO (single sign on) worden ingezet waardoor beschikbaarheid, schaalbaarheid en stabiliteit fors worden vergroot.

- **Data beveiliging:** Naast organisatorische maatregelen worden door de bovenstaande maatregelen datalekken en onbevoegde toegang tot bedrijfsinformatie voorkomen. Kwetsbaarheden in het netwerk proberen we op te sporen door jaarlijks een Pentest uit te voeren.

- **Wachtwoordbeleid:** Een wachtwoordbeleid wordt ingesteld om te voorkomen dat er misbruik wordt gemaakt van de toegang tot een digitale omgeving en data. Het beleid is meer dan alleen een aantal eisen. Naast complexe wachtwoorden, 2 stappen authenticatie, controle op het aantal inlogpogingen traint Amstelring ook op bewustwording en het belang van informatiebeveiliging in trainingen/cursussen.

## Leveranciersmanagement

Doordat cloud-applicaties worden ingezet is het minder duidelijk waar applicaties en gegevens zich feitelijk bevinden. Strenge afspraken met leveranciers over beveiliging (oa. ISO- en NEN-normen) en verantwoordelijkheid zijn belangrijk: dit wordt vastgelegd in verwerkers-overeenkomsten en Service Level Agreements. Om er zeker van te zijn dat de leveranciers voldoen aan de afspraken, vragen wij jaarlijks ISAE 3402 type II rapportages op. Daarnaast vragen wij om een ISO-certificering en aanvullend of wordt voldaan aan de NEN-normen. Wanneer dit niet het geval is wordt gezocht naar manieren om erachter te komen of een leverancier de zaken goed heeft geregeld.

## Continuïteitsplan

Om de beschikbaarheid van de vitale bedrijfsprocessen en informatievoorziening onder normale en buitengewone omstandigheden te waarborgen, zijn enkele processtappen en activiteiten nodig.

## Risico Impact Assessment (RIA)

Als jij of je team besluit om nieuwe IT systemen of processen te gebruiken, bestaande systemen of processen aan te passen (of stop te zettenn) moeten de **privacy, beveiliging en IT risico's** in kaart worden gebracht en eventueel risicoverlagende maatregelen genomen worden voordat de wijzigingen gemaakt worden.

Bij aanpassingen van systemen of processen bedoelen wij aanpassingen die leiden tot een andere werking of toepassing (bijvoorbeeld een verandering in inlogmethode of toevoeging van een nieuwe categorie persoonsgegevens) van persoonsgegevens ongeacht de grootte van de verandering. Het gaat hierbij niet over veranderingen op het gebied van inhoud of het aanpassen van andere soorten gegevens.

Het in kaart brengen van de risico's en het bedenken van risico verlagende maatregelen is mogelijk met behulp van de Amstelring Risico Impact Assessment (hierna: RIA). RIA's bestaan uit een vragenlijst die door een initiatiefnemer moet worden ingevuld. Dit assessment start met een aantal situatie vragen zodat snel duidelijk wordt of er een kort assessment (laag risico) of uitvoerig assessment (hoog risico) nodig is. Mocht de initiatiefnemer hulp nodig hebben bij het invullen, kan hij/zij ondersteuning vragen aan het ISA en/of ICT concernstaf medewerkers (via informatieveiligheid@amstelring.nl).

Het resultaat van het assessment (de antwoorden op de vragen) wordt uiteindelijk gedeeld met de functionaris gegevensbescherming en/of stuurgroep informatieveiligheid, wat eventueel kan leiden tot aanvullende privacy- en/of beveiligingsmaatregelen.

Hier is een link naar het formulier. Vul dit altijd in als je met een nieuwe wijziging bezig bent.

### Links

procedure datalekken
privacyverklaring
website Amstelring
Autoriteit persoonsgegevens
NEN 7510