ARTEMIS
HEALTH

Informatiebeveiligingsbeleid
&
Gedragscode

Document: 820330 A02
Versie: 1.0
Status: Goedgekeurd door de directie

Inhoudsopgave

01 Informatiebeveiligingsbeleid (IBB)

01.01 Algemeen

Artemis Health heeft integriteit, vertrouwen, flexibiliteit en kwaliteit van dienstverlening hoog in het vaandel staan. Binnen het bedrijf heerst een informele sfeer, waar op een professionele manier wordt samengewerkt. Artemis Health wil in alle opzichten een betrouwbare partner zijn. Respect, vertrouwen, passie, lef en innovatie zijn de kernwaarden in het doen en laten van alle medewerkers van Artemis Health.

Een betrouwbare informatievoorziening is onlosmakelijk verbonden met het leveren van kwalitatief goed werk. Risico's voor de klant moeten koste wat het kost worden vermeden. Vandaar dat Artemis Health haar beleid met betrekking tot de informatiebeveiliging heeft vastgelegd in dit document. Het beleid bevat algemene kaders en uitgangspunten, die door alle medewerkers moeten worden nageleefd. De eindverantwoordelijkheid voor het informatiebeveiligingsbeleid berust bij de directie van Artemis Health.

Gelet op de mogelijke impact van verstoringen op de bedrijfsvoering en continuïteit van Artemis Health en haar klanten, moeten maatregelen werkend worden gemaakt, zelfs als dit ten koste gaat van de effectiviteit, flexibiliteit en efficiency van de dienstverlening.

Het informatiebeveiligingsbeleid heeft tot doel het optreden van bedreigingen die de informatievoorziening van Artemis Health kunnen schaden, te voorkomen en/of de kans te verkleinen en/of eventuele gevolgen te beperken. Het IBB dient als uitgangspunt voor het inrichten van de informatiebeveiliging.

Het IBB is erop gericht de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren, waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de klant en/of medewerker wordt gerespecteerd en dat Artemis Health voldoet aan relevante wet- en regelgeving. Het omschrijft de doelstellingen en processen aangaande informatiebeveiliging.

Alle betrokkenen moeten zorgen dat aan de in dit IBB geformuleerde beleidsuitgangspunten wordt voldaan bij de inrichting van de organisatie, procedures, werkwijze en de daarbij gehanteerde informatiesystemen.

Dit beleid is van toepassing op alle informatie die gecreëerd, ontvangen, verzonden of bewaard wordt binnen de dienstverlening van Artemis Health aan klanten en de daarmee samenhangende contractuele verplichtingen, wetgeving en ondersteunende processen. Het beleid en de uitwerking hiervan gelden voor alle medewerkers van Artemis Health. Afwijkingen hierop moeten gemeld worden, zodat het systeem continu wordt verbeterd.

Het beleid geldt ook voor contractanten en stagiaires, die Artemis Health ondersteunen bij haar dienstverlening aan klanten. Dit zal kenbaar gemaakt worden bij het aangaan van een contract met een contractant en/of stagiaire.

De gedragscode met ethische normen van Artemis Health, waaraan alle medewerkers, contractanten en stagiaires zich moeten houden, is een integraal onderdeel van dit beleid.

Er wordt zoveel mogelijk gestreefd naar beveiligingsmaatregelen die gebaseerd zijn op logische principes, mede omdat deze kosteneffectief en duurzaam zijn.

Deze principes zijn:

- Vertrouwelijke gegevens die je niet hebt, hoef je niet te beveiligen;
- Niet slepen met vertrouwelijke gegevens;
- Scheiden van gegevens.

Alle medewerkers, contractanten en stagiaires worden geacht deze principes in de praktijk te brengen.

01.02 Informatiebeveiliging

Bedreigingen van een veilige en betrouwbare informatievoorziening kunnen fysiek van aard zijn, zoals brand en waterschade. Maar het kan ook technisch van aard zijn, bijvoorbeeld in de vorm van storingen in de programmatuur, apparatuur of de stroomvoorziening. De informatievoorziening kan ook worden bedreigd door fouten en vergissingen of door kwaadaardige acties, zoals hacking, phishing, computerfraude etc..

Informatiebeveiliging heeft tot doel het optreden van bedreigingen die de informatievoorziening van Artemis Health kunnen schaden, te voorkomen en/of de kans te verkleinen en/of eventuele gevolgen te beperken.

Artemis Health is verantwoordelijk voor het beschikbaar stellen van haar diensten met voldoende beveiligingsopties, zodat haar klanten kunnen voldoen aan de voor haar geldende wet- en regelgeving en informatiebeveiligingsnormen. Dit ontslaat de klant echter niet van de eindverantwoordelijkheid voor de beveiliging van zijn eigen informatievoorziening.

Artemis Health is verantwoordelijk voor het uitvoeren van taken, inclusief het bepalen van de te onderkennen risico's bij het systeem, het classificeren van het systeem en de daarbij behorende gegevens en het (laten) ontwikkelen van adequate beveiligingsmiddelen en interne controlemaatregelen.

Naast de applicatie(s) betreft dit ook de juiste inzet van de infrastructurele componenten (werkstations, servers en het interne en externe netwerk). De juiste verwerking, het adequate beheer, het goed functioneren van het personeel, het maken van afspraken met derden, fysieke beveiliging en voorzieningen om incidenten en calamiteiten te voorkomen of af te handelen.

Artemis Health blijft eindverantwoordelijk voor de aspecten van het informatiesysteem die uitbesteed worden aan de leveranciers. Hierbij wordt niet een maximaal beveiligingsniveau nagestreefd, maar een optimaal niveau, zodat Artemis Health haar bedrijfscontinuïteit te allen tijde kan borgen.

Jaarlijks wordt een interne audit gehouden. Onderdeel van deze interne audit is het opnieuw beoordelen van risico's en een beoordeling van nieuwe contracten en nieuwe wet- en regelgeving.

Onderdeel van deze interne audit is een plan met verbetervoorstellen. De directie beoordeelt het plan, stelt een oorzaakanalyse op en keurt verbetervoorstellen al dan niet goed. De directie kent een budget toe voor de realisatie van de verbetervoorstellen.

Daarnaast wordt jaarlijks een externe audit uitgevoerd op de werking van het IBB door een onafhankelijke externe partij, die hiertoe bevoegd en deskundig is. De rapportage hiervan is op aanvraag beschikbaar voor (potentiële) klanten.

01.03 Uitgangspunten

De beleidsuitgangspunten vormen de brug tussen de informatiebeveiligingsrisico's en de beheerdoelstellingen en -maatregelen van Artemis Health. De beleidsuitgangspunten bieden bovendien het kader voor de directie, met betrekking tot de wijze waarop de informatie-beveiligingsdoelstellingen, die passend zijn voor Artemis Health, worden vormgegeven. Genoemde beleidsuitgangspunten gelden voor die gegevensbewerkingen, waarvoor Artemis Health wettelijk en/of contractueel verantwoordelijk is.

Artemis Health hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging (en privacy) te bereiken:

01 Artemis Health voldoet aan alle relevante wet- en regelgeving en conformeert zich met betrekking tot de informatiebeveiliging aan de contractuele afspraken met klanten en leveranciers.

02 Bij Artemis Health is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel.

03 Artemis Health streeft ernaar, binnen haar dienstverlening aan klanten, de informatiebeveiliging continu te verbeteren.

04 Artemis Health zal alle betrokken partijen helder en actief informeren over de verwerkingen van hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokken partijen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens of de beperking van verwerking van de aanwezige data.

05 Binnen Artemis Health is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van de aanwezige geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van alle op papier aanwezige informatie.

06 Informatiebeveiliging is een belangrijk bedrijfsrisico voor Artemis Health. De directie stelt daarom het beleid vast, beoordeelt de risico’s, stelt de maatregelen vast, stelt voldoende middelen ter beschikking en laat periodiek de werking van het beleid en de naleving van deze maatregelen intern en extern beoordelen om ervoor te zorgen dat het informatiesysteem blijvend adequaat werkt en waar nodig verbeterd wordt.

07 De beheerdoelstellingen en -maatregelen van de norm NEN-1S0/IEC 27001 en de

privacyrichtlijnen van de Autoriteit Persoonsgegevens (AP) vormen, voor zover zij bijdragen aan de informatiebeveiliging van Artemis Health, het uitgangspunt voor de te definiëren maatregelen.

08 Artemis Health beschouwt computercriminaliteit als een ongewenst maatschappelijk probleem en ziet het als haar taak om passende maatregelen te nemen om schade ten gevolge van criminele activiteiten zoveel mogelijk te beperken.

09 Vertrouwen is voor Artemis Health een groot goed en zij hanteert naar medewerkers, klanten, leveranciers en andere stakeholders het wederkerigheidsprincipe. Artemis Health gaat ervan uit dat zij afspraken nakomen m.b.t. beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening.

10 Het personeelsbeleid is mede gericht op het verbeteren van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening bij medewerkers. Tijdens de inwerkperiode en een jaarlijkse awareness training wordt dit aan de orde gesteld.

11 De fysieke en logistieke beveiliging van de gebouwen en de ruimtes daarin zijn zodanig, dat de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens en gegevensverwerking inclusief de bedrijfsmiddelen gewaarborgd zijn.

12 Ontwikkeling of aanschaf, installatie en onderhoud van informatie- en communicatiesystemen, alsmede inpassing van nieuwe technologieën, moeten zo nodig met aanvullende maatregelen worden uitgevoerd, zodat hiermee geen afbreuk wordt gedaan aan de informatiebeveiliging.

13 Opdrachten aan derden voor het uitvoeren van werkzaamheden worden zodanig omgeven met maatregelen, dat er geen inbreuk op de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening kan ontstaan.

14 Bij de verwerking en het gebruik van gegevens worden maatregelen getroffen om de privacy van klanten, medewerkers, contractanten, stagiaires en andere betrokkenen te waarborgen.

15 Toegangsbeveiliging zorgt ervoor dat ongeautoriseerde personen of processen geen toegang krijgen tot de informatiesystemen, gegevensbestanden en programmatuur van Artemis Health.

16 Gegevensverstrekking extern gebeurt op basis van 'need to know'. Intern is dit niet altijd wenselijk, omdat kennisdeling essentieel is voor een kosteneffectieve dienstverlening aan klanten.

17 Artemis Health en haar medewerkers treffen maatregelen om te voorkomen dat vertrouwelijke informatie in handen van derden terechtkomt.

18 Input van klanten die vertrouwelijke informatie bevat, wordt na verwerking op korte termijn gearchiveerd of vernietigd.

19 Datatransport is zodanig met beveiligingsmaatregelen omkleed, dat geen inbreuk kan worden gepleegd op de vertrouwelijkheid en de integriteit van deze gegevens.

20 Geautoriseerde medewerkers, contractanten en stagiaires moeten ook op afstand een beveiligde toegang hebben tot de voor hun relevante productieomgevingen. Er worden geen vertrouwelijke gegevens buiten de productieomgeving opgeslagen. Onder condities kan hiervan afgeweken worden, maar dan wordt dit schriftelijk vastgelegd en periodiek beoordeeld of de afwijking valide is.

21 Het beheer en de opslag van gegevens in productieomgevingen zijn zodanig dat geen informatie verloren kan gaan, tenzij er sprake is van overmacht.

22 Bij veiligheidsincidenten of calamiteiten wordt onverwijld de directie geïnformeerd. Alle redelijke maatregelen zullen worden getroffen om de gevolgen van het incident/calamiteit zoveel mogelijk te beperken en/of een nieuw incident te voorkomen. Als het incident adequaat is afgehandeld, zullen hieruit 'lessons learned' uit worden getrokken en zal het systeem eventueel worden aangepast..

23 In het geval van een beveiligingsincident/calamiteit dat leidt tot een meldplicht of een informatieplicht aan de getroffenen, dan zal de directie daartoe het nodige verrichten.

24 Alle beveiligingsincidenten/calamiteiten worden door de directie geregistreerd.

25 Bij uitbesteding van gegevensverwerking kan de directie besluiten om tijdelijk af te wijken van deze beleidsuitgangspunten en de risico's hiervan tijdelijk te accepteren, mits dit schriftelijk vastgelegd en periodiek beoordeeld wordt.

26 Bij conflicten prevaleert het belang van Artemis Health boven de eisen die gesteld worden door de informatiebeveiliging en/of privacy.

27 Informatiebeveiliging is onderdeel van het ontwerpen, ontwikkelen en beheren van software, ook als die door derden wordt ontwikkeld. Security by design, privacy by design en privacy by default vormen hierbij de voornaamste uitgangspunten.

28 Extra aandacht moet worden besteed aan informatie of documenten die persoonsgegevens bevatten. De medewerker moet zich ervan bewust zijn dat hiervoor strenge wetgeving geldt.

29 Artemis Health en haar medewerkers, contractanten en stagiaires realiseren zich de privacy gevoeligheid van de (bijzondere) persoonsgegevens die zij verwerken. Zij waarborgen te allen tijde de afscherming, corrigeerbaarheid en transparantie van deze gegevens, ter bescherming van de persoonlijke levenssfeer van de betrokkenen.

01.04 Management bepalingen
Vaststelling van dit beleid geschiedt door de directie.

De directie informeert de medewerkers voorafgaande aan de invoering en bij wijziging van het informatiebeveiligingsbeleid. Daarbij wordt aangegeven wat over toezicht en controle is opgenomen.

Evaluatie van de inhoud, de werking en eventuele wijziging van dit beleid geschiedt conform de in dit informatiebeveiligingsbeleid opgenomen planning.

In alle gevallen waarin dit informatiebeveiligingsbeleid niet voorziet, beslist de directie.

02 Gedragscode

02.01 Algemeen

Deze gedragscode geeft regels voor het gebruik van de door Artemis Health aan de medewerker, contractant en stagiaire ter beschikking gestelde computerfaciliteiten. Tevens wordt aangegeven op welke wijze de controle op de naleving van deze regels zal plaatsvinden.

Naleving van het informatiebeveiligingsbeleid en de bijbehorende stukken is een verantwoordelijkheid van elke medewerker, contractant en stagiaire zelf. De directie zal medewerkers, contractanten en stagiaires coachen waar nodig. Ook wordt er voldoende training aangeboden op dit gebied.

Een aanvraag voor accounts, apparatuur en/of programmatuur wordt uitsluitend in behandeling genomen als deze wordt gedaan onder duidelijke vermelding van wat er precies benodigd is en met welk doel.

Alle ter beschikking gestelde apparatuur is bedoeld voor zakelijk gebruik. Privégebruik is alleen toegestaan als dit de dagelijkse werkzaamheden niet negatief beïnvloedt en niet schadelijk is voor de (prestaties van) computerfaciliteiten van Artemis Health.

Uitlevering van apparatuur en/of programmatuur wordt geregistreerd. Bij uitgifte wordt een bruikleenovereenkomst ter ondertekening aangeboden aan de medewerker.

02.02 Regels

De medewerker, contractant en stagiaire werkt altijd vanuit de beveiligde omgeving van het bedrijf: de programma's waartoe de medewerker gemachtigd is, zijn automatisch toegewezen op basis van rechten. Alleen in geval van uiterste noodzaak en/of met toestemming van de directie mag hierop een uitzondering worden gemaakt.

Medewerkers, contractanten en stagiaires zijn te allen tijde verantwoordelijk voor de aan hen beschikbaar gestelde apparatuur en programmatuur en worden geacht hier zorgvuldig mee om te gaan.

Het is niet toegestaan om eigen, meegebrachte apparatuur en programmatuur te gebruiken of te installeren. Dit geldt in het bijzonder voor externe gegevensdragers als USB-sticks, mobiele telefoons of externe harde schijven.

Alle uitgegeven apparaten (waaronder laptops, smartphones. etc.) die mogelijk toegang geven tot bedrijfsgevoelige of medische gegevens worden van een wachtwoord en/of encryptie voorzien. Het is aan de medewerker, contractant en stagiaire om zorg te dragen dat deze beveiliging in stand blijft en mogelijke problemen tijdig aan te melden bij de directie.

Het aansluiten van apparatuur op het netwerk van Artemis Health door middel van een netwerkkabel is niet toegestaan, tenzij goedgekeurd door de directie. Dit geldt ook voor apparaten die zijn uitgegeven door Artemis Health.

Het is de medewerker, contractant en stagiaire niet toegestaan de ter beschikking gestelde apparatuur, programmatuur, gegevensbestanden of documentatie ongeautoriseerd te kopiëren of ter beschikking te stellen aan derden.

Contractanten die meer dan 24 uur per week voor Artemis Health werken, krijgen dezelfde hardware en software als de medewerker in loondienst. Contractanten die minder dan 24 uur per week voor Artemis Health werken krijgen alleen een 'mail only' account.

Contractanten mogen nooit hun eigen e-mailadres gebruiken aangaande informatie van klanten van Artemis Health.

Werkplekken worden altijd netjes achtergelaten. Gevoelige documenten worden opgeborgen en het werkstation en/of de telefoon wordt vergrendeld.

Het is niet toegestaan informatie, die strijdig is met de wet of de goede zeden (o.a. pornografisch materiaal), informatie die een discriminerend, opruiend, aanstootgevend of bedreigend karakter heeft, met behulp van computerfaciliteiten van Artemis Health te produceren, te benaderen, te verzenden of in de openbaarheid te brengen.

Het is niet toegestaan andere personen met behulp van de computerfaciliteiten onheus te bejegenen of lastig te vallen.

Van een medewerker wordt verwacht dat hij gezond verstand toepast bij het openen van websites, e-mails en dergelijke. Ditzelfde geldt voor het (door)sturen van informatie. Bij twijfel dient een medewerker altijd contact op te nemen met de directie.

Het is de medewerker, contractant en stagiaire verboden om vertrouwelijke en/of schadelijke informatie te verstrekken over zijn werkzaamheden, de werkgever, collega's en/of relaties, partners of leveranciers.

02.03 Beveiliging

Alle uitgereikte toegangscodes en wachtwoorden zijn persoonlijk en mogen niet gedeeld worden. De medewerker is zelf verantwoordelijk voor een verantwoorde omgang met het gebruiken, beheren en wijzigen van wachtwoorden. De medewerker is verplicht om periodiek, doch minstens eenmaal per jaar, het wachtwoord te wijzigen.

Het is niet toegestaan om e-mails onnodig lang op te slaan. Als e-mails niet meer nodig zijn, dienen deze verwijderd te worden. Daarbij dient ook de prullenbak leeg te worden gemaakt, anders zijn de e-mails niet compleet verwijderd.

Indien gegevensdragers niet langer nodig zijn of defect zijn, moeten deze te allen tijde ingeleverd worden bij de directie. De directie zorgt dat de gegevensdrager veilig wordt gewist en/of op een veilige manier wordt vernietigd.

De medewerker is verantwoordelijk voor het verantwoord afdrukken van gegevens op printers en zal de vertrouwelijkheid van afgedrukt materiaal waarborgen.

02.04 Publiceren
Als een medewerker, contractant of stagiaire voornemens is iets te gaan publiceren over een klant of concurrent, dient voorafgaand overleg met de directie plaats te vinden. Degene, die na verkregen toestemming, tot publicatie overgaat, is persoonlijk verantwoordelijk voor de inhoud die hij, voor zover dat niet tot zijn functie behoort, publiceert, ongeacht van welk medium gebruik wordt gemaakt. Daarnaast dient hij altijd kenbaar te maken dat hij op persoonlijke titel publiceert.

Bij de geringste twijfel over de inhoud van een voorgenomen publicatie en/of over de raakvlakken met de werkgever, dient er voorafgaand overleg met de directie plaats te vinden.

02.05 Incidenten
De directie van Artemis Health heeft het recht om, na een gerezen verdenking van handelen in strijd met deze gedragscode, een gerichte controle uit te voeren. De gerichte controle zal slechts een beperkte periode duren van maximaal drie maanden.

Bij geconstateerde (beveiligings-) incidenten heeft de directie het recht om apparatuur en/of medewerkers, contractanten en stagiaires de toegang tot computers en/of netwerken (tijdelijk} te ontzeggen.

02.06 Ethische normen
In de gedragscode staat wat de kern is van waaruit Artemis Health en haar medewerkers, contractanten en stagiaires werken. De medewerkers van Artemis Health en/of medewerkers van externe partijen, die voor of namens Artemis Health werkzaamheden verrichten, voldoen aan onderstaande ethische normen.

Elke medewerker, contractant en stagiaire van Artemis Health:

Behandelt iedere klant, collega en externe relatie met aandacht en respect;

Is toegankelijk en aanspreekbaar;

Verplaatst zich in de belevingswereld van de ander en gaat in gesprek om duidelijk te krijgen wat nodig is;

Is vakbekwaam en weet wat zijn sterke en zwakke punten zijn;
Vertoont goed huisvaderschap[1] tegenover mensen en middelen waarmee wordt omgegaan;

Neemt verantwoordelijkheid voor het oplossen van problemen en mag daarbij altijd om hulp en advies vragen;

Gaat collegiaal, veiligheidsbewust en oplossingsgericht te werk;

[1] Goed huisvaderschap is een juridisch principe dat ervan uitgaat dat iemand zich redelijkerwijze als een verantwoord persoon gedraagt, die alles doet wat nodig is om voorzienbare schade te voorkomen.

Komt zijn afspraken na en stelt het zelf aan de orde als dit onverhoopt niet lukt;

Neemt een onderzoekende houding aan en vraagt feedback op zijn gedrag en prestaties;

Vraagt zich af wat hij kan betekenen voor de organisatie en degenen met wie wordt samengewerkt;

Weet wat in de samenleving en organisatie grensoverschrijdend is, handelt daarnaar en is daarop aanspreekbaar;

Signaleert in de eigen werkomgeving wat niet door de beugel kan en wat goed is maar verbeterd kan worden;

Begrijpt het belang van informatiebeveiliging en privacy voor de organisatie, klanten en ketenpartners en handelt daar naar;

De medewerker, contractant en stagiaire dient extra voorzichtig te zijn met het in discussie gaan met een klant of concurrent.

Kan -ook tegenover een kritische buitenstaander- uitleggen dat hij integer handelt.

Indien u bijgaande gelezen heeft en begrepen heeft en u gaat akkoord met naleving van bijgaand beleid, ontvangen wij een door u ondertekend exemplaar graag digitaal retour. Gelieve elke pagina te voorzien van uw paraaf.

ONDERTEKENING

Opdrachtnemer:

Naam:
Plaats:
Datum:

Handtekening:

……